Directrices 6/2020 sobre la interacción de la Segunda Directiva sobre servicios de pago y el Reglamento general de protección de datos

Versión 2.0

Adoptadas el 15 de diciembre de 2020

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

Historial de versiones

Versión 2.0	15.12.2020	Adopción de las Directrices después de la consulta pública
Versión 1.0	17.7.2020	Adopción de las Directrices para 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 adelante, «el RGPD»),

Visto el Acuerdo EEE, y en particular su anexo XI y su Protocolo 37, modificado por la Decisión n.º 154/2018 del Comité Mixto del EEE, de 6 de julio de 2018[1],

Vistos los artículos 12 y 22 de su Reglamento interno,

Considerando lo siguiente:

(1) El Reglamento general de protección de datos establece un conjunto de normas coherentes para el tratamiento de datos personales en toda la UE.

(2) La segunda Directiva sobre servicios de pago (Directiva 2015/2366/UE del Parlamento Europeo y del Consejo, de 23 de diciembre de 2015, en adelante la «DSP2») deroga la Directiva 2007/64/CE y establece nuevas normas para garantizar la seguridad jurídica de los consumidores, los comerciantes y las empresas en la cadena de pagos y modernizar el marco jurídico del mercado de servicios de pago[2]. Los Estados miembros estaban obligados a transponer la DSP2 a su Derecho nacional a más tardar el 13 de enero de 2018.

(3) Un elemento importante de la DSP2 es la introducción de un marco regulador de los nuevos servicios de iniciación de pagos y servicios de información sobre cuentas. La DSP2 permite a estos nuevos proveedores de servicios de pago obtener acceso a las cuentas de pago de los interesados a efectos de la prestación de dichos servicios.

(4) Con respecto a la protección de datos, de conformidad con el artículo 94, apartado 1, de la DSP2, todo tratamiento de datos personales, incluida la facilitación de información sobre el tratamiento, a los fines de los dispuesto en dicha Directiva, se llevará a cabo de conformidad con el RGPD[3] y con el Reglamento (UE) 2018/1725.

(5) El considerando 89 de la DSP2 establece que, cuando a efectos de dicha Directiva hayan de tratarse datos personales, deben especificarse los fines precisos, mencionarse la base jurídica pertinente y cumplir los requisitos de seguridad pertinentes establecidos en el RGPD, y se deben respetar los principios de necesidad, proporcionalidad, limitación de finalidad y plazo de retención de datos proporcionado. Asimismo, la protección de datos desde el diseño y la protección de datos por defecto deben incorporarse en todos los sistemas de tratamiento de datos desarrollados y usados en el marco de la DSP2[4].

(6) El considerando 93 de la DSP2 establece que el proveedor de servicios de iniciación de pagos y el proveedor de servicios de información sobre cuentas, por una parte, y el proveedor de servicios de

[1] Las referencias a los «Estados miembros» en el presente documento deben entenderse como referencias a los «Estados miembros del EEE».
[2] Considerando 6 de la DSP2.
[3] Dado que la DSP2 es anterior al RGPD, sigue haciendo referencia a la Directiva 95/46/CE. El artículo 94 del RGPD establece que las referencias a la Directiva 95/46/CE derogada se entenderán hechas al RGPD.
[4] Considerando 89 de la DSP2.

pago gestor de cuenta, por otra, deben cumplir las disposiciones sobre la necesaria protección y seguridad de los datos que se establecen o a las que se alude en dicha Directiva, o que figuren en normas técnicas de regulación.

HA ADOPTADO LAS SIGUIENTES DIRECTRICES

1. INTRODUCCIÓN

1. La segunda Directiva de servicios de pago (en adelante, la «DSP2») ha introducido una serie de novedades en el ámbito de los servicios de pago. Si bien crea nuevas oportunidades para los consumidores y aumenta la transparencia en este campo, la aplicación de la DSP2 plantea ciertas dudas y preocupaciones respecto a la necesidad de que los interesados sigan teniendo el pleno control de sus datos personales. El Reglamento general de protección de datos (en adelante, el «RGPD») se aplica al tratamiento de los datos personales, incluidas las actividades de tratamiento realizadas en el contexto de los servicios de pago, tal como se definen en la DSP2[5]. Así pues, los responsables del tratamiento que actúen en el ámbito cubierto por la DSP2 deben garantizar siempre el cumplimiento de los requisitos del RGPD, entre ellos los principios de protección de datos establecidos en el artículo 5 del RGPD, así como las disposiciones pertinentes de la Directiva sobre la privacidad y las comunicaciones electrónicas[6]. Si bien la DSP2[7] y las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros (en adelante, las «NTR»[8]) contienen ciertas disposiciones relativas a la protección de datos y la seguridad, han surgido dudas sobre la interpretación de estas disposiciones, así como sobre la interacción entre el marco general de protección de datos y la DSP2.

2. El 5 de julio de 2018, el CEPD emitió una carta relativa a la DSP2 en la que aportaba aclaraciones sobre cuestiones relativas a la protección de los datos personales en relación con la DSP2, en particular sobre el tratamiento de los datos personales de las partes no contratantes (los llamados «datos de las partes silenciosas») por parte de los proveedores de información sobre cuentas (en adelante, «PSIC») y los proveedores de servicios de iniciación de pagos (en adelante, «PSIP»), los procedimientos relativos a la comunicación y la retirada del consentimiento, las NTR y la cooperación entre los proveedores de servicios de pago gestores de cuentas (en adelante, «PSPGC») en relación con las medidas de seguridad. El trabajo de preparación de las presentes Directrices implicó recoger las aportaciones de las partes interesadas, tanto por escrito como en un encuentro, para determinar los retos más urgentes.

[5] Artículo 1, apartado 1, del RGPD.
[6] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas); DO L 201 de 31.7.2002, p. 37.
[7] Artículo 94 de la DSP2, etc.
[8] Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros (Texto pertinente a efectos del EEE); C/2017/7782; DO L 69 de 13.3.2018, p. 23; disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R0389&from=ES.

3. Estas Directrices pretenden proporcionar orientaciones adicionales sobre los aspectos de la protección de datos en el contexto de la DSP2, en particular sobre la relación entre las disposiciones pertinentes del RGPD y la DSP2. Las presentes Directrices se centran principalmente en el tratamiento de datos personales por parte de los PSIC y los PSIP. Como tal, este documento aborda las condiciones para conceder acceso a los PSPGC a información de las cuentas de pago y para el tratamiento de los datos personales por parte de los PSIP y los PSIC, así como los requisitos y las garantías en relación con el tratamiento de los datos personales por parte de los PSIC y los PSIP para fines distintos de los fines iniciales para los que se han recogido los datos, especialmente cuando se han recogido en el contexto de la prestación de un servicio de información sobre cuentas[9]. El presente documento también aborda las diferentes nociones de consentimiento explícito en virtud de la DSP2 y el RGPD, el tratamiento de «datos de partes silenciosas», el tratamiento de categorías especiales de datos personales por parte de los PSIP y los PSIC, la aplicación de los principales principios de protección de datos establecidos por el RGPD, como la minimización de datos, la transparencia, la responsabilidad proactiva y las medidas de seguridad. La DSP2 implica responsabilidades transversales en los ámbitos de la protección de los consumidores y la legislación sobre competencia, entre otros. Las consideraciones relativas a estos campos del Derecho quedan fuera del alcance de las presentes Directrices.

4. Para facilitar la lectura de las Directrices, a continuación se ofrecen las principales definiciones utilizadas en este documento.

1.1 Definiciones

«Proveedor de servicios de información sobre cuentas» (PSIC): el proveedor de un servicio en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago;

«Proveedor de servicios de pago gestor de cuenta» (PSPGC): un proveedor de servicios de pago que facilita a un ordenante una o varias cuentas de pago y se encarga de su mantenimiento;

«Minimización de datos»: un principio de protección de datos, según el cual los datos personales deben ser deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados;

«Ordenante»: la persona física o jurídica titular de una cuenta de pago que autoriza una orden de pago a partir de dicha cuenta o, en caso de que no exista una cuenta de pago, la persona física o jurídica que dicta una orden de pago;

«Beneficiario»: la persona física o jurídica que es el destinatario previsto de los fondos objeto de una operación de pago;

«Cuenta de pago»: una cuenta a nombre de uno o varios usuarios de servicios de pago y utilizada para la ejecución de operaciones de pago;

[9] Por «servicio de información sobre cuentas» se entiende un servicio en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago.

