COMISIÓN
EUROPEA

Bruselas, 23.2.2022
COM(2022) 68 final

2022/0047 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

sobre normas armonizadas para un acceso justo a los datos y su utilización (Ley de Datos)

(Texto pertinente a efectos del EEE)

{SEC(2022) 81 final} - {SWD(2022) 34 final} - {SWD(2022) 35 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Razones y objetivos de la propuesta

La presente exposición de motivos acompaña a la propuesta de Reglamento sobre normas armonizadas para un acceso justo a los datos y su utilización (Ley de Datos).

Los datos son un componente fundamental de la economía digital y un recurso esencial para garantizar las transiciones ecológica y digital. En los últimos años, el volumen de datos generados por los seres humanos y las máquinas ha aumentado exponencialmente. Sin embargo, la mayoría de los datos no se utilizan, o su valor se concentra en manos de pocas grandes empresas. La escasa confianza, los incentivos económicos contradictorios y los obstáculos tecnológicos impiden sacar pleno provecho del potencial de la innovación basada en los datos. Resulta por lo tanto crucial liberar este potencial ofreciendo oportunidades para la reutilización de los datos y eliminando los obstáculos al desarrollo de la economía de datos europea de conformidad con las normas europeas y respetando plenamente los valores europeos, en consonancia también con la misión de reducir la brecha digital para que todos se beneficien de estas oportunidades. Si se garantiza un mayor equilibrio en la distribución del valor de los datos, a la par con la nueva oleada de datos industriales no personales y la proliferación de productos conectados a la internet de las cosas, se creará un enorme potencial para impulsar una economía de los datos sostenible en Europa.

Regular el acceso y el uso de los datos es un requisito previo fundamental para aprovechar las oportunidades que ofrece la era digital en la que vivimos. La presidenta de la Comisión, Ursula von der Leyen, declaró en sus orientaciones políticas para la Comisión 2019-2024 que Europa debe «*equilibrar el flujo y el uso de los datos, preservando al mismo tiempo un elevado nivel de privacidad, protección, seguridad y ética*»[1]. En el Programa de trabajo de la Comisión para 2020[2] se enumeran varios objetivos estratégicos, entre los cuales se incluye la Estrategia Europea de Datos[3], adoptada en febrero de 2020. Esta estrategia tiene por objeto construir un auténtico mercado único de datos y hacer de Europa un líder mundial en la economía ágil de los datos. Por este motivo, la Ley de Datos es un pilar clave y la segunda gran iniciativa anunciada en la estrategia de datos. En concreto, contribuye a la creación de un marco de gobernanza intersectorial para el acceso a los datos y su utilización al legislar sobre cuestiones que afectan a las relaciones entre los agentes de la economía de los datos, con el fin de ofrecer incentivos para el intercambio horizontal de datos entre sectores.

En las Conclusiones del Consejo Europeo de los días 21 y 22 de octubre de 2021 se subrayaba «*la importancia de avanzar rápidamente en otras iniciativas existentes y futuras, en particular, explotando el valor de los datos en Europa, concretamente por medio de un marco regulador general que propicie la innovación y facilite una mejor portabilidad de los datos y el acceso equitativo a ellos y garantice la interoperabilidad*»[4]. El 25 de marzo de 2021, el Consejo Europeo pidió que «*se aproveche mejor el potencial de los datos y de las tecnologías*

---

[1] Ursula von der Leyen, «Una Unión que se esfuerza por lograr más resultados — Mi agenda para Europa, Orientaciones políticas para la próxima Comisión Europea 2019-2024», 16 de julio de 2019.

[2] Comisión Europea, «Anexos al Programa de trabajo de la Comisión para 2020 — Una Unión que se esfuerza por lograr más resultados», COM(2020) 37, de 29 de enero de 2020.

[3] COM/2020/66 final.

