COMISIÓN
EUROPEA

Bruselas, 29.5.2019
COM(2019) 250 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea

Contenido

La Comisión publica el presente documento con fines exclusivamente informativos. No contiene ninguna interpretación autorizada del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea y no constituye un decisión o posición de la Comisión Europea. La interpretación de dicho Reglamento con arreglo a los Tratados de la Unión se entiende sin perjuicio de cualquier decisión o posición de la Comisión y de las competencias del Tribunal de Justicia de la Unión Europea.

1 Introducción

En una economía cada vez más basada en los datos, la circulación de los mismos es esencial para las actividades comerciales de las empresas de todos los tamaños y sectores. El desarrollo de nuevas tecnologías digitales ofrece nuevas oportunidades para los ciudadanos, las empresas y las administraciones públicas en la Unión Europea (la «UE»).

Para aumentar aún más el intercambio transfronterizo de datos e impulsar la economía de los datos, en noviembre de 2018, el Parlamento Europeo y el Consejo adoptaron el Reglamento (UE) 2018/1807, relativo a un marco para la libre circulación de datos no personales en la Unión Europea[1] (el «Reglamento sobre la libre circulación de datos no personales»), a partir de una propuesta de la Comisión Europea (la «Comisión»). El Reglamento es aplicable a partir del 28 de mayo de 2019. El principio de libre circulación de datos personales se recoge en el Reglamento (UE) 2016/679 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 (el «Reglamento general de protección de datos»)[2]. Así pues, ahora existe un marco integral para un espacio de datos europeo común y la libre circulación de todos los datos dentro de la Unión Europea[3].

El Reglamento de libre circulación de datos no personales proporciona seguridad jurídica para que las empresas procesen sus datos en cualquier punto de la UE, aumenta la confianza en los servicios de tratamiento de datos y contrarresta las prácticas de dependencia de un solo proveedor. De esta forma, el cliente tendrá más donde elegir, se mejorará la eficiencia y se estimulará la adopción de tecnologías en la nube, lo que generará ahorros significativos para las empresas en la UE. Un estudio demuestra que las empresas de la UE pueden ahorrar entre el 20 -50 % de sus costes en TI al migrar a la nube[4].

Gracias a estos dos Reglamentos, los datos pueden circular libremente entre los Estados miembros, lo que permite a los usuarios de servicios de tratamiento de datos utilizar los datos recopilados en diferentes mercados de la UE para mejorar su productividad y competitividad. Por lo tanto, los usuarios pueden aprovechar al máximo las economías de escala proporcionadas por el gran mercado de la UE, mejorando su competitividad global y aumentando la interconexión de la economía de los datos europea.

El Reglamento de libre circulación de datos no personales tiene tres características notables:

---

1 Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea (DO L 303 de 28.11.2018, p. 59).

2 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (DO L 119 de 4.5.2016, p. 1).

3 El Reglamento general de protección de datos se aplica igualmente en el Espacio Económico Europeo (EEE), que incluye Islandia, Liechtenstein y Noruega. Además, el Reglamento de libre circulación de datos no personales se considera pertinente a efectos del EEE.

4 Deloitte: *Measuring the economic impact of cloud computing in Europe*, SMART 2014/0031, 2016. Disponible en línea (en inglés) en: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

- Por norma, prohíbe a los Estados miembros imponer requisitos sobre dónde deben localizarse los datos. Las excepciones a esta regla solo pueden justificarse por razones de seguridad pública de conformidad con el principio de proporcionalidad.
- Establece un mecanismo de cooperación para garantizar que las autoridades competentes puedan seguir ejerciendo los derechos que tienen para acceder a los datos que se están tratando en otro Estado miembro.
- Proporciona incentivos para que el sector, con el apoyo de la Comisión, elabore códigos de conducta autorreguladores sobre el cambio de proveedores de servicios y la transferencia de datos.

Objetivo de este documento orientativo

El presente documento de orientación cumple lo establecido en el artículo 8, apartado 3, del Reglamento de libre circulación de datos no personales, que exige que la Comisión publique orientaciones sobre la interacción entre este Reglamento y el Reglamento general de protección de datos, «en particular en lo que se refiere a los conjuntos de datos compuestos tanto por datos personales como no personales».

Esta orientación pretende ayudar a los usuarios, especialmente a las pequeñas y medianas empresas, a comprender la interacción entre el Reglamento de libre circulación de datos no personales y el Reglamento general de protección de datos[5]. Por lo tanto, el documento de orientación aborda particularmente: i) los conceptos de datos no personales y datos personales; ii) los principios de libre circulación de datos y la prohibición de los requisitos de localización de datos en virtud de ambos Reglamentos; y iii) la noción de portabilidad de datos dentro del Reglamento de libre circulación de datos no personales. También cubre los requisitos de autorregulación establecidos en ambos Reglamentos.

El Reglamento de libre circulación de datos no personales solo cubre los «datos que no sean datos personales», de acuerdo con la definición del Reglamento general de protección de datos. El Reglamento general de protección de datos regula el tratamiento de datos personales, que es una parte esencial del marco de protección de datos de la UE[6]. Entró en vigor en los

[5] Considerando 37 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

[6]
– Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (DO L 119 de 4.5.2016, p. 1).
– Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).
– Directiva (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre

Estados miembros el 25 de mayo de 2018. El Reglamento establece normas armonizadas para proteger a los ciudadanos en la UE/EEE en relación con el tratamiento de sus datos personales y la libre circulación de los mismos. El Reglamento general de protección de datos: i) especifica qué tipo de información se considera como datos personales; ii) establece fundamentos jurídicos para su tratamiento; y iii) define los derechos y obligaciones que deben observarse al procesar estos datos[7], entre otras disposiciones. Con respecto al principio de libre circulación de datos personales, el artículo 1, apartado 3, del Reglamento general de protección de datos dispone que «la libre circulación de datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales».

En la mayoría de las situaciones cotidianas, los conjuntos de datos suelen estar compuestos tanto por datos personales como no personales. Esto a menudo se conoce como «conjunto de datos mixtos». La sección 2.2 a continuación explica con más detalle la interacción entre el Reglamento de libre circulación de datos no personales y el Reglamento general de protección de datos con respecto a los conjuntos de datos mixtos.

En aras de la claridad, no existen obligaciones contradictorias en virtud del Reglamento general de protección de datos y el Reglamento de libre circulación de datos no personales.

---

circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, (DO L 119 de 4.5.2016, p. 89).

– 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) [pendiente de revisión].

7 Para obtener más orientación sobre diversos aspectos 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 (Reglamento general de protección de datos) y la Ley europea de protección de datos, consulte la página web del Comité Europeo de Protección de Datos, que ha publicado una serie de directrices de conformidad con el artículo 70 del Reglamento general de protección de datos, disponible en: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_es. En esta misma página web se incluyen referencias a directrices, recomendaciones y otros documentos publicados por el predecesor del Comité Europeo de Protección de Datos (Grupo de Trabajo del artículo 29). Además, para sensibilizar a los ciudadanos y las empresas sobre el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), la Comisión emitió una Comunicación sobre protección de datos: Orientaciones sobre la aplicación directa del RGPD (COM/2018/043 final) disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0043

2 La interacción entre el Reglamento de libre circulación de datos no personales y el Reglamento general de protección de datos: conjuntos de datos mixtos

2.1 El concepto de datos no personales en el Reglamento de libre circulación de datos no personales

El Reglamento de libre circulación de datos no personales[8] tiene como objetivo garantizar la libre circulación de datos que no tengan carácter personal. A lo largo de su texto, el Reglamento utiliza el término «datos», que debe entenderse como «los datos que no sean datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679 [Reglamento general de protección de datos]» [9]. Dichos datos, también denominados «**datos no personales**» en el presente documento, se definen por oposición (*a contrario*) a los datos personales, según se establece en el Reglamento general de protección de datos.