«Proveedor de servicios de iniciación de pagos» (PSIP): el proveedor de un servicio que permite iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago;

«Proveedor de servicios de pago»: los organismos contemplados en el artículo 1, apartado 1, de la DSP2[10] y las personas físicas o jurídicas que se acojan a la exención en virtud los artículos 32 y 33 de dicha Directiva;

«Usuario de servicios de pago»: la persona física o jurídica que utiliza un servicio de pago, ya sea como ordenante, beneficiario o ambos;

«Datos personales»: toda información sobre una persona física identificada o identificable («interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

La «protección de datos desde el diseño» se refiere a las medidas técnicas y organizativas integradas en un producto o servicio, que están diseñadas para aplicar los principios de la protección de datos, de manera eficaz, y para integrar las garantías necesarias en el tratamiento con el fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados;

La «protección de datos por defecto» se refiere a las medidas técnicas y organizativas apropiadas aplicadas en un producto o servicio que garantizan que, por defecto, solo se tratan los datos personales que son necesarios para cada finalidad específica del tratamiento;

«NTR» se refiere al Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros;

Los «proveedores terceros» se refieren tanto a los PSIP como a los PSIC.

1.2 Servicios en el marco de la DSP2

[10] El artículo 1, apartado 1, de la DSP2 establece las normas con arreglo a las cuales los Estados miembros distinguirán entre las siguientes categorías de *proveedores de servicios* de pago:
a) entidades de crédito definidas en el artículo 4, apartado 1, punto 1, del Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, incluidas sus sucursales en el sentido del artículo 4, apartado 1, punto 17, de dicho Reglamento que estén ubicadas en la Unión, tanto si las administraciones centrales de esas sucursales de entidades de crédito están ubicadas en el interior de la Unión como si, de conformidad con el artículo 47 de la Directiva 2013/36/UE y con la legislación nacional, lo están en el exterior de la Unión;
b) entidades de dinero electrónico en el sentido del artículo 2, punto 1, de la Directiva 2009/110/CE, incluidas, de conformidad con el artículo 8 de dicha Directiva y con la legislación nacional, sus sucursales si estas están ubicadas en la Unión y tienen su administración central fuera de la Unión, y en la medida en que los servicios de pago prestados por las sucursales estén vinculados a la emisión de dinero electrónico;
c) instituciones de giro postal facultadas en virtud de la legislación nacional para prestar servicios de pago;
d) entidades de pago;
e) el Banco Central Europeo (BCE) y los bancos centrales nacionales cuando no actúen en su condición de autoridad monetaria u otras autoridades públicas;
f) los Estados miembros y sus autoridades regionales y locales, cuando no actúen en su condición de autoridades públicas.

5. La DSP2 introduce dos nuevos tipos de servicios de pago (proveedores): Los proveedores de servicios de iniciación de pagos (PSIP) y los proveedores de servicios de información sobre cuentas (PSIC). El anexo 1 de la DSP2 contiene los ocho servicios de pago a los que se aplica la Directiva.

6. Los PSIP prestan servicios que permiten iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago[11]. Un PSIP puede solicitar a un PSPGC (normalmente un banco) que inicie una transacción en nombre del usuario del servicio de pago. El usuario (del servicio de pago) puede ser una persona física (interesado) o una persona jurídica.

7. Los PSIC prestan servicios en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago[12]. Con arreglo al considerando 28 de la DSP2, el usuario de servicios de pago puede tener en todo momento una visión global e inmediata de su situación financiera.

8. En lo que respecta a los servicios de información sobre cuentas, la oferta de servicios puede depender de según en qué funciones y finalidades se haga hincapié. Por ejemplo, algunos proveedores pueden ofrecer a los usuarios servicios como la planificación de presupuestos y el control del gasto. La DSP2 cubre el tratamiento de los datos personales en el contexto de estos servicios. Los servicios que implican evaluaciones de la solvencia del usuario del servicio de pago o los servicios de auditoría realizados sobre la base de la recopilación de información a través de un servicio de información sobre cuentas quedan fuera del ámbito de aplicación de la DSP2 y, por tanto, están al amparo del RGPD. Además, la DSP2 tampoco se aplica a las cuentas que no sean cuentas de pago (por ejemplo, las de ahorro o las de inversión). En cualquier caso, el RGPD es el marco jurídico aplicable para el tratamiento de datos personales.

Ejemplo 1:

La empresa HappyPayments ofrece un servicio en línea que consiste en el suministro de información sobre una o varias cuentas de pago a través de una aplicación móvil destinado a facilitar al usuario de servicios de pago la supervisión de sus finanzas (un servicio de información sobre cuentas). Con este servicio, este usuario puede consultar de un vistazo los saldos y las operaciones recientes en dos o más cuentas de pago en diferentes entidades bancarias. Si el usuario de servicios de pago opta por ello, también ofrece una categorización de los gastos e ingresos según diferentes tipologías (salario, ocio, energía, hipoteca, etc.) para ayudarle así a la hora de planificar sus finanzas. Con esta aplicación, HappyPayments también ofrece un servicio para iniciar pagos directamente desde la cuenta o cuentas de pago designadas por el usuario (un servicio de iniciación de pagos).

9. Para prestar esos servicios, la DSP2 regula las condiciones legales en las que los PSIP y los PSIC pueden acceder a las cuentas de pago para prestar un servicio al usuario de servicios de pago.

10. El artículo 66, apartado 1, y el artículo 67, apartado 1, de la DSP2 determinan que el acceso y la utilización de los servicios de pago e información de cuentas son derechos del usuario de servicios de pago. Esto significa que el usuario de servicios de pago debe seguir teniendo plena libertad con respecto al ejercicio de tales derechos y no se le puede obligar a que haga uso de ellos.

11. El acceso a las cuentas de pago y el uso de la información de dichas cuentas se regulan en parte en los artículos 66 y 67 de la DSP2, que contienen garantías relativas a la protección de los datos

[11] Artículo 4, apartado 15, de la DSP2.
[12] Artículo 4, apartado 16, de la DSP2.

(personales). El artículo 66, apartado 3, letra f), de la DSP2 establece que el proveedor de servicios de iniciación de pagos no solicitará al usuario de servicios de pago ningún dato distinto de los necesarios para prestar el servicio de iniciación del pago, y el artículo 66, apartado 3, letra g), de dicha Directiva establece que el proveedor de servicios de iniciación de pagos no utilizará, almacenará o accederá a ningún dato para fines distintos de la prestación del servicio de iniciación de pagos expresamente solicitado por el usuario de servicios de pago. Además, el artículo 67, apartado 2, letra d), de la DSP2 limita el acceso de los proveedores de servicios de información sobre cuentas a la información de las cuentas de pago designadas y las operaciones de pago correspondientes, mientras que el artículo 67, apartado 2, letra f), de dicha Directiva establece que el proveedor de servicios de información sobre cuentas no utilizará, almacenará o accederá a ningún dato, para fines distintos de la prestación del servicio de información sobre cuentas expresamente solicitado por el usuario del servicio de pago, de conformidad con las normas sobre protección de datos. Esto último subraya que, en el contexto de los servicios de información sobre cuentas, los datos personales solo pueden recogerse con fines específicos, explícitos y legítimos. Por lo tanto, un PSIC debe explicitar en el contrato para qué fines específicos se van a tratar los datos personales de información sobre cuentas, en el contexto del servicio de información sobre cuentas que presta. El contrato debe ser lícito, leal y transparente de acuerdo con el artículo 5 del RGPD y también debe cumplir con otras normas en materia de protección del consumidor.

12. Dependiendo de las circunstancias específicas, los proveedores de servicios de pago podrían ser un responsable o un encargado del tratamiento de datos con arreglo a lo dispuesto en el RGPD. En las presentes Directrices, los «responsable del tratamiento» son los proveedores de servicios de pago que, sola o conjuntamente con terceros, determinan los fines y medios del tratamiento de datos personales. Se puede encontrar más orientaciones al respecto en las Directrices 7/2020 del CEPD sobre los conceptos de responsable y encargado del tratamiento en el RGPD.

2 FUNDAMENTOS JURÍDICOS Y TRATAMIENTO ULTERIOR CONFORME A LA DSP2

2.1 Fundamentos jurídicos para el tratamiento

13. De conformidad con el RGPD, los responsables del tratamiento deben tener una base jurídica para el tratamiento de datos personales. El artículo 6, apartado 1, del RGPD constituye una lista exhaustiva y restrictiva de seis bases jurídicas para el tratamiento de datos personales en virtud de dicho Reglamento[13]. Corresponde al responsable del tratamiento definir la base jurídica adecuada y asegurarse de que se cumplen todas las condiciones de dicha base. Determinar qué base es válida y más adecuada en una situación concreta depende de las circunstancias en las que se produce el tratamiento, como por ejemplo su finalidad y la relación entre el responsable del tratamiento y el interesado.