[4] Consejo Europeo, reunión del Consejo Europeo (21-22 de octubre de 2021) — Conclusiones EUCO 17/21, 2021, p. 2.

digitales, en beneficio de la sociedad y la economía»[5]. Los días 1 y 2 de octubre de 2020, subrayó «*la necesidad de que se mejore la disponibilidad de datos de gran calidad y de que se fomenten y faciliten un mejor intercambio y puesta en común de los datos, así como la interoperabilidad*»[6]. En cuanto a los servicios en la nube, el 15 de octubre de 2020 los Estados miembros de la UE adoptaron por unanimidad una declaración conjunta sobre la construcción de la nube de próxima generación para las empresas y el sector público de la UE. Esto requeriría, por ejemplo, una nueva generación de ofertas de servicios en la nube de la UE que alcancen los niveles más elevados en materia de portabilidad e interoperabilidad[7].

La Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre una estrategia europea de datos instaba a la Comisión a presentar una ley de datos para fomentar y permitir un flujo de datos mayor y justo entre empresas, entre empresas y la administración, entre la administración y las empresas y entre administraciones, en todos los sectores[8]. En su Resolución de 25 de marzo de 2021, el Parlamento Europeo también destacó la necesidad de crear espacios comunes europeos de datos con el objetivo de garantizar la libre circulación de los datos no personales a través de las fronteras y los sectores e incrementar los flujos de datos entre las empresas, el mundo académico, las partes interesadas pertinentes y el sector público. En este contexto, instó a la Comisión a que aclare los derechos de utilización, especialmente en los mercados entre empresas y entre empresas y administración, y observó que los desequilibrios del mercado derivados de la concentración de datos restringen la competencia, multiplican las barreras de entrada en el mercado y reducen el acceso y el uso más amplios de los datos.

En su Resolución, el Parlamento Europeo también señaló que los acuerdos contractuales entre empresas no garantizan necesariamente el acceso adecuado a los datos para las pequeñas y medianas empresas (pymes), debido a disparidades en el poder de negociación o en los conocimientos técnicos. Por esta razón, el Parlamento Europeo destacó la necesidad de que los contratos establezcan obligaciones y responsabilidades claras para el acceso, el tratamiento, el intercambio y el almacenamiento de datos con el fin de limitar su uso indebido.

Pidió a la Comisión y a los Estados miembros que examinaran los derechos y obligaciones de los agentes en materia de acceso a los datos en cuya generación habían participado y que mejoraran su conocimiento, en particular, del derecho de acceso a los datos, de su transferencia, de cómo instar a otra parte a que deje de utilizarlos, o a corregirlos o eliminarlos, así como de identificar a sus titulares y delinear la naturaleza de esos derechos.

Para el intercambio de datos entre empresas y administraciones, el Parlamento Europeo pidió a la Comisión que definiera las circunstancias, condiciones e incentivos en cuyo contexto debe obligarse al sector privado a compartir los datos con el sector público, por ejemplo debido a su necesidad de organizar unos servicios públicos basados en los datos, y que también examinara los sistemas obligatorios de intercambio de datos entre empresas y administraciones, por ejemplo en situaciones de fuerza mayor.

---

5 Consejo Europeo, Declaración de los miembros de la reunión del Consejo Europeo (25 de marzo de 2021) — Declaración SN 18/21, p. 4.

6 Consejo Europeo, reunión del Consejo Europeo (1-2 de octubre de 2020) — Conclusiones EUCO 13/20, 2020, p. 5.

7 Comisión Europea (2020): *La Comisión acoge con satisfacción la declaración de los Estados miembros sobre la federación de la nube de la UE*, comunicado de prensa.

8 Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre una Estrategia Europea de Datos [2020/2217(INI)]

En este contexto, la Comisión presenta la propuesta de **Ley de Datos** con el objetivo de **garantizar la equidad en la asignación del valor de los datos entre los agentes de la economía de los datos y de fomentar el acceso a los datos y su utilización**.