Datos personales

A efectos del Reglamento general de protección de datos se entenderá por: «"Datos personales" toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos 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 física».

Que la definición de datos personales sea tan amplia es intencional, manteniéndose prácticamente sin cambios en el Reglamento general de protección de datos, en comparación con la legislación anterior[10]. Varios aspectos de la definición de datos personales, como «toda información», «sobre», «identificada o identificable», fueron tratados previamente por el Grupo de Trabajo del artículo 29[11] en su Dictamen 4/2007 sobre el concepto de datos personales, de 20 de junio de 2007, WP 136.

---

8 Artículo 1 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

9 Véase el artículo 3, apartado 1, del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 2018/1807, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

10 Véase el artículo 2, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (fecha de fin de vigencia: 24 de mayo de 2018, derogada por el Reglamento general de protección de datos). Véase también la jurisprudencia del Tribunal de Justicia sobre la definición de datos personales, que reconoce la amplia interpretación de dicha noción, por ejemplo, sentencia del Tribunal de Justicia de 29 de enero de 2009, *Productores de Música de España (Promusicae)*/*Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; sentencia del Tribunal de Justicia (Sala Tercera) de 24 de noviembre de 2011, *Scarlet Extended SA*/*Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; sentencia del Tribunal de Justicia de 19 de octubre de 2016, *Patrick Breyer*/*Bundersrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

11 El Grupo de Trabajo del artículo 29 era un órgano consultivo que proporcionaba asesoramiento a la Comisión sobre cuestiones de protección de datos y que ayudaba a desarrollar políticas armonizadas de

La seudonimización de los datos personales es una práctica común en ámbitos como la investigación, a fin de ocultar la identidad de una persona. La **seudonimización** consiste en el tratamiento de datos personales de manera tal que ya no puedan atribuirse a una persona específica sin utilizar información adicional. Esta información adicional figura por separado y está sujeta a medidas organizativas o técnicas (por ejemplo, el cifrado)[12,13]. No obstante, los datos que han sido seudonimizados se consideran información sobre una persona identificable si pueden atribuirse a esta persona mediante el uso de información adicional[14]. Dichos datos **constituyen datos personales** de conformidad con el Reglamento general de protección de datos.

Datos no personales

Cuando los datos no son «datos personales» tal como se definen en el Reglamento general de protección de datos, se entiende que son **no personales**. Los datos no personales se pueden clasificar por origen como:

- Primero: datos que originalmente no se relacionaban con una persona física identificada o identificable, como los datos sobre las condiciones climáticas generados por los sensores instalados en aerogeneradores o los datos sobre las necesidades de mantenimiento de las máquinas industriales.

- Segundo: datos que inicialmente eran datos personales, pero más tarde se convirtieron en **anónimos**[15]. La «anonimización» de los datos personales es diferente a la seudonimización (véase más arriba), ya que los datos debidamente anonimizados no

protección de datos en la UE. Tras la entrada en vigor del Reglamento general de protección de datos, el 25 de mayo de 2018, el Comité de Protección de Datos Europeo sucedió al Grupo de Trabajo del artículo 29.

12 Véase el artículo 4, apartado 5, 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 (Reglamento general de protección de datos) que define la «seudonimización».

13 Por ejemplo, un estudio de investigación sobre los efectos de un nuevo medicamento entraría dentro del concepto de seudonimización si los datos personales de los participantes de dicho estudio se reemplazaran por atributos únicos (por ejemplo, número o código) en la documentación de la investigación y sus datos personales figuraran por separado con los atributos únicos asignados en un documento seguro (por ejemplo, en una base de datos protegida por contraseña).

14 Véase el considerando 26 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 (Reglamento general de protección de datos).

15 Véase el considerando 26 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y sobre la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que establece que «…los principios la protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo».

pueden atribuirse a una persona específica, ni siquiera mediante el uso de datos adicionales[16] y, por lo tanto, son datos no personales.

La evaluación de si los datos están correctamente anonimizados depende de las circunstancias específicas y únicas de cada caso individual[17]. Varios ejemplos de reidentificación de conjuntos de datos que supuestamente fueron anonimizados han demostrado que tal evaluación puede ser complicada[18]. Para establecer si un individuo es identificable, uno debe buscar todos los medios razonablemente susceptibles de ser utilizados por el responsable del tratamiento o por otra persona para identificar un individuo directa o indirectamente[19].

Ejemplos de datos no personales

- Los datos que se agregan en la medida en que los eventos individuales (como los viajes a título particular de una persona al extranjero o los patrones de viaje que podrían constituir datos personales) ya no son identificables, se pueden calificar como datos anónimos[20]. Los datos anónimos se utilizan, por ejemplo, en estadísticas o en informes de ventas (por ejemplo, para evaluar la popularidad de un producto y sus características).
- Datos comerciales de alta frecuencia en el sector financiero, o datos sobre agricultura de precisión que ayudan a controlar y optimizar el uso de pesticidas, nutrientes y agua.

16 Véase la sentencia del Tribunal de Justicia, de 19 de enero de 2016, *Patrick Breyer* /*Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779. El Tribunal de Justicia sostuvo que la dirección del protocolo de Internet (IP) dinámica puede constituir datos personales incluso si un tercero (por ejemplo, un proveedor de servicios de Internet) está en posesión de datos adicionales, lo que permitiría identificar a la persona. La posibilidad de identificar a la persona debe constituir un medio que puede ser razonablemente utilizado para identificar a la persona, ya sea directa o indirectamente.

17 La anonimización de datos siempre debe realizarse utilizando técnicas de anonimización de última generación.

18 Para ver ejemplos de reidentificación de datos supuestamente anonimizados, consúltese el estudio sobre circulación de datos futuros realizado para el comité ITRE del Parlamento Europeo por Blackman, C., Forge, S .: *Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee*, 2017, p. 22, Box 2. Disponible en línea (en inglés) en: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

19 Véase el considerando 26 del Reglamento (UE) 2016/679, el Reglamento general de protección de datos, en virtud del cual «Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos».

20 Véase el Grupo de Trabajo del artículo 29: *Dictamen 05/2014 sobre técnicas de anonimización*, adoptado el 10 de abril de 2014, WP216, p. 9: «Tan solo si el responsable del tratamiento agrega los datos a un nivel en el que los eventos individuales dejan de ser identificables, el conjunto de datos resultantes puede calificarse de anónimo. Por ejemplo: Por ejemplo, si una organización recoge datos sobre los desplazamientos de personas, los patrones de viaje individuales a nivel de evento seguirían considerándose datos personales para cualquier parte mientras el responsable del tratamiento (o cualquier otra parte) siga teniendo acceso a los datos originales no tratados, aun en el caso de que se hayan eliminado los identificadores directos del conjunto entregado a terceros. Por el contrario, si el responsable del tratamiento borra los datos no tratados y entrega únicamente estadísticas agregadas a terceros a un nivel general (por ejemplo, "los lunes, en el trayecto X, hay un 160 % más de pasajeros que los martes"), entonces estaríamos hablando de datos anónimos».