2.2 Artículo 6, apartado 1, letra b), del RGPD (el tratamiento es necesario para la ejecución de un contrato)

14. Los servicios de pago se prestan sobre una base contractual entre el usuario de servicios de pago y el proveedor de servicios de pago. Como se indica en el considerando 87 de la DSP2, «[l]a presente Directiva debe referirse únicamente a las obligaciones y responsabilidades contractuales entre el usuario de servicios de pago y su proveedor de servicios de pago». Por lo que respecta al RGPD, la principal base jurídica para el tratamiento de datos personales para la prestación de servicios de pago es el artículo 6, apartado 1, letra b), de dicho Reglamento, lo que significa que el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

15. Los servicios de pago en virtud de la DSP2 se definen en su anexo I. La prestación de estos servicios, según la definición de la DSP2, es un requisito para la celebración de un contrato en el que las partes tienen acceso a los datos de la cuenta de pago del usuario de servicios de pago. Estos proveedores de servicios de pago también tienen que ser operadores con licencia. En relación con los servicios de iniciación de pagos y los servicios de información sobre cuentas en el marco de la DSP2, los contratos pueden incorporar cláusulas que también impongan condiciones sobre

[13] De conformidad con el artículo 6, el tratamiento solo será lícito en la medida en que sea de aplicación alguno de los siguientes supuestos:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

servicios suplementarios que no están regulados por dicha Directiva. Las *Directrices 2/2019 del CEPD 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* dejan claro que los responsables del tratamiento tienen que evaluar qué tratamiento de datos personales es objetivamente necesario para la ejecución del contrato. Dichas Directrices señalan que la justificación de la necesidad depende de la naturaleza del servicio, de las perspectivas recíprocas y las expectativas de las partes del contrato, la justificación y de sus elementos esenciales del mismo.

16. Las Directrices 2/2019 del CEPD también dejan claro que, a la luz del artículo 7, apartado 4, del RGPD, se introduce una distinción entre las actividades de tratamiento necesarias para la ejecución de un contrato y las cláusulas que supeditan el servicio a determinadas actividades de tratamiento que no son en realidad necesarias para la ejecución del contrato. La expresión «necesario para la ejecución» indica claramente que no basta una mera cláusula contractual[14]. El responsable del tratamiento debe poder demostrar cómo el objeto principal del contrato específico con el interesado no puede, de hecho, ejecutarse si no se produce el tratamiento específico de los datos personales en cuestión. La mera referencia o mención del tratamiento de datos en un contrato no es suficiente para considerar incluido dicho tratamiento en el ámbito de aplicación del artículo 6, apartado 1, letra b), del RGPD.

17. El artículo 5, apartado 1, letra b), del RGPD contempla el principio de limitación de la finalidad, que requiere que los datos personales se recojan con fines determinados, explícitos y legítimos, y no se traten ulteriormente de manera incompatible con dichos fines. Al valorar si el artículo 6, apartado 1, letra b), constituye un fundamento jurídico adecuado para el tratamiento en el contexto de un servicio contractual en línea, debe prestarse atención al fin, el propósito o el objetivo particular del servicio[15]. Estos fines deben especificarse y comunicarse de manera clara al interesado, respetando así las obligaciones de limitación de la finalidad y transparencia que debe cumplir el responsable del tratamiento. Al evaluar qué es «necesario», debe realizarse una valoración combinada y basada en los hechos del tratamiento «para el objetivo que se persigue, evaluando si resulta menos intrusivo que otras opciones disponibles para conseguir el mismo objetivo». El artículo 6, apartado 1, letra b), no cubre los tratamientos que resulten útiles pero no sean objetivamente necesarios para la prestación del servicio contractual o para la aplicación de las medidas precontractuales pertinentes a petición del interesado, incluso si resultan necesarios para los demás fines comerciales del responsable del tratamiento[16].

18. Las Directrices 2/2019 del CEPD dejan claro que los contratos no pueden ampliar artificialmente las categorías de datos personales o los tipos de operaciones de tratamiento que el responsable del tratamiento necesita llevar a cabo para la ejecución del contrato en los términos del artículo 6, apartado 1, letra b)[17]. Estas Directrices también abordan los casos en los que pueden crearse situaciones de «todo o nada» para los interesados que únicamente deseen contratar uno de los servicios. Esto puede ocurrir cuando un responsable del tratamiento desea agrupar en un único contrato distintos servicios o elementos de un servicio con diferentes objetivos fundamentales, características o justificaciones. Cuando el contrato incluya varios servicios o elementos de un

[14] 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, CEPD, página 10.
[15] Véase la nota 15.
[16] Véase la nota 15, página 10.
[17] Véase la nota 15, página 11.

servicio independientes que razonablemente pueden ejecutarse de manera independiente entre sí, la aplicabilidad del artículo 6, apartado 1, letra b), debe evaluarse en el contexto de cada uno de dichos servicios por separado, examinando qué es necesario desde un punto de vista objetivo para ejecutar cada uno de los servicios que el interesado haya solicitado o a los que se haya suscrito[18].

19. De acuerdo con las citadas Directrices, los responsables del tratamiento deben evaluar lo que es necesario desde un punto de vista objetivo para la ejecución del contrato. Cuando los responsables del tratamiento no pueden demostrar que el tratamiento de los datos personales de las cuentas de pago es necesario desde un punto de vista objetivo para la prestación de cada uno de estos servicios por separado, el artículo 6, apartado 1, letra b), del RGPD no es un fundamento jurídico válido para el tratamiento. En estos casos, el responsable del tratamiento deberá tener en cuenta otro fundamento jurídico para el tratamiento.

2.3 Prevención del fraude

20. El artículo 94, apartado 1, de la DSP2 establece que los Estados miembros autorizarán el tratamiento de datos personales por los sistemas de pago y los proveedores de servicios de pago cuando sea necesario a fin de garantizar la prevención, la investigación y el descubrimiento del fraude en los pagos. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude podría constituir un interés legítimo del proveedor de servicios de pago en cuestión, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado[19]. Las actividades de tratamiento con fines de prevención del fraude deben basarse en una cuidadosa evaluación caso por caso por parte del responsable del tratamiento, de conformidad con el principio de responsabilidad proactiva. Además, para prevenir el fraude, los responsables del tratamiento también pueden estar sujetos a obligaciones legales específicas que requieran el tratamiento de datos personales.

2.4 Tratamiento ulterior (PSIC y PSIP)

21. El artículo 6, apartado 4, del RGPD determina las condiciones para el tratamiento de datos personales para otro fin distinto de aquel para el que se recogieron. Más concretamente, este tratamiento ulterior puede tener lugar, cuando está basado en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, cuando el interesado haya dado su consentimiento o cuando el tratamiento para un fin distinto de aquel para el que se recogieron los datos personales sea compatible con el fin inicial.

22. Hay que tener muy en cuenta el artículo 66, apartado 3, letra g) y el artículo 67, apartado 2, letra f) de la DSP2. Como ya se ha mencionado, el artículo 66, apartado 3, letra g) de la DSP2 establece que el PSIP no utilizará, almacenará o accederá a ningún dato para fines distintos de la prestación del servicio de iniciación de pagos expresamente solicitado por el ordenante. En el artículo 67, apartado 2, letra f), de la DSP2, se establece que el PSIC no utilizará, almacenará o accederá a ningún dato, para fines distintos de la prestación del servicio de información sobre cuentas expresamente solicitado por el usuario del servicio de pago, de conformidad con las normas sobre protección de datos.

23. En consecuencia, el artículo 66, apartado 3, letra g) y el artículo 67, apartado 2, letra f), de la DSP2 restringen considerablemente las posibilidades de tratamiento para otros fines, lo que significa

[18] Véase la nota 15, página 12.
[19] Considerando 47 del RGPD.

que no se permite el tratamiento para otro fin, a menos que el interesado haya dado su consentimiento de conformidad con el artículo 6, apartado 1, letra a), del RGPD o que el tratamiento esté establecido por el Derecho de la Unión o del Estado miembro al que está sujeto el responsable del tratamiento, de conformidad con el artículo 6, apartado 4, del RGPD. Cuando el tratamiento de datos personales para otro fin distinto de aquel para el que se recogieron no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de un Estado miembro, las restricciones establecidas en el artículo 66, apartado 3, letra g), y en el artículo 67, apartado 2, letra f), de la DSP2 dejan claro que cualquier otra finalidad no es compatible con la finalidad para la que se recogen inicialmente los datos personales. La prueba de compatibilidad del artículo 6, apartado 4, del RGPD no puede constituir una base jurídica para el tratamiento.

24. El artículo 6, apartado 4, del RGPD permite el tratamiento ulterior basado en el Derecho de la Unión o de los Estados miembros. Por ejemplo, todos los PSIP y los PSIC son entidades obligadas en virtud del artículo 3, apartado 2, letra a), de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. Estas entidades obligadas, por consiguiente, deben aplicar las medidas de diligencia debida con respecto al cliente especificadas en la Directiva. Por lo tanto, los datos personales tratados en relación con un servicio cubierto por la DSP2 se tratan ulteriormente sobre la base de al menos una obligación legal que recae sobre el proveedor de servicios[20].