La propuesta contribuirá a alcanzar objetivos políticos más amplios, como el de garantizar que las empresas de la UE de todos los sectores estén en condiciones de innovar y competir, capacitar eficazmente a los individuos con respecto a sus datos, y preparar mejor a las empresas y a los organismos del sector público con un mecanismo proporcionado y predecible para hacer frente a los principales retos políticos y sociales, entre los que se incluyen las emergencias públicas y otras situaciones excepcionales. Las empresas podrán transferir fácilmente sus datos y otros activos digitales entre proveedores competidores de servicios en la nube y otros servicios de tratamiento de datos. El intercambio de datos sectorial e intersectorial requiere un marco de interoperabilidad de las medidas de procedimiento y legislativas para aumentar la confianza y mejorar la eficiencia. La creación de espacios comunes europeos de datos para sectores estratégicos de la economía y ámbitos de interés público contribuirá a un auténtico mercado interior de datos que permita el intercambio y la utilización de datos entre sectores. Por consiguiente, el presente Reglamento contribuye a la definición de estos marcos e infraestructuras de gobernanza, así como a la puesta en común de datos fuera de los espacios de datos.

A continuación se exponen los objetivos específicos de la propuesta.

– **Facilitar el acceso a los datos y su utilización por parte de los consumidores y las empresas, preservando al mismo tiempo los incentivos para invertir en formas de generar valor a través de los datos.** Esto incluye aumentar la seguridad jurídica en torno al intercambio de datos obtenidos o generados por el uso de productos o servicios relacionados, así como normas operativas para garantizar la equidad en los contratos de intercambio de datos. La propuesta **aclara** la aplicación de los derechos pertinentes en virtud de la Directiva 96/9/CE, sobre la protección jurídica de las bases de datos (**Directiva sobre bases de datos**)[9], a sus disposiciones.

– **En aquellas situaciones en las que exista una necesidad excepcional de obtener datos, prever el uso de los datos que obren en poder de las empresas por parte de los organismos del sector público y de las instituciones de la Unión.** Esto afecta principalmente a las emergencias públicas, pero también a otras situaciones excepcionales en las que está justificado el intercambio obligatorio de datos entre empresas y administraciones, con el fin de apoyar políticas y servicios públicos eficientes, eficaces y basados en pruebas y en exigencias de rendimiento.

– **Facilitar el cambio entre servicios en la nube y en el borde.** El acceso a servicios de tratamiento de datos competitivos e interoperables es una condición previa para una economía de datos floreciente, en la que los datos puedan compartirse fácilmente dentro de los ecosistemas sectoriales y entre ellos. El nivel de confianza en los servicios de tratamiento de datos determina la aceptación de dichos servicios por parte de los usuarios en todos los sectores de la economía.

– **Establecer salvaguardias contra la transferencia ilegal de datos sin notificación por parte de los proveedores de servicios en la nube**. Se ha expresado preocupación acerca del acceso ilegal a los datos por parte de gobiernos de terceros países o del Espacio Económico Europeo (EEE). Las salvaguardias deberían reforzar

9 DO L 77 de 27.3.1996, p. 20.

aún más la confianza en los servicios de tratamiento de datos que, cada vez más, sostienen la economía europea de los datos.

– **Prever el desarrollo de normas de interoperabilidad para la reutilización de los datos entre sectores**, a fin de eliminar los obstáculos al intercambio de datos entre espacios comunes europeos de datos, en consonancia con los requisitos de interoperabilidad sectoriales, y entre otros datos que no entren en el ámbito de aplicación de un espacio común europeo de datos específico. La propuesta también apoya el establecimiento de normas para los «contratos inteligentes». Se trata de programas informáticos en libros mayores electrónicos que ejecutan y liquidan operaciones sobre la base de condiciones predeterminadas. Tienen el potencial de ofrecer a los titulares y destinatarios de datos garantías de que se respetan las condiciones para compartir datos.

• **Coherencia con las disposiciones existentes en la misma política sectorial**

La presente propuesta es coherente con las normas vigentes sobre el **tratamiento de datos personales** [incluido el Reglamento general de protección de datos (RGPD)[10]], la protección de la vida privada y la **confidencialidad de las comunicaciones** y de cualquier dato (personal y no personal) almacenado en equipos terminales y accesible desde los mismos (la Directiva sobre la privacidad y las comunicaciones electrónicas[11], que será sustituida por el Reglamento sobre la privacidad y las comunicaciones electrónicas, actualmente objeto de negociaciones legislativas). La presente propuesta complementa los derechos existentes, en particular los derechos relativos a los datos generados por el producto de un usuario conectado a una red de comunicaciones electrónicas de acceso público.