Sin embargo, si los datos no personales pueden relacionarse con una persona de alguna manera, haciendo que sean identificables directa o indirectamente, los datos deben considerarse datos personales.

Por ejemplo, si un informe de control de calidad en una línea de producción permite relacionar los datos con ciertos operarios en particular (por ejemplo, aquellos que establecen los parámetros de producción), dichos datos se considerarían en consecuencia datos personales y ha de aplicarse el Reglamento general de protección de datos. Se aplicarán las mismas reglas cuando la evolución de la tecnología y los análisis de datos haga posible convertir datos anónimos en datos personales. [21]

En tanto que la definición de datos personales hace referencia a «personas físicas», los conjuntos de datos que contienen los nombres y los datos de contacto de personas jurídicas se consideran, en principio, datos no personales[22]. Sin embargo, en determinadas situaciones pueden ser datos personales[23]. Este será el caso si, por ejemplo, el nombre de la persona jurídica es el mismo que el de una persona física que lo posee o si la información se relaciona con una persona física identificada o identificable[24].

2.2 Conjuntos de datos mixtos

El Reglamento de libre circulación de datos no personales y el Reglamento general de protección de datos abordan la libre circulación de datos en la UE desde dos ángulos diferentes.

El Reglamento de libre circulación de datos no personales establece una prohibición general de los requisitos de localización de datos para datos no personales. El artículo 4, apartado 1, de dicho Reglamento prohíbe los requisitos de localización de datos a menos que estén

---

21 Si los datos personales se tratan de forma ilícita o si su tratamiento infringe el Reglamento general de protección de datos, los interesados (personas físicas) tienen derecho, en virtud del Reglamento general de protección de datos, a presentar una reclamación ante una autoridad nacional de supervisión (autoridad de protección de datos) en la UE, así como a una tutela judicial efectiva ante un tribunal nacional. Las funciones, competencias y poderes de las autoridades nacionales de control están reguladas en el capítulo VI, sección 2, del Reglamento general de protección de datos.

22 El considerando 14 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 (Reglamento general de protección de datos) establece que «[e]l presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto». Sin embargo, esto debe leerse a la luz de la definición de datos personales del artículo 4, apartado 1, del Reglamento general de protección de datos.

23 Véase la sentencia del Tribunal de Justicia de 9 de noviembre de 2010 en los casos conjuntos *Volker und Markus Schecke GbR*, C-92/09 y *Hartmut Eifert*, C-93/09/*Land Hessen*, ECLI:EU:C:2010:662, apartado 52.

24 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_es

justificados por razones de seguridad pública en cumplimiento del principio de proporcionalidad.

El Reglamento general de protección de datos, además de garantizar un alto nivel de protección de datos personales, garantiza la libre circulación de datos personales. De conformidad con el artículo 1, apartado 3, del Reglamento, la libre circulación de datos personales «no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales». Juntos, ambos Reglamentos contemplan la libre circulación de «todos» los datos en el territorio de la UE. Las disposiciones específicas se tratan más a fondo en las secciones 3.1 y 3.2.

Un conjunto de datos mixtos consta de datos personales y no personales. Los conjuntos de datos mixtos representan la mayoría de los conjuntos de datos utilizados en la economía de datos y son comunes debido a desarrollos tecnológicos como el Internet de las cosas (es decir, objetos que se conectan digitalmente), la inteligencia artificial y las tecnologías que permiten el análisis de macrodatos.

Ejemplos de conjuntos de datos mixtos

- el registro fiscal de una empresa, que mencione el nombre y número de teléfono del director general de la empresa;
- conjuntos de datos bancarios, particularmente aquellos con información de clientes y detalles de transacciones, como servicios de pago (tarjetas de crédito y débito), aplicaciones de gestión de relaciones con socios (PRM) y acuerdos de préstamo, documentos que combinan datos relativos a personas físicas y jurídicas;
- los datos estadísticos anonimizados de una institución de investigación y los datos sin tratar recopilados inicialmente, como las respuestas individuales de los encuestados a las preguntas de una encuesta estadística;
- una base de datos de conocimientos de una empresa en cuanto a problemas de TI y sus soluciones basadas en informes de cada uno de los incidentes de TI;
- datos relacionados con el Internet de las cosas, donde algunos de los datos permitan hacer suposiciones sobre personas identificables (por ejemplo, presencia en una dirección particular y patrones de uso); y
- análisis de los datos de registro operacional de los equipos de fabricación en la industria manufacturera.

Ejemplo: servicios de administración de relaciones con los clientes

Algunos bancos utilizan los servicios de administración de relaciones con clientes (CRM, por sus siglas en inglés) proporcionados por terceros que requieren que los datos de un cliente estén disponibles en el entorno de la CRM. Los datos almacenados en el servicio de la CRM incluirán toda la información necesaria para gestionar eficazmente la interacción con el cliente, como su dirección postal y de correo electrónico, su número de teléfono, los

productos y servicios que compra, y los informes de ventas, incluidos los datos agregados. Por lo tanto, estos datos pueden incluir datos personales y no personales de los clientes.

Con respecto a los conjuntos de datos mixtos, el Reglamento de libre circulación de datos personales[25] establece que:

«En el caso de los conjuntos de datos compuestos por datos personales y no personales, el presente Reglamento debe aplicarse a los datos no personales de dichos conjuntos. Cuando los datos no personales y personales estén inextricablemente ligados, el presente Reglamento debe aplicarse sin perjuicio del Reglamento (UE) 2016/679».

Esto significa que, en el caso de un conjunto de datos compuesto por datos personales y no personales:

- el Reglamento de libre circulación de datos no personales se aplica a la parte de datos no personales del conjunto de datos;
- la disposición de libre circulación del Reglamento general de protección de datos[26] se aplica a la parte de datos personales del conjunto de datos; y
- si la parte de datos no personales y las partes de datos personales están «inextricablemente ligados», los derechos y obligaciones de protección de datos derivados del Reglamento general de protección de datos se aplicarán completamente a todo el conjunto de datos mixtos, incluso cuando los datos personales representen solo una pequeña parte del conjunto de datos[27].

Esta interpretación es acorde con el derecho a la protección de datos personales garantizado por la Carta de los Derechos Fundamentales de la Unión Europea[28] y con el considerando 8 del Reglamento de libre circulación de datos no personales[29]. El considerando 8 del mismo dispone que «El marco jurídico relativo a la protección de las personas físicas en lo que atañe al tratamiento de datos personales [...] y en particular [el Reglamento general de protección de datos] [...] y las Directivas (UE) 2016/680 y 2002/58/CE [...] no se ven afectados por el presente Reglamento».

Ejemplo práctico:

25 Artículo 2, apartado 2.

26 Artículo 1, apartado 3, 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 (Reglamento general de protección de datos). Véase también la sección 3.2 del presente.

27 Como se recuerda en el *Documento de trabajo de los servicios de la Comisión, Evaluación de impacto que acompaña al documento Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un marco para la libre circulación de datos no personales en la Unión Europea* (SWD(2017) 304 final), parte 1/2, p. 3, «independientemente de la cantidad de datos personales que se incluyan en conjuntos de datos mixtos, el RGPD [el Reglamento general de protección de datos] debe cumplirse completamente con respecto a la parte de datos personales del conjunto».