25. Como se menciona en el apartado 20, el artículo 6, apartado 4, del RGPD indica que el tratamiento de datos personales para otro fin distinto de aquel para el que se recogieron podría basarse en el consentimiento del interesado, si se cumplen todas las condiciones para el consentimiento con arreglo al RGPD. Como ya se ha indicado, el responsable del tratamiento debe demostrar que es posible denegar o retirar el consentimiento sin sufrir perjuicio alguno (considerando 42 del RGPD).

2.5 Fundamento jurídico para conceder el acceso a la cuenta (PSPGC)

26. Como se menciona en el apartado 10, los usuarios de servicios de pago pueden ejercer su derecho a hacer uso de los servicios de iniciación de pagos e información sobre cuentas. Las obligaciones impuestas a los Estados miembros en el artículo 66, apartado 1, y en el artículo 67, apartado 1, de la DSP2 deben incorporarse a la legislación nacional a fin de garantizar la aplicación efectiva del derecho del usuario de servicios de pago a beneficiarse de los mencionados servicios de pago. La aplicación efectiva de estos derechos no sería posible sin la existencia de la correspondiente obligación del proveedor de servicios de pago, normalmente un banco, de conceder al proveedor de servicios de pago acceso a la cuenta con la condición de que haya cumplido todos los requisitos para obtener el acceso a la cuenta del usuario de servicios de pago. Además, el artículo 66, apartado 5, y el artículo 67, apartado 4, de la DSP2 establecen claramente que prestación de servicios de iniciación de pagos no se supeditará a la existencia de una relación contractual a tal fin entre los proveedores de servicios de iniciación de pagos y los proveedores de servicios de pago gestores de cuentas.

27. El tratamiento de los datos personales por parte del PSPGC, consistente en conceder el acceso a los datos personales solicitados por el PSIP y el PSIC para prestar su servicio de pago al usuario de servicios de pago, se basa en una obligación legal. Para lograr los objetivos de la DSP2, los PSPGC deben proporcionar los datos personales para los servicios de los PSIP y los PSIC, lo cual es una condición necesaria para que estos puedan prestar sus servicios y así garantizar los derechos

[20] Téngase en cuenta que el presente documento no tiene por objeto examinar en profundidad la cuestión de si la Directiva antiblanqueo cumple la norma del artículo 6, apartado 4, del GDPR.

previstos en el artículo 66, apartado 1, y el artículo 67, apartado 1, de la DSP2. Por lo tanto, el fundamento jurídico aplicable en este caso es el artículo 6, apartado 1, letra c), RGPD.

28. Dado que el RGPD ha especificado que el tratamiento basado en una obligación legal debe estar expresamente establecido por el Derecho de la Unión o de los Estados miembros (véase el artículo 6, apartado 3, del RGPD), la obligación de los PSPGC de conceder acceso debe derivarse de la legislación nacional que transpone la DSP2.

3 CONSENTIMIENTO EXPLÍCITO

3.1 Consentimiento según el RGPD

29. Con arreglo al RGPD, el consentimiento es uno de los seis fundamentos jurídicos de la licitud del tratamiento de datos personales. En virtud del artículo 4, apartado 11, del RGPD, «consentimiento» se define como «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen». Estas cuatro condiciones, a saber, voluntad libre, específica, informada e inequívoca, resultan esenciales para la validez del consentimiento. De acuerdo con las Directrices 5/2020 del CEPD sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, el consentimiento solo puede ser una base jurídica adecuada si se ofrece al interesado control y una capacidad real de elección con respecto a si desea aceptar o rechazar las condiciones ofrecidas o rechazarlas sin sufrir perjuicio alguno. Cuando solicita el consentimiento, el responsable del tratamiento tiene la obligación de evaluar si dicho consentimiento cumplirá todos los requisitos para la obtención de un consentimiento válido. Si se obtiene en pleno cumplimiento del RGPD, el consentimiento es una herramienta que otorga a los interesados el control sobre si los datos personales que les conciernen van a ser tratados o no. Si no es así, el control del interesado será meramente ilusorio y el consentimiento no será una base jurídica válida para el tratamiento, lo que convertirá dicha actividad de tratamiento en una actividad ilícita[21].

30. El RGPD también contiene otras garantías en su artículo 7, que establece que el responsable debe ser capaz de demostrar que hubo un consentimiento válido en el momento del tratamiento. Asimismo, la solicitud de consentimiento debe presentarse de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. Además, el interesado debe ser informado del derecho a retirar el consentimiento en cualquier momento, de forma tan sencilla como lo fue otorgarlo.

31. Según el artículo 9 del RGPD, el consentimiento es una de las excepciones a la prohibición general de tratamiento de categorías especiales de datos personales. Sin embargo, en tal caso, el consentimiento del interesado debe ser «explícito»[22].

32. Según las Directrices 5/2020 del CEPD sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, el término «explícito» conforme al RGPD se refiere a la manera en que el interesado expresa el consentimiento. Significa que el interesado debe realizar una declaración expresa de consentimiento para fines de tratamiento específicos. Una manera evidente de garantizar que el consentimiento es explícito sería confirmar de manera expresa dicho consentimiento en una declaración escrita. Cuando proceda, el responsable podría asegurarse de que el interesado firma la declaración escrita, con el fin de eliminar cualquier posible duda o falta de prueba en el futuro.

33. En ningún caso puede inferirse el consentimiento de declaraciones o acciones potencialmente ambiguas. Un responsable del tratamiento debe tener también en cuenta que el consentimiento

[21] Directrices 5/2020 del CEPD sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, apartado 3.

[22] Véase también el Dictamen 15/2011 sobre la definición de consentimiento (WP 187), p. 6, o el 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), pp. 9, 10, 13 y 14.

no puede obtenerse mediante la misma acción por la que el usuario acuerda un contrato o acepta los términos y condiciones generales de un servicio.

3.2 Consentimiento según la DSP2

34. El CEPD señala que el marco jurídico relativo al consentimiento explícito es complejo, ya que tanto la DSP2 como el RGPD incluyen el concepto de «consentimiento explícito». Esto lleva a la cuestión de si el «consentimiento expreso» mencionado en el artículo 94, apartado 2, de la DSP2 debe interpretarse de la misma manera que el consentimiento explícito en virtud del RGPD.

3.2.1 Consentimiento expreso según el artículo 94, apartado 2, de la DSP2

35. La DSP2 incluye una serie de normas específicas relativas al tratamiento de datos personales, en particular en su artículo 94, apartado 1, que determina que el tratamiento de datos personales a efectos de la DSP2 debe cumplir con la legislación de protección de datos de la UE. Asimismo, el artículo 94, apartado 2, de la DSP2 establece que los proveedores de servicios de pago únicamente obtendrán, tratarán y conservarán los datos personales necesarios para la provisión de sus servicios de pago, únicamente con el consentimiento expreso del usuario del servicio de pago. De conformidad con el artículo 33, apartado 2, de la DSP2, este requisito del consentimiento expreso del usuario de servicios de pago no se aplica a los PSIC. Sin embargo, el artículo 67, apartado 2, letra a), de la DSP2 sigue previendo el consentimiento explícito de los PSIC para la prestación del servicio.

36. Como se ha mencionado anteriormente, la lista de bases jurídicas para el tratamiento según el RGPD es exhaustiva. Como se ha mencionado en el apartado 14, la base jurídica para el tratamiento de datos personales para la prestación de servicios de pago es, en principio, el artículo 6, apartado 1, letra b), de dicho Reglamento, lo que significa que el tratamiento es necesario para la ejecución de un contrato del que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. De ello se deduce que el artículo 94, apartado 2, de la DSP2 no puede considerarse una base jurídica adicional para el tratamiento de datos personales. El CEPD considera que, a la vista de lo anterior, este apartado debe interpretarse, por un lado, en coherencia con el marco jurídico de protección de datos aplicable y, por otro, de forma que se preserve su efecto útil. Por lo tanto, el consentimiento expreso en virtud del artículo 94, apartado 2, de la DSP2 debe considerarse un requisito adicional de carácter contractual[23] en relación con el acceso y el posterior tratamiento y almacenamiento de datos personales con el fin de prestar servicios de pago y, por lo tanto, no es lo mismo que el consentimiento (explícito) en virtud del RGPD.

37. El «consentimiento expreso» al que se refiere el artículo 94, apartado 2, de la DSP2 es un consentimiento contractual. Esto implica que el artículo 94, apartado 2, de la DSP2 debe interpretarse en el sentido de que, al celebrar un contrato con un proveedor de servicios de pago en el marco de dicha Directiva, los interesados deben ser plenamente conscientes de las categorías específicas de datos personales que se tratarán. Además, tienen que ser informados de la finalidad específica (del servicio de pago) para la que se tratarán sus datos personales y tienen que aceptar de manera expresa estas cláusulas. Dichas cláusulas deben distinguirse claramente de las demás cuestiones tratadas en el contrato y el interesado las deberá aceptar expresamente.