El **Reglamento relativo a un marco para la libre circulación de datos no personales**[12] establece un componente fundamental de la economía de los datos europea, garantizando que los datos no personales puedan almacenarse, tratarse y transferirse en cualquier lugar de la Unión. También presenta un enfoque autorregulador del problema de la dependencia de un solo proveedor en el ámbito de los proveedores de servicios de tratamiento de datos, introduciendo un código de conducta para facilitar el traslado de datos entre servicios en la nube («SWIPO», por sus siglas en inglés, es el código de conducta desarrollado por la industria para el cambio de proveedor de servicios en la nube y la portabilidad de los datos). La presente propuesta desarrolla este enfoque para ayudar a las empresas y a los ciudadanos a aprovechar al máximo el derecho a cambiar de proveedor y transferir datos. También es plenamente coherente con la Directiva sobre cláusulas contractuales abusivas en lo que respecta al Derecho contractual[13]. En cuanto a los servicios en la nube, dado que el enfoque autorregulador no parece haber afectado significativamente a la dinámica del mercado, la presente propuesta presenta un enfoque regulador del problema destacado en el Reglamento relativo a un marco para la libre circulación de datos no personales.

El tratamiento y el almacenamiento de datos internacionales y las transferencias de datos se rigen por el RGPD, los compromisos comerciales de la Organización Mundial del Comercio (OMC), el Acuerdo General sobre el Comercio de Servicios (AGCS) y los acuerdos comerciales bilaterales.

---

10 DO L 119 de 4.5.2016, p. 1.
11 DO L 201 de 31.7.2002, p. 37.
12 DO L 303 de 28.11.2018, p. 59; SWIPO (2021), véase el *sitio web*
13 DO L 95 de 21.4.1993, p. 29.

El **Derecho de la competencia**[14] es aplicable, entre otras cosas, en el contexto del control de las concentraciones, el intercambio de datos por parte de las empresas o el abuso de posición dominante de una empresa.

La **Directiva sobre bases de datos**[15] establece la protección *sui generis* de las bases de datos creadas como consecuencia de una inversión sustancial, aunque la propia base de datos no sea una creación intelectual original protegida por derechos de autor. Basándose en la considerable cantidad de jurisprudencia que interpreta las disposiciones de la Directiva sobre bases de datos, la presente propuesta aborda las incertidumbres jurídicas existentes sobre si las bases de datos que contienen datos generados u obtenidos mediante el uso de productos o servicios relacionados, como sensores, u otros tipos de datos generados por máquinas, tendrían derecho a dicha protección.

El **Reglamento sobre las relaciones entre plataformas y empresas**[16] impone obligaciones de transparencia, exigiendo a las plataformas que describan para los usuarios profesionales los datos generados por la prestación del servicio.

La **Directiva sobre datos abiertos**[17] establece normas mínimas sobre la reutilización de los datos en poder del sector público y de los datos de las investigaciones financiadas con fondos públicos que se ponen a disposición del público a través de repositorios.

La **iniciativa «Interoperable Europe»** tiene por objeto establecer una política de interoperabilidad cooperativa para un sector público modernizado. La iniciativa surgió del programa ISA^2, un programa de financiación de la Unión que se desarrolló entre 2016 y 2021 y que apoyó el desarrollo de soluciones digitales que permitieran la interoperabilidad de los servicios públicos transfronterizos e intersectoriales[18].

La presente propuesta complementa la **Ley de Gobernanza de Datos** recientemente adoptada, que tiene por objeto facilitar el intercambio voluntario de datos por parte de particulares y empresas y armoniza las condiciones para el uso de determinados datos del sector público, sin alterar los derechos materiales sobre los datos ni los derechos establecidos de acceso y utilización de datos[19]. También complementa la propuesta de **Ley de Mercados Digitales**, que exigirá que determinados proveedores de servicios básicos de plataforma, conocidos como «guardianes de acceso» proporcionen, entre otras cosas, una portabilidad más eficaz de los datos generados a través de las actividades profesionales y de los usuarios finales[20].