28 Carta de los Derechos Fundamentales de la Unión Europea (DO C 362 de 26.10.2012, p. 391).

29 Considerando 8 del mismo.

Una empresa que opera en la UE ofrece sus servicios a través de una plataforma. Las empresas (clientes) suben sus documentos, que contienen conjuntos de datos mixtos, a la plataforma. Como «responsable del tratamiento», la empresa que carga los documentos debe asegurarse de que el tratamiento de datos cumpla el Reglamento general de protección de datos. Al procesar el conjunto de datos en nombre del responsable del tratamiento, la empresa que ofrece los servicios (el «encargado del tratamiento») necesita almacenar y tratar los datos de conformidad con el Reglamento general de protección de datos, por ejemplo, para garantizar que haya un nivel adecuado de seguridad respecto a los datos, incluso mediante cifrado.

El concepto de «inextricablemente ligado» no está definido en ninguno de los dos Reglamentos[30]. A efectos prácticos, puede referirse a una situación en la que un conjunto de datos contiene datos personales así como datos no personales y la separación de ambos sería imposible o sería considerada por el responsable del tratamiento como económicamente ineficiente o no viable desde el punto de vista técnico. Por ejemplo, al comprar sistemas de informes de ventas y de CRM, la empresa tendría que duplicar sus costes en software mediante la compra por separado de software para datos de CRM (datos personales) y sistemas de informes de ventas (datos agregados/no personales) en base a los datos de CRM.

También es probable que la separación del conjunto de datos disminuya significativamente el valor del conjunto de datos. Además, la naturaleza cambiante de los datos (véase sección 2.1) hace que sea más difícil diferenciar claramente y, por lo tanto, separar entre diferentes categorías de datos.

Es importante destacar que ninguno de los dos Reglamentos obliga a las empresas a separar los conjuntos de datos que controlan o tratan.

En consecuencia, un conjunto de datos mixtos generalmente estará sujeto a las obligaciones de los responsables del tratamiento y los encargados del tratamiento de datos y respetará los derechos de los interesados establecidos por el Reglamento general de protección de datos.

Tratamiento de datos relativos a la salud

Los datos relativos a la salud pueden formar parte de un conjunto de datos. Los ejemplos incluyen registros de salud electrónicos, ensayos clínicos o conjuntos de datos recopilados por varias aplicaciones móviles relativas a la salud y al bienestar (como las aplicaciones para medir nuestro estado de salud, para recordarnos que debemos tomar nuestros medicamentos o para realizar un seguimiento de nuestro progreso físico)[31]. Los avances tecnológicos han

30 El Reglamento de libre circulación de datos no personales y el Reglamento general de protección de datos.

31 El desarrollo y el funcionamiento de las aplicaciones móviles relativas a la salud requieren el cumplimiento estricto de las normas del Reglamento general de protección de datos. Estos requisitos se especificarán con más detalle en el código de conducta sobre confidencialidad para aplicaciones móviles relativas a la salud, actualmente en preparación. Para más información sobre el estado de su desarrollo, consúltese: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

provocado que la frontera entre datos personales y no personales en estos conjuntos de datos sea cada vez menos nítida. En consecuencia, su tratamiento debe cumplir con el Reglamento general de protección de datos, en particular (dado que los datos relativos a la salud son una categoría especial de datos según el Reglamento) con el artículo 9, que establece una prohibición general del tratamiento de categorías especiales de datos y excepciones a esta prohibición.

Los datos en conjuntos de datos mixtos que contienen datos relativos a la salud pueden ser una fuente valiosa de información, por ejemplo, en el caso de investigaciones médicas adicionales, para medir los efectos secundarios de un medicamento recetado, para fines estadísticos de enfermedades o para desarrollar nuevos servicios o tratamientos de atención médica. Sin embargo, el Reglamento general de protección de datos debe cumplirse al realizar las operaciones de tratamiento inicial y al realizar operaciones de tratamiento de datos adicionales. Por lo tanto, cualquier tratamiento de datos relativos a la salud debe tener un fundamento jurídico válido[32] y una justificación apropiada, ser seguro y proporcionar suficientes garantías.

Por último, es esencial que las personas y las empresas tengan seguridad jurídica y confianza en el tratamiento de los datos. Esto también es vital para la economía de datos. Los dos Reglamentos lo garantizan y ambos persiguen el objetivo de no alterar la libre circulación de datos.

3 Libre circulación de datos y eliminación de requisitos de localización de datos

Esta sección explica con más detalle los conceptos de requisitos de localización de datos en virtud del Reglamento de libre circulación de datos no personales y el principio de libre circulación en el Reglamento general de protección de datos. Aunque estas disposiciones están destinadas a los Estados miembros, puede ser informativo para las empresas tener una idea más precisa de cómo estos dos Reglamentos contribuyen a la libre circulación de todos los datos dentro de la UE.

3.1 Libre circulación de datos no personales

El Reglamento de libre circulación de datos no personales[33] establece que «los requisitos para la localización de datos estarán prohibidos, salvo que estén justificados por razones de seguridad pública, de conformidad con el principio de proporcionalidad».

Los **requisitos de localización de datos** se definen[34] como «cualquier obligación, prohibición, condición, restricción u otro requisito previsto en las disposiciones legales, reglamentarias o

[32] Véase el artículo 6, apartado 1, 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 (Reglamento general de protección de datos).

[33] Artículo 4, apartado 1.

administrativas de los Estados miembros o que se derive de prácticas administrativas generales y coherentes en un Estado miembro y en organismos de Derecho público, también en el ámbito de la contratación pública sin perjuicio de la Directiva 2014/24/UE, que imponga el tratamiento de datos en el territorio de un determinado Estado miembro o dificulte el tratamiento de datos en cualquier otro Estado miembro[35]».

La definición ilustra que las medidas que restringen la libre circulación de datos dentro de la UE pueden tomar varias formas. Pueden figurar en leyes, reglamentos y disposiciones administrativas o incluso ser resultado de prácticas administrativas generales y coherentes. Además, la prohibición de los requisitos de localización de datos abarca tanto las medidas directas como las indirectas que restringirían la libre circulación de datos no personales.

Los requisitos directos de localización de datos pueden consistir, por ejemplo, en una obligación de almacenar datos en una localización geográfica específica (por ejemplo, los servidores deben estar ubicados en un Estado miembro en concreto) o en una obligación de cumplir requisitos técnicos nacionales únicos (por ejemplo, los datos deben utilizar formatos nacionales específicos).

Los **requisitos indirectos de localización de datos**, que pueden dificultar el tratamiento de los datos no personales en cualquier otro Estado miembro, se presentan en formas muy diversas. Pueden incluir requisitos para utilizar instalaciones tecnológicas que estén certificadas o aprobadas dentro de un Estado miembro específico u otros requisitos que tengan el efecto de dificultar el tratamiento de datos fuera de un área geográfica o territorio específico dentro de la Unión Europea[36,37].

La evaluación de si una medida específica representa un requisito indirecto de localización de datos debe considerar las circunstancias particulares de cada caso.

---

34 Artículo 3, apartado 5, del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

35 Téngase en cuenta que la inseguridad jurídica en cuanto al alcance de los requisitos legítimos e ilegítimos en materia de localización de datos limita aún más las opciones a disposición de los agentes del mercado y del sector público relativas a la localización del tratamiento de datos [véase el considerando 4 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea].