38. Un aspecto central del concepto de «consentimiento expreso», según el artículo 94, apartado 2, de la DSP2, es la obtención del acceso a los datos personales para su posterior tratamiento y

[23] Carta del CEPD relativa a la DSP2, 5 de julio de 2018, página 4.

almacenamiento con el fin de prestar servicios de pago. Esto implica que el proveedor del servicio de pago[24] aún no está tratando los datos personales, pero necesita acceder a datos de carácter personal que han sido tratados bajo la responsabilidad de cualquier otro responsable del tratamiento. Si un usuario de servicios de pago celebra un contrato, por ejemplo, con un proveedor de servicios de iniciación de pagos, este proveedor necesita obtener acceso a datos personales del usuario de servicios de pago que se están tratando bajo la responsabilidad del proveedor de servicios de pago gestor de cuentas. El objeto del consentimiento expreso en virtud del artículo 94, apartado 2, de la DSP2 es el permiso para obtener el acceso a dichos datos de carácter personal, para poder tratar y almacenar los datos necesarios para la prestación del servicio de pago. Si el interesado da su consentimiento expreso, el proveedor de servicios de pago gestor de cuentas está obligado a dar acceso a los datos personales indicados.

39. Aunque el consentimiento del artículo 94, apartado 2, de la DSP2 no es un fundamento jurídico para el tratamiento de datos personales, este consentimiento está específicamente relacionado con los datos personales y la protección de datos, y garantiza la transparencia y un cierto grado de control para el usuario del servicio de pago[25]. Si bien la DSP2 no especifica los requisitos de fondo del consentimiento en virtud de su artículo 94, apartado 2, debe entenderse, como se ha indicado, en coherencia con el marco jurídico de protección de datos aplicable y de forma que se preserve su efecto útil.

40. En cuanto a la información que deben proporcionar los responsables del tratamiento y el requisito de transparencia, las Directrices del Grupo de Trabajo del Artículo 29 sobre la transparencia especifican que «[u]na consideración fundamental del principio de transparencia esbozado en estas disposiciones es que el interesado debe poder determinar de antemano el alcance y las consecuencias derivadas del tratamiento, y que no debe verse sorprendido en un momento posterior por el uso que se ha dado a sus datos personales»[26].

41. Además, tal como exige el principio de limitación de la finalidad, los datos personales deben recogerse con fines específicos, explícitos y legítimos [artículo 5, apartado 1, letra b), del RGPD]. Cuando los datos personales se recojan para más de un fin, *los responsables del tratamiento deben evitar determinar solo una finalidad general para justificar diversas actividades de tratamiento ulteriores que, de hecho, solo están remotamente relacionadas con el fin inicial real*[27]. El CEPD ha puesto de relieve, más recientemente en el contexto de los contratos de servicios en línea, el riesgo de incluir cláusulas generales de tratamiento en los contratos y ha declarado que la finalidad de la recogida debe identificarse de manera clara y concreta: debe estar lo suficientemente detallada como para determinar qué tratamientos se incluyen y cuáles no se incluyen en la finalidad especificada y para permitir la evaluación del cumplimiento de la normativa y la aplicación de las garantías relativas a la protección de datos[28].

42. Cuando se considera en el contexto del requisito adicional del consentimiento expreso de conformidad con el artículo 94, apartado 2, de la DSP2, esto implica que los responsables del

[24] Esto se aplica a los servicios 1 a 7 del anexo I de la DSP2.
[25] El artículo 94, apartado 2, de la DSP2 está incluido en el capítulo 4 «Protección de datos».
[26] Grupo de Trabajo del Artículo 29, Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, apartado 10 (adoptadas el 11 de abril de 2018) y refrendadas por el CEPD.
[27] Dictamen 3/2013 del Grupo de Trabajo del Artículo 29 sobre la limitación de la finalidad (WP203), página 16.
[28] 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, apartado 16 (versión de la consulta pública) y Dictamen 03/2013 del Grupo de Trabajo del Artículo 29 sobre la limitación de la finalidad (WP203), página 15.

tratamiento deberán proporcionar a los interesados información específica y explícita sobre los fines concretos identificados por el responsable del tratamiento para los que se accede, se trata y se conservan sus datos personales. De acuerdo con el artículo 94, apartado 2, de la DSP2, los interesados deben aceptar expresamente estos fines específicos.

43. Además, como se indica en el apartado 10, el CEPD destaca que el usuario de servicios de pago debe poder elegir si utiliza o no el servicio y no se le puede obligar a hacerlo. Por lo tanto, el consentimiento en virtud del artículo 94, apartado 2, de la DSP2 también tiene que ser un consentimiento basado en la voluntad libre.

3.3 Conclusión

44. El consentimiento expreso en el marco de la DSP2 es diferente del consentimiento (explícito) entendido conforme al RGPD. El consentimiento expreso en virtud del artículo 94, apartado 2, de la DSP2 constituye un requisito adicional de carácter contractual. Cuando un proveedor de servicios de pago necesita acceder a los datos personales para la prestación de un servicio de pago, es necesario el consentimiento expreso del usuario del servicio de pago, de conformidad con el artículo 94, apartado 2, de la DSP2.

4 EL TRATAMIENTO DE LOS DATOS DE PARTES SILENCIOSAS

4.1 Datos de partes silenciosas

45. Una cuestión de protección de datos que requiere una cuidadosa consideración es el tratamiento de los llamados «datos de partes silenciosas». En el contexto de este documento, los datos de partes silenciosas son datos personales relativos a un interesado que no es el usuario de un proveedor de servicios de pago específico, pero cuyos datos personales son tratados por ese proveedor de servicios de pago específico para la ejecución de un contrato entre el proveedor y el usuario de servicios de pago. Este es el caso, por ejemplo, de un usuario de servicios de pago, el interesado A, que utiliza los servicios de un PSIC, y el interesado B ha realizado una serie de operaciones de pago en la cuenta de pago del interesado A. En este caso, el interesado B se considera la «parte silenciosa» y los datos personales (como el número de cuenta del interesado B y la cantidad de dinero que se ha empleado en estas operaciones) relativos al interesado B, se consideran «datos de la parte silenciosa».

4.2 El interés legítimo del responsable del tratamiento

46. El artículo 5, apartado 1, letra b), del RGPD requiere que los datos personales se recojan exclusivamente con fines determinados, explícitos y legítimos, y que no se traten ulteriormente de manera incompatible con dichos fines. Además, el RGPD exige que todo tratamiento de datos personales sea tanto necesario como proporcionado y se ajuste a los principios de protección de datos, como los de limitación de la finalidad y minimización de datos.

47. El RGPD puede permitir el tratamiento de datos de partes silenciosas cuando este tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero [artículo 6, apartado 1, letra f), del RGPD]. Sin embargo, este tratamiento solo puede tener lugar cuando sobre dichos intereses «no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales».

48. Una base jurídica para el tratamiento de datos de partes silenciosas por parte de los PSIC y los PSIP —en el contexto de la prestación de servicios de pago en el marco de la DSP2— podría ser, por tanto, el interés legítimo de un responsable del tratamiento o de un tercero para ejecutar el contrato con el usuario de servicios de pago. La necesidad de tratar los datos personales de la parte silenciosa está limitada y se determina por las expectativas razonables de estos interesados. En el contexto de la prestación de los servicios de pago cubiertos por la DSP2, deben establecerse medidas efectivas y apropiadas para garantizar que no se anulen los intereses o los derechos y libertades fundamentales de las partes silenciosas, y asegurar que se respeten las expectativas razonables de estos interesados respecto al tratamiento de sus datos personales. A este respecto, el responsable del tratamiento (PSIC o PSIP) debe establecer las garantías necesarias para el tratamiento con el fin de proteger los derechos de los interesados. Por ejemplo, puede adoptar medidas técnicas para garantizar que los datos de las partes silenciosas no se traten para un fin distinto del fin para el que los recogieron originalmente los PSIP y los PSIC. Si es posible, también se debe aplicar el cifrado u otras técnicas para lograr un nivel adecuado de seguridad y minimización de los datos.

4.3 Tratamiento ulterior de los datos personales de la parte silenciosa

49. Como se indica en el apartado 29, los datos personales tratados en relación con un servicio de pago regulado por la DSP2 podrían ser objeto de un tratamiento ulterior basado en las obligaciones

legales que recaen sobre el proveedor de servicios. Estas obligaciones legales podrían afectar a los datos personales de la parte silenciosa.