La presente propuesta no afecta a las normas vigentes en los ámbitos de la propiedad intelectual (excepto la aplicación del derecho *sui generis* de la Directiva sobre bases de datos), la competencia, la justicia y los asuntos de interior y la cooperación (internacional) conexa, las obligaciones relacionadas con el comercio ni la protección jurídica de los secretos comerciales.

Serán necesarias adaptaciones legislativas para promover la transición digital en varios ámbitos. En el marco del pasaporte europeo de productos digitales (como parte de la Iniciativa

14 DO L 335 de 18.12.2010, p. 36.
15 DO L 77 de 27.3.1996, p. 20.
16 DO L 186 de 11.7.2019, p. 57.
17 DO L 172 de 26.6.2019, p. 56.
18 DO L 318 de 4.12.2015, p. 1.
19 COM/2020/767 final.
20 DO L 186 de 11.7.2019, p. 57.

sobre Productos Sostenibles)[21], se establecerán normas claras sobre el acceso a datos específicos necesarios para la circularidad y la sostenibilidad de determinados productos a lo largo de su ciclo de vida y en situaciones no excepcionales. Las normas de Derecho privado constituyen un elemento clave del marco general. Por consiguiente, el presente Reglamento adapta el Derecho contractual y otras normas para mejorar las condiciones de reutilización de los datos en el mercado interior, y evitar que las partes contratantes abusen de los desequilibrios en el poder de negociación en detrimento de las partes más débiles.

Como propuesta horizontal, la **Ley de Datos** prevé **normas básicas para todos los sectores** en lo que respecta a los derechos de utilización de los datos, como, por ejemplo, en los ámbitos de la maquinaria inteligente o los bienes de consumo. Sin embargo, los derechos y obligaciones en materia de acceso y utilización de los datos también se han regulado en distinta medida a nivel sectorial. La Ley de Datos no modificará ninguna legislación existente de este tipo, pero la futura legislación en esos ámbitos deberá, en principio, ajustarse a los principios horizontales de la Ley de Datos. Así pues, cuando se revisen los instrumentos sectoriales, debe evaluarse la convergencia con las normas horizontales de la Ley de Datos. La presente propuesta deja margen para que la legislación vertical establezca normas más detalladas para la consecución de los objetivos reglamentarios sectoriales.

Habida cuenta de la legislación sectorial existente, en lo que respecta a la creación del espacio de datos del Pacto Verde, la revisión[22] de la **Directiva INSPIRE**[23] permitirá una mayor disponibilidad y reutilización libre de los datos espaciales y medioambientales. Esta iniciativa hará que sea más fácil para las autoridades públicas, las empresas y los ciudadanos de la UE apoyar la transición hacia una economía más ecológica y neutra en carbono y la reducción de la carga administrativa. Se espera que respalde los servicios de datos reutilizables a gran escala para ayudar a recopilar, compartir, tratar y analizar grandes volúmenes de datos pertinentes a fin de garantizar el cumplimiento de la legislación medioambiental y las acciones prioritarias del Pacto Verde Europeo. El objetivo es racionalizar la comunicación de informes y reducir la carga mediante una mejor reutilización de los datos existentes, la generación automática de informes a través de la extracción de datos y la inteligencia empresarial.

El **Reglamento sobre la electricidad**[24] de la UE exige a los gestores de redes de transporte que faciliten datos a los reguladores y para una planificación de la adecuación de los recursos, mientras que la **Directiva sobre la electricidad**[25] de la UE prevé un acceso transparente y no discriminatorio a los datos y encomienda a la Comisión que desarrolle los correspondientes requisitos y procedimientos de interoperabilidad para facilitar dicho acceso. La **Segunda Directiva sobre servicios de pago**[26] inaugura algunos tipos de información sobre transacciones de pago y cuentas en determinadas condiciones, permitiendo así el intercambio de datos entre empresas en el ámbito de la tecnología financiera. En el sector de la movilidad y el transporte existe una gran variedad de normas de acceso e intercambio de datos. La información sobre reparación y mantenimiento procedente de vehículos de motor y máquinas agrícolas está sujeta a obligaciones específicas de acceso o intercambio de datos en virtud de la **legislación sobre homologación de tipo**[27]. Sin embargo, se necesitan nuevas normas para