36 Considerando 4 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

37 Véanse dos estudios sobre los requisitos de localización de datos realizados antes de la adopción del Reglamento de libre circulación de datos no personales: 1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Marke*t, SMART number 2015/2016. Disponible en línea (en inglés) en: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 y 2) Time.lex, Spark Legal Network and Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*. SMART number 2015/0054. Disponible en línea (en inglés) en: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

El Reglamento de libre circulación de datos no personales[38] hace referencia al concepto de **seguridad pública** según lo contempla la jurisprudencia del Tribunal de Justicia de la Unión Europea. El concepto de seguridad pública «abarca la seguridad interna y externa de un Estado miembro[39], así como cuestiones de orden público, para, en particular, permitir la investigación, detección y enjuiciamiento de infracciones penales. Presupone la existencia de una amenaza real y suficientemente grave que afecte a uno de los intereses fundamentales de la sociedad[40], tales como una amenaza al funcionamiento de las instituciones y los servicios públicos esenciales y la supervivencia de la población, así como el riesgo de una perturbación grave de las relaciones exteriores o la coexistencia pacífica de las naciones, o un riesgo para los intereses militares».

Además, cualquier requisito de localización de datos justificado por razones de seguridad pública debe ser proporcional. De conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea, el principio de proporcionalidad exige que las medidas adoptadas sean adecuadas para garantizar el cumplimiento del objetivo perseguido y que no vayan más allá de lo necesario para tal fin[41].

En aras de la claridad, la prohibición de los requisitos de localización de datos se realiza sin perjuicio de las restricciones ya existentes establecidas por la legislación de la UE[42].

Además, el Reglamento de libre circulación de datos no personales no impone ninguna obligación a las empresas ni limita su libertad contractual para decidir dónde se tratarán sus datos.

Los Estados miembros están obligados a proporcionar información sobre cualquier requisito de localización de datos aplicable en su territorio, y a ponerla a disposición públicamente en un **punto único nacional de información en línea** (sitios web nacionales). Deben mantener

---

38 Considerando 19.

39 Véanse, por ejemplo, la sentencia del Tribunal de Justicia de 23 de noviembre de 2010, *Land Baden-Württemberg*/*Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, apartado 43 y la sentencia de 4 de abril 2017, *Sahar Fahimian*/*Bundesrepublik Deutschland*, C-544/15, ECLI:EU:C:2017:225, apartado 39.

40 Véanse, por ejemplo, la sentencia del Tribunal de Justicia de 22 de diciembre de 2008, *Comisión de las Comunidades Europeas*/*República de Austria*, C-161/07, ECLI:EU:C:2008:759, apartado 35 y la jurisprudencia citada en la misma y la sentencia de 26 de marzo de 2009, *Comisión de las Comunidades Europeas*/*República italiana*, C-326/07, ECLI:EC:C:2009:193, apartado 70, y la jurisprudencia citada en la misma.

41 Véase, por ejemplo, la sentencia del Tribunal de Justicia de 8 de julio de 2010, *Afton Chemical Limited*/*Secretary of State for Transport*, C-343/09, ECLI:EU:C:2010:419, apartado 45, y la jurisprudencia citada en la misma.

42 Véase, por ejemplo, el artículo 245, apartado 2, de la Directiva 2006/112/CE, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido, que establece que «[l]os Estados miembros podrán imponer a los sujetos pasivos establecidos en su territorio la obligación de comunicarles el lugar de conservación en caso de que esté situado fuera de su territorio». Sin embargo, este requisito debe entenderse de conformidad con el artículo 249, que establece que: «Cuando un sujeto pasivo conserve las facturas que expida o reciba por medios electrónicos que garanticen un acceso en línea a los datos y cuando el lugar de conservación esté situado en un Estado miembro distinto de aquel en el que está establecido, las autoridades competentes del Estado miembro en el que está establecido tendrán derecho, a efectos de la presente Directiva, a acceder a dichas facturas por medios electrónicos, a proceder a su carga remota y a utilizarlas, dentro de los límites fijados por la normativa del Estado miembro de establecimiento del sujeto pasivo y en la medida en que ello les resulte necesario con fines de control».

dicho sitio actualizado o proporcionar detalles actualizados a un punto de información central establecido en otro acto legislativo de la UE[43]. Por comodidad para las empresas y a fin de facilitar su acceso a información de importancia de la UE, la Comisión publicará enlaces a estos puntos de información en el portal Tu Europa[44].

3.2 Libre circulación de datos personales

El Reglamento general de protección de datos[45] establece que «la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales».

Si un Estado miembro impone requisitos de localización de datos personales por cualquier otra razón que no sea la protección de los datos personales, tendrán que evaluarse en relación con las disposiciones sobre las libertades fundamentales y los motivos permitidos para derogar esas libertades en el Tratado de Funcionamiento de la Unión Europea[46,47] y la legislación pertinente de la UE, como la Directiva de servicios[48] y la Directiva de comercio electrónico[49].

Ejemplo:

Una ley nacional exige que las cuentas de las nóminas estén ubicadas en un determinado Estado miembro por razones relacionadas con el control reglamentario, por ejemplo, por parte de la autoridad fiscal nacional. Dicha disposición nacional quedaría fuera del ámbito del artículo 1, apartado 3, del Reglamento general de protección de datos, ya que los motivos son distintos a la protección de datos personales. En su lugar, este requisito debería evaluarse en relación con las disposiciones sobre las libertades fundamentales y las razones admitidas para derogar esas libertades en el Tratado de Funcionamiento de la Unión Europea.

43 Artículo 4, apartado 4, del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

44 https://europa.eu/youreurope/index.htm

45 Artículo 1, apartado 3, 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 (Reglamento general de protección de datos).

46 Versión consolidada del Tratado de Funcionamiento de la Unión Europea, DO C 326 de 26.10.2012, pp. 47-390.

47 Véase también la sentencia del Tribunal de Justicia de 19 de junio de 2008, *Comisión de las Comunidades Europeas/Gran Ducado de Luxemburgo*, C-319/06, ECLI:EU:C:2008:350, apartados 90-91: el Tribunal consideró que la obligación de mantener disponibles y conservar ciertos documentos en un Estado miembro en particular constituye una restricción a la libre prestación de servicios; la justificación de que es «generalmente más fácil para las autoridades realizar su labor inspectora» no es suficiente.

48 Directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior, DO L 376 de 27.12.2006, pp. 36-68.

49 Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior («Directiva sobre el comercio electrónico») DO L 178 de 17.7.2000, pp. 1-16.

El Reglamento general de protección de datos[50] reconoce que los Estados miembros puedan imponer condiciones, incluidas limitaciones, en el tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. Sin embargo, tal como se establece en el considerando 53, dichas limitaciones nacionales no deben obstaculizar la libre circulación de datos personales en la UE cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos. Esto es acorde con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, que proporciona el fundamento jurídico para la adopción de normas relativas al derecho a la protección de datos personales y las normas relativas a la libre circulación de dichos datos.

3.3 Ámbito de aplicación del Reglamento de libre circulación de datos no personales

Como ya se ha mencionado, el Reglamento de libre circulación de datos no personales tiene como objetivo garantizar la libre circulación de datos que no tengan carácter personal «en la Unión»[51]. Por lo tanto, no se aplicará a las operaciones de tratamiento que tienen lugar fuera de la UE y a los requisitos de localización de datos relacionados con dicho tratamiento[52,53].