50. Por lo que respecta al tratamiento ulterior de los datos de la parte silenciosa sobre la base del interés legítimo, el CEPD opina que estos datos no pueden utilizarse para un fin distinto de aquel para el que se han recogido los datos personales, salvo sobre la base del Derecho de la Unión o de los Estados miembros. El consentimiento de la parte silenciosa es legalmente inviable, ya que para obtenerlo habría que recoger o tratar datos personales de la parte silenciosa, para lo cual no se puede encontrar ningún fundamento jurídico en virtud del artículo 6 del RGPD. La prueba de compatibilidad del artículo 6, apartado 4, del RGPD tampoco puede ofrecer un fundamento para el tratamiento con otros fines (por ejemplo, actividades de venta directa). Los derechos y libertades de estos interesados silenciosos no se respetarán si el nuevo responsable del tratamiento utiliza los datos personales para otros fines, teniendo en cuenta el contexto en el que se han recogido dichos datos, especialmente la ausencia de relación con los interesados silenciosos[29]; la ausencia de conexión entre cualquier otra finalidad y la finalidad para la que se recogieron inicialmente los datos personales (es decir, el hecho de que los proveedores de servicios de pago solo necesiten los datos de la parte silenciosa para ejecutar un contrato con la otra parte contratante); la naturaleza de los datos personales afectados[30]; la circunstancia de que los interesados no estén en condiciones de esperar razonablemente ningún tratamiento ulterior o de saber siquiera qué responsable del tratamiento puede estar tratando sus datos personales, y dadas las restricciones legales al tratamiento establecidas en el artículo 66, apartado 3, letra g), y en el artículo 67, apartado 2, letra f), de la DSP2.

[29] El considerando 87 de la DSP2 indica que la Directiva se refiere únicamente a las «obligaciones y responsabilidades contractuales entre el usuario de servicios de pago y su proveedor de servicios de pago». Por lo tanto, los datos de las partes silenciosas no entran en el ámbito de aplicación de la DSP2.

[30] Debe tenerse especial cuidado al tratar datos personales de carácter financiero, ya que puede considerarse que el tratamiento aumenta el posible riesgo para los derechos y libertades de las personas, según las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD).

5 EL TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS PERSONALES EN EL MARCO DE LA DSP2

5.1 Categorías especiales de datos personales

51. El artículo 9, apartado 1, del RGPD prohíbe el tratamiento de «datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual u orientación sexual de una persona física».

52. Hay que destacar que en algunos Estados miembros los pagos electrónicos ya están extendidos y que muchas personas los prefieren al efectivo en sus operaciones cotidianas. Al mismo tiempo, las transacciones financieras pueden revelar información sensible sobre un interesado, como las relacionadas con categorías especiales de datos personales. Por ejemplo, dependiendo de los detalles de la transacción, pueden divulgarse las opiniones políticas y las creencias religiosas mediante las donaciones hechas a partidos u organizaciones políticas, iglesias o parroquias. La afiliación sindical puede revelarse por la deducción de una cuota anual de afiliación en la cuenta bancaria de una persona. Los datos personales relativos a la salud pueden obtenerse a partir del análisis de las facturas médicas pagadas por el interesado a un profesional médico (por ejemplo, un psiquiatra). Por último, la información sobre determinadas compras puede revelar datos relativos a la vida sexual o la orientación de una persona. Como muestran estos ejemplos, incluso las operaciones individuales pueden contener categorías especiales de datos personales. Además, los servicios de información sobre cuentas podrían basarse en la elaboración de perfiles, tal como se define en el artículo 4, apartado 4, del RGPD. Como ya se indicó en las Directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679, refrendadas por el CEPD, la elaboración de perfiles «puede crear datos de categoría especial por inferencia a partir de datos que no pertenecen a una categoría especial por derecho propio pero que entran en ella al combinarse con otros datos»[31]. Esto significa que, a través de la suma de las transacciones financieras, se pueden revelar diferentes tipos de modelos de comportamiento, que pueden incluir categorías especiales de datos personales. Por lo tanto, son considerables las posibilidades de que un proveedor de servicios que trate información sobre las transacciones financieras de los interesados también trate categorías especiales de datos personales.

53. Por lo que respecta al término «datos de pago sensibles», el CEPD señala lo siguiente: la definición de datos de pago sensibles recogida en la DSP2 difiere considerablemente de la forma en que el término «datos sensibles» se utiliza comúnmente en el contexto del RGPD y la legislación en materia de protección de datos. Mientras que la DSP2 define los «datos de pago sensibles» como «datos, incluidas las credenciales de seguridad personalizadas, que pueden ser utilizados para cometer un fraude», el RGPD hace hincapié en la necesidad de proteger específicamente las categorías especiales de datos personales que, en virtud del artículo 9 del RGPD, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales[32]. En este sentido, se recomienda al menos trazar y categorizar con precisión qué tipo de datos

[31] Directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles
a los efectos del Reglamento (UE) 2016/679, WP251rev.01, página 16.
[32] Por ejemplo, en el considerando 10 del RGPD, las categorías especiales de datos personales se denominan «datos sensibles».

personales serán objeto de tratamiento. Lo más probable es que se requiera una evaluación de impacto relativa a la protección de datos (EIPD) de acuerdo con el artículo 35 del RGPD, que ayudará en este ejercicio de trazamiento. Se pueden encontrar más orientaciones sobre las EIPD en las Directrices Grupo de Trabajo del Artículo 29 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, refrendado por el CEPD.

5.2 Posibles excepciones

54. La prohibición del artículo 9 del RGPD no es absoluta. En particular, mientras que las excepciones del artículo 9, apartado 2, letras b) a f), y h) a j), del RGPD no son manifiestamente aplicables al tratamiento de datos personales en el contexto de la DSP2, podrían considerarse las dos excepciones siguientes del artículo 9, apartado 2, del RGPD:

a) la prohibición no se aplica si el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados [artículo 9, apartado 2, letra a), del RGPD];

b) la prohibición no se aplica si el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado [artículo 9, apartado 2, letra g), del RGPD].

55. Cabe señalar que la lista de excepciones del artículo 9, apartado 2, del RGPD es exhaustiva. El proveedor de servicios debe reconocer la posibilidad de que se incluyan categorías especiales de datos personales en los datos personales tratados para la prestación de cualquiera de los servicios comprendidos en la DSP2. Dado que la prohibición del artículo 9, apartado 1, del RGPD es aplicable a tales proveedores de servicios, estos deben asegurarse de que les resulte de aplicación una de las excepciones del artículo 9, apartado 2, de dicho Reglamento. Cabe destacar que cuando el proveedor de servicios no puede demostrar que se cumple una de las excepciones, se aplica la prohibición del artículo 9, aparado 1.

5.3 Interés público esencial

56. Los servicios de pago pueden tratar datos personales de categorías especiales por razones de interés público esencial, pero solo cuando se cumplan todas las condiciones del artículo 9, apartado 2, letra g), del RGPD. Esto significa que el tratamiento de las categorías especiales de datos personales tiene que abordarse en una excepción específica al artículo 9, apartado 1, del RGPD en el Derecho de la Unión o de los Estados miembros. Esta disposición tendrá que abordar la proporcionalidad en relación con el objetivo perseguido del tratamiento y contener medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. Además, esta disposición del Derecho de la Unión o de los Estados miembros deberá respetar en lo esencial el derecho a la protección de datos. Por último, también debe demostrarse que el tratamiento de las categorías especiales de datos es necesario por razones de un interés público esencial, incluidos los intereses de importancia sistémica. Solo cuando se cumplan todas estas condiciones, esta excepción podría aplicarse a determinados tipos de servicios de pago.

5.4 Consentimiento explícito

57. En los casos en los que no se aplica la excepción del artículo 9, apartado 2, letra g), del RGPD, la obtención del consentimiento explícito de acuerdo con las condiciones para el consentimiento válido del RGPD, parece seguir siendo la única excepción legal posible para el tratamiento de categorías especiales de datos personales por parte de proveedores terceros. En las Directrices 5/2020 del CEPD sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 se establece[33] que «[e]l artículo 9, apartado 2, no reconoce la circunstancia de "necesario para la ejecución de un contrato" como una excepción a la prohibición general de tratar categorías especiales de datos. Por lo tanto, los responsables y los Estados miembros que aborden esta situación deben estudiar las excepciones específicas que figuran en el artículo 9, apartado 2, letras b) a j)». Cuando los proveedores de servicios se basan en el artículo 9, apartado 2, letra a) del RGPD, deben asegurarse de que se les ha concedido el consentimiento explícito antes de comenzar el tratamiento. El consentimiento explícito establecido en el artículo 9, apartado 2, letra a), del RGPD debe cumplir todos los requisitos de dicho Reglamento.