21 COM/2020/98 final.
22 Iniciativa GreenData4All (REFIT) Calendario del tren legislativo Parlamento Europeo (europa.eu)
23 DO L 108 de 25.4.2007, p. 1.
24 DO L 158 de 14.6.2019, p. 54.
25 DO L 158 de 14.6.2019, p. 125.
26 DO L 337 de 23.12.2015, p. 35 DO L 337 de 23.12.2015, p. 35.
27 DO L 151 de 14.6.2018, p. 1. DO L 60 de 2.3.2013, p. 1.

garantizar que la legislación existente sobre homologación de tipo de los vehículos se adapte a la era digital y promueva el desarrollo de vehículos limpios, conectados y automatizados. A partir del marco para el acceso y la utilización de datos de la Ley de Datos, estas normas abordarán los retos específicos del sector, incluido el acceso a las funciones y los recursos de los vehículos.

En el marco de la **Directiva sobre los sistemas de transporte inteligentes**[28], se han elaborado varios reglamentos delegados que seguirán desarrollándose, en particular para especificar la accesibilidad de los datos para el transporte de viajeros por carretera y multimodal, especialmente a través de los puntos de acceso nacionales. En la gestión del tránsito aéreo, los datos no operativos son importantes para mejorar la intermodalidad y la conectividad. Los datos operativos relacionados con la gestión del tránsito aéreo estarían sujetos al régimen específico definido en el marco del **Cielo Único Europeo**[29]. En el seguimiento del tráfico marítimo, los datos relacionados con los buques (seguimiento y localización) son importantes para mejorar la intermodalidad y la conectividad: estos datos se inscriben en el régimen específico de la Directiva de sistemas de seguimiento y de información sobre el tráfico marítimo[30], y también entran en el ámbito de competencias del sistema y los servicios marítimos digitales[31]. La propuesta de Reglamento relativa a la implantación de **infraestructura para los combustibles alternativos**[32] especifica los tipos de datos pertinentes que deben suministrarse, en sinergia con el marco general establecido en la Directiva sobre los sistemas de transporte inteligentes.

- **Coherencia con otras políticas de la Unión**

La presente propuesta está en consonancia con las prioridades de la Comisión de construir **una Europa adaptada a la era digital** y una economía al servicio de las personas y preparada para el futuro[33], en la que la digitalización del mercado interior se caracterice por un alto grado de confianza, seguridad y libertad de elección para los consumidores. La digitalización del mercado interior es altamente competitiva gracias a un marco que favorece la transparencia, la competencia y la innovación, y que es tecnológicamente neutro. Apoya el **Mecanismo de Recuperación y Resiliencia**[34], sacando provecho de las lecciones de la pandemia de COVID-19 y de los beneficios que se obtienen gracias a unos datos más fácilmente accesibles cuando sea necesario.

La presente propuesta apoya el papel fundamental que, de varias maneras, juegan los datos en la consecución de los objetivos del Pacto Verde Europeo. En primer lugar, profundizando en la comprensión por parte de los gobiernos, las empresas y los ciudadanos de las repercusiones de los productos, servicios y materiales en la sociedad y la economía a lo largo de enteras cadenas de suministro. En segundo lugar, movilizando la riqueza existente de datos pertinentes del sector privado para abordar las cuestiones climáticas, de biodiversidad, contaminación[35] y recursos naturales, en consonancia con los objetivos del Pacto Verde Europeo[36], las pertinentes Conclusiones del Consejo[37] y las posiciones[38] del Parlamento

28 DO L 207 de 6.8.2010, p. 1.
29 DO L 96 de 31.3.2004, p. 1; DO L 96 de 31.3.2004, p. 10; DO L 96 de 31.3.2004, p. 20.
30 DO L 308 de 29.10.2014, p. 82.
31 DO L 96 de 12.4.2016, p. 46.
32 COM/2021/559 final.
33 COM/2020/67 final.
34 DO L 57 de 18.2.2021, p. 17.
35 COM/2021/400 final.
36 COM/2019/640 final.