El ámbito de aplicación del Reglamento se limita, de conformidad con el artículo 2, apartado 1, al tratamiento en la UE de datos electrónicos que no tengan carácter personal, que:

a) se preste como un servicio a usuarios que residan o tengan un establecimiento en la Unión, independientemente de si el proveedor de servicios está establecido o no en la Unión; o
b) efectuado por una persona física o jurídica que resida o tenga un establecimiento en la Unión para sus propias necesidades.

Ejemplos:

Artículo 2, apartado 1, letra a), del Reglamento de libre circulación de datos no personales:

- Un proveedor de servicios en nube establecido en los EE. UU. proporciona sus servicios de tratamiento de datos a clientes residentes o establecidos en la UE. El proveedor de servicios en nube administra sus actividades a través de servidores ubicados en el

[50] Artículo 9, apartado 4, 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 (Reglamento general de protección de datos).

[51] Véase el artículo 1 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

[52] Véase el considerando 15 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

[53] El término «tratamiento» se define en términos generales (artículo 3, apartado 2, del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea) y, como se subraya en el considerando 17, el Reglamento debería aplicarse al tratamiento en su sentido más amplio, abarcando el uso de todos los tipos de sistemas de TI.

territorio de la UE, donde los datos de sus clientes europeos son conservados o tratados de otra forma. El proveedor de servicios en nube no tiene que ser propietario de la infraestructura ubicada en la UE, sino que puede por otra parte alquilar espacio de servidor en la UE. El Reglamento de libre circulación de datos no personales se aplica a dicho tratamiento de datos.

- Un proveedor de servicios en nube establecido en Japón ofrece sus servicios a clientes europeos. Las instalaciones del proveedor se encuentran en Japón y todas las actividades de tratamiento tienen lugar allí. El Reglamento de libre circulación de datos no personales no se aplicará en este caso, si todas las actividades de tratamiento tienen lugar fuera de la UE[54].

Artículo 2, apartado 1, letra b), del Reglamento de libre circulación de datos no personales:

- Una pequeña empresa europea recién creada del Estado miembro A decide ampliar su actividad comercial abriendo un establecimiento en el Estado miembro B. Para minimizar los costes, esta nueva empresa decide centralizar el almacenamiento y procesamiento de datos del nuevo establecimiento en su servidor que se encuentra en el Estado miembro A. Los Estados miembros no pueden prohibir tales esfuerzos de centralización de TI, excepto cuando esté justificado por razones de seguridad pública de conformidad con el principio de proporcionalidad.

Aunque el Reglamento de libre circulación de datos no personales no es de aplicación si todas las actividades de tratamiento de datos no personales se realizan fuera de la UE, el Reglamento general de protección de datos debe respetarse cuando los datos personales formen parte del conjunto de datos. En particular, las reglas para la transferencia de datos personales a terceros países u organizaciones internacionales en virtud del Reglamento general de protección de datos deben cumplirse en cualquier caso[55].

[54] Téngase en cuenta que el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea no hace referencia a los requisitos de localización de datos impuestos por los Estados miembros para el almacenamiento de datos no personales en terceros países, que pueden estar presentes en ordenamientos jurídicos nacionales. En aras de la claridad, el Reglamento general de protección de datos se aplica al tratamiento de datos personales de interesados que se encuentran en la UE, por parte de un responsable o un encargado del tratamiento no establecido en la UE, cuando las actividades de tratamiento se refieran a: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago; o b) el control de su comportamiento en la medida en que tenga lugar en la Unión (véase el artículo 3, apartado 2, del Reglamento general de protección de datos).

[55] En relación con la transferencia de datos personales a terceros países, consúltese la página web de la Comisión: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_es y la *Comunicación de la Comisión al Parlamento Europeo y al Consejo — Intercambio y protección de los datos personales en un mundo globalizado*, COM/2017/07 final, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM%3A2017 %3A7 %3AFIN. Respecto a Japón, la Comisión adoptó su decisión de adecuación el 23 de enero de 2019, permitiendo que los datos personales circulen libremente entre las dos economías sobre la base de fuertes garantías de protección.

3.4 Actividades relacionadas con la organización interna de los Estados miembros

El Reglamento de libre circulación de datos no personales no obliga a los Estados miembros a subcontratar la prestación de servicios relacionados con datos no personales que deseen proporcionarse u organizarse por medios distintos de los contratos públicos[56].

El artículo 2, apartado 3, segundo subapartado, del Reglamento de libre circulación de datos no personales establece:

«El presente Reglamento se aplica sin perjuicio de las disposiciones legales, reglamentarias y administrativas relativas a **la organización interna** de los Estados miembros y por las que se atribuyen, entre las autoridades públicas y organismos de Derecho público definidos en el artículo 2, apartado 1, punto 4, de la Directiva 2014/24/UE[57], competencias y responsabilidades para el **tratamiento de datos sin remuneración contractual de personas o entidades privadas**, así como las disposiciones legales, reglamentarias y administrativas de los Estados miembros que disponen la aplicación de dichas competencias y responsabilidades»[58].

Es posible que existan intereses legítimos que justifiquen la elección de este tipo de «suministro propio» de servicios de tratamiento de datos, como el «autoaprovisionamiento» o acuerdos mutuos entre las administraciones públicas. Los ejemplos típicos incluyen el uso de una «nube gubernamental» o un gobierno que contrata a una agencia de TI centralizada para proporcionar servicios de tratamiento de datos a instituciones y organismos públicos.

Sin embargo, el Reglamento de libre circulación de datos no personales alienta a los Estados miembros a considerar la eficiencia económica y otros beneficios del uso de proveedores de servicios externos[59,60]. Tan pronto como las autoridades nacionales comiencen a

---

56 Considerando 14 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

57 El artículo 2, apartado 1, punto 4, de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65), establece que un «organismo de Derecho público» es «cualquier organismo que reúna todas las características siguientes: a) que se haya creado específicamente para satisfacer necesidades de interés general que no tengan carácter industrial o mercantil; b) que esté dotado de personalidad jurídica propia, y c) que esté financiado mayoritariamente por el Estado, las autoridades regionales o locales, u otros organismos de Derecho público, o cuya gestión esté sujeta a la supervisión de dichas autoridades u organismos, o que tenga un órgano de administración, de dirección o de supervisión, en el que más de la mitad de los miembros sean nombrados por el Estado, las autoridades regionales o locales, u otros organismos de Derecho público».

58 El considerando 13 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea señala que el Reglamento se aplica sin perjuicio de la Directiva 2014/24/UE.

59 Considerando 14 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

60 Un proveedor de servicios externo sería cualquier entidad que no sea un «organismo de Derecho público», según lo dispuesto en el artículo 2, apartado 1, punto 4, de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

«subcontratar» el tratamiento de datos con la remuneración contractual de partes privadas, y este tratamiento se realice en la UE, dicho tratamiento se regirá por el Reglamento de libre circulación de datos no personales, lo que significa que el principio de la libre circulación de datos no personales se aplica a las prácticas generales y administrativas de las autoridades nacionales. En particular, tienen que abstenerse de imponer restricciones en materia de localización de datos, por ejemplo, en las licitaciones de contratación pública[61].

4 Enfoques de autorregulación que respaldan la libre circulación de datos

La autorregulación contribuye a la innovación y la confianza entre los agentes del mercado y tiene el potencial de dar mejor respuesta a los cambios del mercado. Esta sección ofrece una descripción general de las iniciativas de autorregulación respecto al tratamiento de datos personales y no personales.