5.5 No se aplican excepciones adecuadas

58. Como se ha señalado anteriormente, cuando el proveedor de servicios no puede demostrar que se cumple una de las excepciones, se aplica la prohibición del artículo 9, aparado 1. En este caso, podrían establecerse medidas técnicas para evitar el tratamiento de categorías especiales de datos personales; por ejemplo, se puede impedir el tratamiento de determinados puntos de datos. A este respecto, los proveedores de servicios de pago pueden explorar las posibilidades técnicas para excluir categorías especiales de datos personales y permitir un acceso seleccionado que impida el tratamiento de categorías especiales de datos personales relacionados con partes silenciosas por parte de proveedores terceros.

[33] Directrices 5/2020 del CEPD sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, apartado 99.

6 MINIMIZACIÓN DE DATOS, SEGURIDAD, TRANSPARENCIA, RESPONSABILIDAD PROACTIVA Y ELABORACIÓN DE PERFILES

6.1 Minimización de datos y protección de datos desde el diseño y por defecto

59. El principio de minimización de datos está consagrado en el artículo 5, apartado 1, letra c), del RGPD: «Los datos personales serán [...] adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados». Esencialmente, según el principio de minimización de datos, los responsables del tratamiento no deben tratar más datos personales que los necesarios para lograr el propósito específico en cuestión. Como se ha señalado en el capítulo 2, la cantidad y el tipo de datos personales necesarios para prestar el servicio de pago vienen determinados por el objetivo y la finalidad tal como la entienden las dos partes del contrato[34]. La minimización de datos es aplicable a todo tratamiento (por ejemplo, a toda recogida o acceso y solicitud de datos personales). Las Directrices 4/2019 del CEPD sobre el artículo 25 relativo a la protección de datos desde el diseño y por defecto establecen que los encargados del tratamiento y los proveedores de tecnología también reconocidos como actores clave para la protección de datos desde el diseño y por defecto, deben asimismo ser conscientes de que los responsables del tratamiento están obligados a tratar los datos personales únicamente con sistemas y tecnologías que incorporan mecanismos de protección de datos[35].

60. El artículo 25 del RGPD contempla las obligaciones de aplicar la protección de datos desde el diseño y por defecto. Estas obligaciones son de especial importancia para el principio de minimización de datos. Este artículo determina que el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, concebidas para aplicar de forma efectiva los principios de protección de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta 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. Estas medidas pueden incluir el cifrado, la seudonimización y otras medidas técnicas.

61. Cuando se aplica la obligación del artículo 25 del RGPD, los elementos que deben tenerse en cuenta son el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. Se ofrecen más aclaraciones sobre esta obligación en las citadas Directrices 4/2019 del CEPD sobre el artículo 25 en relación con la protección de datos desde el diseño y por defecto.

6.2 Medidas de minimización de datos

62. El proveedor tercero que acceda a los datos de la cuenta de pago para prestar los servicios solicitados debe tener en cuenta también el principio de minimización de datos y solo debe recoger los datos personales necesarios para prestar los servicios de pago específicos solicitados por el usuario del servicio de pago. Como principio, el acceso a los datos personales debe limitarse a lo

[34] 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, CEPD, apartado 32.
[35] *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (Directrices 4/2019 sobre la protección de datos desde el diseño y por defecto del artículo 25), página 29.

necesario para la prestación de los servicios de pago. Como se ha mostrado en el capítulo 2, la DSP2 exige a los PSPGC que compartan la información del usuario de servicios de pago a petición de dicho usuario, cuando este desee utilizar un servicio de iniciación de pagos o un servicio de información sobre cuentas.

63. Cuando no todos los datos de las cuentas de pago sean necesarios para la ejecución del contrato, el PSIC deberá realizar una selección de las categorías de datos pertinentes antes de recoger los datos. Por ejemplo, las categorías de datos que pueden no resultar necesarias podrían incluir la identidad de la parte silenciosa y las características de la operación. Además, a menos que lo exija el Derecho de los Estados miembros o de la Unión, no es necesario mostrar el IBAN de la cuenta bancaria de la parte silenciosa.

64. A este respecto, podría considerarse la posible aplicación de medidas técnicas que permitan o apoyen a los proveedores terceros en la limitación de su obligación de acceso y recuperación únicamente a los datos personales necesarios para la prestación de sus servicios, como parte de la aplicación de las oportunas políticas de protección de datos, en consonancia con el artículo 24, apartado 2, del RGPD. A este respecto, el CEPD recomienda el uso de herramientas digitales para apoyar a los PSIC en su obligación de recoger únicamente los datos personales necesarios en relación con los fines para los que son tratados. Por ejemplo, cuando un proveedor de servicios no necesita las características de la operación (en el campo de descripción de los registros de la operación) para prestar su servicio, una herramienta de selección digital podría funcionar como un medio para que los proveedores terceros excluyan este campo de las operaciones generales de tratamiento por su parte.

Ejemplo 2:

HappyPayments, nuestro proveedor de servicios de información de cuentas del ejemplo 1, quiere asegurarse de que únicamente trata los datos personales de las cuentas de pago que interesan a sus usuarios. No es necesario solicitar acceso a más datos de cuentas de pago de cara a prestar el servicio. Por lo tanto, permite a los usuarios seleccionar los tipos específicos de información que les interesan.

El usuario A quiere acceder a una visión general de sus gastos de los últimos dos meses. Así, solicita sus dos cuentas bancarias, mantenidas en dos PSPGC diferentes, la información de todas las operaciones de los dos últimos meses, el importe de la operación, la fecha de ejecución y el nombre del destinatario, y marca las casillas correspondientes en la interfaz de usuario de HappyPayments.

HappyPayments comienza entonces a solicitar a los respectivos PSPGC únicamente la información correspondiente a los campos establecidos por el usuario A y solo para el período de los dos últimos meses. No se solicitan datos como la «comunicación» de la operación o incluso el IBAN, ya que el usuario A no solicitó esta información.

A fin de que HappyPayments pueda cumplir con sus obligaciones de minimización de datos, los PSPGC permiten a HappyPayments solicitar campos específicos para un rango de fechas.

65. A este respecto, cabe señalar también que, con arreglo a la DSP2, los PSPGC solo pueden proporcionar acceso a la información de las cuentas de pago. No existe ninguna base jurídica en virtud de la DSP2 para facilitar el acceso con respecto a los datos personales contenidos en otras cuentas, como las de ahorro, las hipotecarias o las de inversión. En consecuencia, con arreglo a la DSP2, deben aplicarse medidas técnicas para garantizar que el acceso se limite a la información necesaria de las cuentas de pago.

66. Además de recoger la menor cantidad de datos posible, el proveedor de servicios también tiene que aplicar períodos de retención limitados. El proveedor de servicios no debe conservar los datos personales durante un periodo superior al necesario en relación con los fines solicitados por el usuario del servicio de pago.

67. Si el contrato entre el interesado y el PSIC requiere la transmisión de datos personales a terceros, solo podrán transmitirse aquellos datos personales que sean necesarios para la ejecución del contrato. También se debe informar a los interesados específicamente sobre la transmisión y los datos personales que se van a transmitir a este tercero.

6.3 Seguridad

68. El CEPD ya destacó que la violación de la seguridad de los datos personales financieros «implica claramente graves repercusiones en la vida cotidiana del interesado» y cita como ejemplo los riesgos de fraude en los pagos[36].

69. Cuando una violación de la seguridad de los datos afecta a datos financieros, el interesado puede estar expuesto a riesgos considerables. En función de la información que se filtre, los interesados pueden estar expuestos a un riesgo de robo de identidad, de robo de los fondos de sus cuentas y de otros activos. Además, existe la posibilidad de que la exposición de los datos de las operaciones esté relacionada con considerables riesgos para la intimidad, ya que estos datos pueden contener referencias a todos los aspectos de la vida privada del interesado. Al mismo tiempo, los datos financieros son obviamente valiosos para los delincuentes y, por tanto, un objetivo atractivo.

70. Como responsables del tratamiento, los proveedores de servicios de pago están obligados a adoptar medidas adecuadas para proteger los datos personales de los interesados (artículo 24, apartado 1, del RGPD). Cuanto mayores sean los riesgos asociados a la actividad de tratamiento llevada a cabo por el responsable del tratamiento, más estrictas serán las normas de seguridad que deben aplicarse. Dado que el tratamiento de datos financieros está relacionado con una serie de graves riesgos, las medidas de seguridad deben ser consecuentemente elevadas.

71. Los proveedores de servicios deben estar sujetos a normas estrictas, como por ejemplo mecanismos de autenticación reforzada de cliente y altos estándares de seguridad para el equipo técnico[37]. También son importantes otros procedimientos, como la verificación de las normas de seguridad de los encargados del tratamiento y la aplicación de procedimientos contra el acceso no autorizado.