4.1 La portabilidad de datos y el cambio entre proveedores de servicios en nube

Uno de los propósitos del Reglamento de libre circulación de datos no personales es evitar las prácticas de dependencia de un solo proveedor. Estas prácticas ocurren cuando los usuarios no pueden cambiar de proveedor de servicios porque sus datos se encuentran «bloqueados» en el sistema del proveedor, por ejemplo, debido a un formato de datos específico o acuerdos contractuales, y no pueden transferirse fuera del sistema de TI del proveedor. Que no existan obstáculos a la hora de portar datos es clave para que los usuarios puedan elegir libremente entre proveedores de servicios de tratamiento de datos y así garantizar una competencia efectiva en el mercado.

La portabilidad de datos entre empresas es cada vez más importante en una amplia gama de sectores digitales, incluidos los servicios en nube.

Con arreglo al artículo 6 del Reglamento de libre circulación de datos no personales, la Comisión fomentará y facilitará la elaboración de códigos de conducta autorreguladores a escala de la Unión («códigos de conducta»), con el fin de contribuir a una economía de datos competitiva. De esta forma se sientan las bases para que la industria elabore códigos de conducta de autorregulación sobre el cambio de proveedores de servicios y la transferencia de datos entre diferentes sistemas de TI.

Se deben tener en cuenta varios aspectos al desarrollar estos códigos de conducta en la transferencia de datos, en particular:

- **las mejores prácticas** para facilitar el cambio de proveedores de servicios y la portabilidad en un formato estructurado, de uso común y de lectura automática;
- **los requisitos de información mínimos** para garantizar que los usuarios profesionales, antes de celebrar un contrato de tratamiento de datos, reciban información suficientemente detallada, clara y transparente relativa a los procedimientos, los requisitos técnicos, los

[61] Considerando 13 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

plazos y los costes aplicables en caso de que un usuario profesional desee cambiar de proveedor de servicios o transferir sus datos a sus propios sistemas informáticos;

- **los enfoques de regímenes de certificación** que faciliten la comparación de los servicios en nube; y
- **los planes de comunicación** para concienciar sobre los códigos de consulta.

Respecto al mercado de servicios en nube, la Comisión ha comenzado a promover las actividades de grupos de trabajo de partes interesadas en la nube del Mercado Único Digital (MuD), que reúne a expertos en la nube y usuarios profesionales, incluidas pequeñas y medianas empresas. En la actualidad existe un subgrupo dedicado a desarrollar códigos de conducta autorregulados sobre la portabilidad de datos y el cambio entre proveedores de servicios en nube (Grupo de trabajo SWIPO)[62], mientras otro subgrupo se encuentra trabajando en el desarrollo de una certificación de seguridad en nube (Grupo de trabajo CSPCERT)[63].

El Grupo de trabajo SWIPO está desarrollando códigos de conducta que cubren todo el espectro de servicios en nube; infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS).

La Comisión espera que los diferentes códigos de conducta se complementen con **cláusulas contractuales modelo**[64]. Esto permitirá una especificidad técnica y legal suficiente en la adopción y la aplicación de los códigos de conducta, lo que será de particular importancia para las pequeñas y medianas empresas. La redacción de las cláusulas contractuales modelo se ha programado una vez esté terminada la elaboración de los códigos de conducta (que debe estar listo antes del 29 de noviembre de 2019).

De conformidad con el artículo 8 del Reglamento de libre circulación de datos no personales, la Comisión evaluará la adopción del Reglamento antes del 29 de noviembre de 2022. Esto permitirá evaluar: i) el impacto de la libre circulación de datos en la Unión; ii) la aplicación del Reglamento, en particular en lo que respecta a los conjuntos de datos mixtos; iii) la medida en que los Estados miembros han derogado efectivamente las restricciones injustificadas de localización de datos; y iv) la efectividad en el mercado de los códigos de conducta en el área de la portabilidad de datos y el cambio entre proveedores de servicios en nube.

62 El Grupo de trabajo de intercambio y portabilidad de datos en nube (SWIPO).

63 El Grupo de trabajo europeo de certificación de proveedores de servicios en nube (CSPCERT). Véase también la sección 4.3.

64 Véase el considerando 30 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

La noción de portabilidad y la interacción con el Reglamento general de protección de datos

Ambos Reglamentos[65] hacen referencia a la portabilidad de los datos y al objetivo de facilitar la portabilidad de los datos de un entorno de TI a otro, es decir, a los sistemas de otro proveedor o dentro de un sistema propio. Esto evita la dependencia de un solo proveedor y fomenta la competencia entre las diferentes ofertas de servicios. No obstante, los Reglamentos difieren en su enfoque de portabilidad cuando se trata de la relación entre los grupos de interesados y la naturaleza legal de las disposiciones.

El derecho a la portabilidad de los datos personales en virtud del artículo 20 del Reglamento general de protección de datos se centra en la relación entre el interesado y el responsable del tratamiento. Hace referencia al derecho del interesado a recibir los datos personales que este haya proporcionado al responsable del tratamiento, en un formato estructurado, comúnmente utilizado y legible por la máquina, y transmitir esos datos a otro responsable del tratamiento o a sus propias instalaciones de almacenamiento sin obstáculos desde el responsable del tratamiento al que se le han facilitado los datos personales[66]. Por lo general, los interesados en esta relación son consumidores de diversos servicios en línea que desean cambiar entre estos proveedores de servicios.

El artículo 6 del Reglamento de libre circulación de datos no personales no establece un derecho para que los usuarios profesionales porten datos, pero tiene un enfoque autorregulador, con códigos de conducta voluntarios para el sector. Al mismo tiempo, está enfocado a una situación en la que un usuario profesional ha externalizado el tratamiento de sus datos a un tercero que ofrece un servicio de tratamiento de datos[67]. Con arreglo al artículo 3, apartado 8, del Reglamento de libre circulación de datos no personales, se puede considerar como «usuario profesional» a toda «persona física o jurídica, incluidas las autoridades y organismos de Derecho público, que utiliza o solicita un servicio de tratamiento de datos para fines relacionados con su actividad comercial, negocio, oficio, profesión o función».

En la práctica, la portabilidad con arreglo al artículo 6 del Reglamento de libre circulación de datos no personales abarca las interacciones de empresa a empresa entre un usuario profesional (que, en casos que incluyen el tratamiento de datos personales, puede calificarse como «responsable del tratamiento» de acuerdo con el Reglamento general de protección de

65 Véanse el artículo 6 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea y el artículo 20 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 (Reglamento general de protección de datos).

66 Véase el Grupo de Trabajo del artículo 29: *Directrices sobre el derecho a la portabilidad de los datos*. WP 242 rev.01, adoptadas el 13 de diciembre de 2016, revisadas por última vez y adoptadas el 5 de abril de 2017.

67 Considerando 29 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea: «Mientras que los consumidores particulares se benefician del Derecho vigente de la Unión [es decir, del Reglamento general de protección de datos], la capacidad de cambiar de un proveedor de servicios a otro no se facilita a aquellos usuarios que actúan en el marco de sus actividades empresariales o profesionales».

datos) y un proveedor de servicios (que, de manera similar, puede denominarse «encargado del tratamiento»).

A pesar de las diferencias, pueden surgir situaciones en las que la portabilidad de datos se rijan tanto por el Reglamento de libre circulación de datos no personales como por el Reglamento general de protección de datos en relación con conjuntos de datos mixtos.

Ejemplo:

Una empresa que utiliza un servicio en nube decide cambiar su proveedor de servicios en nube y portar todos los datos a un nuevo proveedor. El cambio de proveedor de servicios y la portabilidad de los datos se contempla en el contrato entre el cliente y el proveedor de servicios en nube. Si el antiguo proveedor de servicios en nube se adhiere a los códigos de conducta desarrollados al auspicio del Reglamento de libre circulación de datos no personales, la portabilidad de datos debe realizarse de conformidad con los requisitos especificados en los mismos.

Si los datos personales también forman parte de los conjuntos de datos portados, la portabilidad debe cumplir con todas las disposiciones pertinentes del Reglamento general de protección de datos, en particular, garantizar que el nuevo proveedor de servicios en nube cumple con los requisitos aplicables, como la seguridad[68].

Ejemplo:

En el caso de que un banco decida cambiar su proveedor de administración basada en las relaciones con el cliente (CRM, por sus siglas en inglés), es posible que algunos datos (personales y no personales) deban migrarse del proveedor anterior al nuevo. Dichos datos estarán posteriormente sujetos a diferentes requisitos reglamentarios, algunos derivados del Reglamento general de protección de datos y otros del Reglamento de libre circulación de datos no personales.

4.2 Códigos de conducta y mecanismos de certificación de protección de datos personales

Los códigos de conducta y los mecanismos de certificación pueden utilizarse para demostrar el cumplimiento de las obligaciones en virtud del Reglamento general de protección de datos (véanse los artículos 24, apartado 3, y 28, apartado 5).

De conformidad con el artículo 40, apartado 1, y el artículo 42, apartado 1, del Reglamento general de protección de datos, los Estados miembros, las autoridades de control, el Comité Europeo de Protección de Datos y la Comisión deberían alentar a la industria a desarrollar códigos de conducta y establecer mecanismos de certificación para la protección de datos.

[68] Véase el Grupo de Trabajo del artículo 29: *Dictamen 05/2012 sobre la computación en nube* adoptado el 1 de julio de 2012, WP196, que analiza la posición y las obligaciones de los usuarios de la nube y los proveedores de servicios de nube en relación con el procesamiento de datos personales.

Las asociaciones u otros organismos que representan una categoría específica de responsables o encargados del tratamiento pueden preparar un código de conducta para el sector específico. Debe enviarse un borrador del código a la autoridad de control competente respectiva para su aprobación[69]. Si el borrador del código de conducta está relacionado con actividades de tratamiento en varios Estados miembros, la autoridad de control debe enviarlo al Comité Europeo de Protección de Datos antes de aprobarlo. El Comité emitirá entonces un dictamen sobre si el proyecto de código cumple con el Reglamento general de protección de datos.

El Comité Europeo de Protección de Datos publicó sus Directrices 1/2019 sobre códigos de conducta y órganos de seguimiento con arreglo al Reglamento general de protección de datos[70]. Estas directrices incluyen información sobre la elaboración de códigos de conducta, criterios para su aprobación y otra información útil. Del mismo modo, las Directrices 1/2018 del Comité Europeo de Protección de Datos sobre certificación e identificación de criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento general de protección de datos proporcionan información sobre la certificación en virtud del presente Reglamento y el desarrollo y aprobación de criterios de certificación[71].

Ejemplos de códigos de conducta desarrollados por la industria de la nube:

El Código de conducta en la nube de la UE, cuyo desarrollo fue facilitado por la Comisión, se redactó en colaboración con el Cloud Industry Group (C-SIG) en base a la Directiva de protección de datos[72] y posteriormente el Reglamento general de protección de datos. El Código de conducta para proveedores de servicios en nube de la UE cubre todo el espectro de servicios en nube: software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS)[73].

El Código de conducta para proveedores de servicios de infraestructura (por sus siglas en inglés, CISPE)[74] se centra en los proveedores de IaaS. El Código de conducta CISPE consta de requisitos relativos a los proveedores de IaaS que actúan como encargados del tratamiento de datos en virtud del Reglamento general de protección de datos. Establece

69 Véanse el artículo 40, apartado 5, y el artículo 55 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 (Reglamento general de protección de datos).

70 Comité Europeo de Protección de Datos: *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, adoptadas el 12 de febrero de 2019, versión para consulta pública (en inglés), disponible en línea en: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

71 Comité Europeo de Protección de Datos: *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679*, adoptadas el 23 de enero de 2019, disponible (en inglés) en línea en: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

72 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (fecha de fin de vigencia: 24 de mayo de 2018).

73 Para más información sobre el Código de conducta para proveedores de servicios en nube de la UE véase: https://eucoc.cloud/en/home.html

74 Para más información sobre el Código de conducta CISPE véase: https://cispe.cloud/code-of-conduct/

igualmente disposiciones sobre la estructura de gobierno para la adopción y la aplicación del código.

El Código de conducta de la alianza de seguridad en nube (por sus siglas en inglés, CSA) para el cumplimiento de RGPD se dirige a todos los interesados en la computación en nube y la legislación europea de datos personales, así como a los proveedores de servicios en nube, los clientes en la nube y los clientes potenciales, los auditores de la nube y agentes intermediarios en la nube. El código de conducta cubre todo el espectro de proveedores de servicios en nube[75].

4.3 Aumentar la confianza en la seguridad del tratamiento de datos transfronterizo – certificación de seguridad

Como se establece en el considerando 33 del Reglamento de libre circulación de datos no personales, aumentar la confianza en la seguridad del tratamiento de datos transfronterizo debe reducir la propensión de los agentes del mercado y del sector público a utilizar la localización de datos como un indicador para la seguridad de estos. Junto con el paquete de seguridad cibernética propuesto por la Comisión en 2017[76], el Grupo de trabajo CSPCERT está desarrollando recomendaciones para establecer un mecanismo de certificación de nube europeo que se presentará a la Comisión. Dicho mecanismo tiene el potencial de facilitar la libre circulación de datos, permitir una mejor comparabilidad de los servicios en nube y promover su uso. La Comisión puede solicitar a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) que prepare una propuesta de mecanismo de conformidad con las disposiciones pertinentes del Reglamento sobre la Ciberseguridad[77]. Dicho mecanismo podrá abordar tanto datos personales como no personales. Además del Reglamento sobre la Ciberseguridad, y como se destaca en la sección 4.2, el RGPD también se puede utilizar para demostrar la existencia de medidas de protección adecuadas para la seguridad de los datos[78].

Observaciones finales

Garantizar la seguridad jurídica y la confianza en el tratamiento de datos es esencial para la capacidad de la UE de sacar el máximo partido de los datos, donde las cadenas de valor pueden desarrollarse a través de sectores y fronteras. Los dos Reglamentos lo garantizan y ambos persiguen el objetivo de la libre circulación de datos. Juntos, el Reglamento de libre circulación de datos no personales y el Reglamento general de protección de datos, conforman la base para la libre circulación de todos los datos en la Unión Europea y una economía europea de datos altamente competitiva.

---

75 Para más información sobre el Código de conducta CSA véase: https://gdpr.cloudsecurityalliance.org/

76 Para más información, véase: https://ec.europa.eu/digital-single-market/en/cyber-security

77 Reglamento del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»).

78 Véase el considerando 74 del Reglamento sobre la Ciberseguridad.