6.4 Transparencia y responsabilidad proactiva

72. La transparencia y la responsabilidad proactiva son dos principios fundamentales del RGPD.

73. Por lo que respecta a la transparencia [artículo 5, apartado 1, letra a), del RGPD], el artículo 12 del RGPD especifica que los responsables del tratamiento tomarán las medidas oportunas para facilitar toda información indicada en los artículos 13 y 14 del RGPD. Además, exige que la información o comunicación sobre el tratamiento de datos personales sea concisa, transparente, inteligible y de fácil acceso. La información será facilitada con un lenguaje claro y sencillo y por escrito o «por otros medios, inclusive, si procede, por medios electrónicos». Las Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679 del Grupo de Trabajo del Artículo 29,

[36] Directrices del Grupo de Trabajo del Artículo 29 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 (WP248 rev.01, refrendadas por el CEPD.
[37] Véanse las NTR.

refrendadas por el CEPD, ofrecen orientaciones específicas para el cumplimiento del principio de transparencia en los entornos digitales.

74. De acuerdo con las citadas Directrices, el artículo 11 del RGPD debe interpretarse como una manera de imponer una auténtica minimización de datos pero sin impedir el ejercicio de los derechos de los interesados, y que el ejercicio de estos derechos debe ser posible con ayuda de información adicional facilitada por el interesado. Puede haber situaciones en las que un responsable del tratamiento trate datos personales que no requieran la identificación de un interesado (por ejemplo, con datos anonimizados). En estos casos, el artículo 11, apartado 1, también puede resultar pertinente, ya que establece que el responsable del tratamiento no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el RGPD.

75. Con respecto a los servicios en el marco de la DSP2, el artículo 13 del RGPD es aplicable a los datos personales recogidos del interesado y el artículo 14 resulta de aplicación cuando los datos personales no se han obtenido del interesado.

76. En particular, el interesado debe ser informado sobre el período de conservación de los datos personales o, si no es posible, los criterios utilizados para determinar dicho período y, en su caso, los intereses legítimos perseguidos por el responsable del tratamiento o por un posible tercero. Cuando el tratamiento se base en el consentimiento a que se refiere el artículo 6, apartado 1, letra a), del RGPD o en el consentimiento explícito a que se refiere el artículo 9, apartado 2, letra a), del RGPD, el interesado deberá ser informado de la existencia del derecho a retirar el consentimiento en cualquier momento.

77. El responsable del tratamiento facilitará la información al interesado, teniendo en cuenta las circunstancias específicas en las que se traten dichos datos. Si los datos personales han de utilizarse para comunicación con el interesado[38], lo que probablemente será el caso de los PSIC, la información debe facilitarse a más tardar en el momento de la primera comunicación a dicho interesado. Si los datos personales se van a comunicar a otro destinatario, la información debe facilitarse, a más tardar, en el momento de la primera comunicación de los datos personales.

78. Por lo que respecta a los servicios de pago en línea, las citadas Directrices aclaran que los responsables del tratamiento pueden seguir un enfoque en niveles cuando opten por utilizar una combinación de métodos para garantizar la transparencia. En particular, se recomienda que se utilicen declaraciones/avisos de privacidad estructurados en niveles para enlazar con las distintas categorías de información que se debe facilitar al interesado, en lugar de mostrar toda esta información en un solo aviso en pantalla, a fin de evitar la fatiga informativa y al mismo tiempo garantizar la eficacia de la información.

79. Las citadas Directrices también aclaran que los responsables del tratamiento también pueden optar por utilizar herramientas de transparencia adicionales para proporcionar información al interesado, como ventanillas de privacidad. Una ventanilla de privacidad es un punto único desde el cual los interesados pueden consultar la «información de privacidad» y administrar sus preferencias de privacidad permitiendo o impidiendo que el responsable del tratamiento de datos en cuestión utilice sus datos de determinadas maneras[39]. Una ventanilla de privacidad podría

[38] Artículo 14, apartado 3, letra b), del RGPD.

[39] De conformidad con las Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679 del Grupo de Trabajo del Artículo 29, refrendadas por el CEPD, las ventanillas de privacidad son especialmente útiles cuando

proporcionar una visión general de los proveedores terceros que han obtenido el consentimiento explícito de los interesados, y también podría ofrecer información relevante sobre la naturaleza y la cantidad de datos personales a los que han accedido dichos proveedores. En principio, un PSPGC puede ofrecer al usuario la posibilidad de retirar un consentimiento explícito específico conforme a la DSP2[40] a través de la visión general, lo que daría lugar a una denegación de acceso a sus cuentas de pago a uno o varios proveedores terceros. El usuario también podría solicitar a un PSPGC que deniegue el acceso a su(s) cuenta(s) de pago a uno o varios proveedores terceros concretos[41], ya que el usuario tiene derecho a (no) hacer uso de un servicio de información sobre cuentas. Si las ventanillas de privacidad se utilizan para dar o retirar un consentimiento explícito, deben diseñarse y aplicarse de forma legal y, en particular, evitar la creación de obstáculos al derecho de los proveedores terceros a prestar servicios de conformidad con la DSP2. A este respecto, y de conformidad con las disposiciones aplicables en virtud de la DSP2, un proveedor tercero puede volver a obtener el consentimiento explícito del usuario después de que este haya sido retirado.

80. El principio de responsabilidad proactiva exige que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas, a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, en particular con los principales principios de protección de datos previstos en su artículo 5, apartado 1. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas, y se deben revisar y actualizar cuando sea necesario[42].

6.5 Elaboración de perfiles

81. El tratamiento de datos personales por parte de los proveedores de servicios de pago puede implicar la elaboración de perfiles, tal como se menciona en el artículo 4, apartado 4, del RGPD. Por ejemplo, los PSIC podrían recurrir al tratamiento automatizado de datos personales para evaluar determinados aspectos personales relacionados con una persona física. Podría evaluarse la situación económica personal del interesado, en función de las características del servicio. Los servicios de información sobre cuentas, que se prestan a petición de los usuarios, pueden implicar una amplia evaluación de los datos personales de las cuentas de pago.

82. El responsable del tratamiento también tiene que ser transparente con el interesado sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles. En estos casos, el responsable del tratamiento tiene que proporcionar información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado [artículo 13, apartado 2, letra f), y artículo 14, apartado 2, letra g), y considerando 60][43]. Asimismo, en virtud del artículo 15 del RGPD, el interesado tiene derecho a solicitar y obtener información del responsable del tratamiento sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles, la lógica aplicada y las consecuencias para el interesado y, en

los interesados utilizan un mismo servicio en varios dispositivos distintos, ya que les da acceso y control a sus datos personales independientemente de la forma en que usen el servicio. Permitir que los interesados ajusten manualmente su configuración de privacidad a través de una ventanilla de privacidad también hace más fácil personalizar una declaración/aviso de privacidad al reflejar únicamente los tipos de tratamiento que se llevan a cabo para ese interesado en concreto.

[40] Véase, por ejemplo, el «consentimiento explícito» mencionado en el artículo 67, apartado 2, de la DSP2.

[41] Véase también EBA/OP/2020/10, apartado 45.

[42] Artículo 5, apartado 2, y artículo 24, del RGPD.

[43] Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, WP 260 rev.01, refrendadas por el CEPD

determinadas circunstancias, el derecho a oponerse a la elaboración de perfiles, independientemente de que las decisiones automatizadas se basen en la elaboración de perfiles[44].

83. Asimismo, lo que también es relevante en este contexto es el derecho del interesado a no ser objeto de una decisión que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar que se establece en el artículo 22 del RGPD. Esta norma también incluye, en determinadas circunstancias, la necesidad de que los responsables del tratamiento apliquen medidas adecuadas para salvaguardar los derechos del interesado, como la información específica al interesado, el derecho a obtener intervención humana en la toma de decisiones y a expresar su punto de vista y a impugnar la decisión. Como también se indica en el considerando 71 del RGPD, esto significa, entre otras cosas, que los interesados tienen derecho a no ser objeto de una decisión, como la denegación automática de una solicitud de crédito en línea sin ninguna intervención humana[45].

84. Las decisiones automatizadas, incluida la elaboración de perfiles que implican categorías especiales de datos personales, solo se permiten en las condiciones contempladas en el artículo 22, apartado 4, del RGPD:

- hay una exención aplicable del artículo 22, apartado 2;
- y se aplica el artículo 9, apartado 2, letras a) o g), del RGPD. En ambos casos, el responsable del tratamiento establecerá asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado[46].

85. También deben observarse los requisitos para el tratamiento ulterior, tal como se indica en las presentes Directrices. Las aclaraciones e instrucciones sobre las decisiones individuales automatizadas y la elaboración de perfiles recogidas en las Directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679, refrendadas por el CEPD, son plenamente pertinentes en el contexto de los servicios de pago y, por tanto, deben tenerse debidamente en cuenta.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)

[44] Directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, WP251rev.01

[45] Considerando 71 del RGPD.

[46] Directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679, WP251rev.01 la página 25.