Europeo. En tercer lugar, colmando las lagunas de conocimiento y gestionando las crisis conexas mediante la mejora de las medidas de mitigación, preparación, respuesta y recuperación.

En consonancia con la **Estrategia Industrial**[39], la propuesta aborda las tecnologías altamente estratégicas, como la computación en la nube y los sistemas de inteligencia artificial, que son áreas cuyo pleno potencial la UE tiene aún que aprovechar ante la nueva oleada de datos industriales. La propuesta lleva a la práctica el objetivo de la **Estrategia de Datos**[40], para que las empresas sean más capaces de innovar y competir sobre la base de los valores de la UE y el principio de **libre circulación de datos en el mercado interior**. También coincide con el **Plan de acción en materia de propiedad intelectual**[41], en el que la Comisión se comprometió a revisar la Directiva sobre bases de datos.

La presente propuesta también debe cumplir los principios del Plan de Acción del Pilar Europeo de Derechos Sociales (PEDS)[42] y los requisitos de accesibilidad de la Directiva (UE) 2019/882, sobre los requisitos de accesibilidad de los productos y servicios[43].

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La base jurídica de la presente propuesta es el artículo 114 del Tratado de Funcionamiento de la Unión Europea, cuyo objetivo es el establecimiento y el funcionamiento del mercado interior reforzando las medidas de aproximación de las normas nacionales.

La presente propuesta pretende impulsar la realización del mercado interior de datos, en el que los datos del sector público, las empresas y los particulares se utilicen de la mejor manera posible, respetando al mismo tiempo los derechos en relación con dichos datos y las inversiones realizadas para recopilarlos. Las disposiciones relativas al cambio entre servicios de tratamiento de datos tienen por objeto establecer unas condiciones de mercado equitativas y competitivas para el mercado interior en la nube, el borde y los servicios relacionados.

La protección de los datos comerciales confidenciales y los secretos comerciales es un aspecto importante del buen funcionamiento del mercado interior, como ocurre en otros contextos en los que se intercambian servicios y se comercializan bienes. La presente propuesta garantiza el respeto de los secretos comerciales en el contexto del uso de datos entre empresas o por parte de los consumidores. La iniciativa permitirá a la Unión beneficiarse de la escala del mercado interior, ya que los productos o servicios relacionados se desarrollan a menudo utilizando datos de diferentes Estados miembros, que posteriormente se comercializan en toda la Unión.

Algunos Estados miembros han adoptado medidas legislativas para abordar los problemas descritos anteriormente, en las relaciones entre empresas y entre empresas y administraciones,

---

37 Digitalización en beneficio del medio ambiente, 11 de diciembre de 2020, Conclusiones del Consejo sobre el nuevo Plan de acción para la economía circular, 11 de diciembre de 2020, Conclusiones del Consejo acerca de la estrategia sobre la biodiversidad de aquí a 2030, 16 de octubre de 2020, Conclusiones sobre la mejora de la calidad del aire, 5 de marzo de 2020

38 Emergencia climática y medioambiental — jueves, 28 de noviembre de 2019 (europa.eu)

39 COM/2021/350 final.

40 COM/2020/66 final.

41 COM/2020/760 final.

42 COM/2021/102 final.

43 DO L 151 de 7.6.2019.

mientras que otros no lo han hecho. Esto puede dar lugar a una fragmentación legislativa en el mercado interior y a diferentes normas y prácticas en toda la Unión, así como a costes conexos por parte de las empresas, que tendrían que cumplir regímenes diferentes. Por lo tanto, es importante garantizar que las medidas propuestas se apliquen de manera coherente en todos los Estados miembros.

- **Subsidiariedad (en el caso de competencia no exclusiva)**

Dado el carácter transfronterizo del uso de los datos y los numerosos ámbitos en los que impacta la Ley de Datos, las cuestiones que trata la presente propuesta no pueden abordarse eficazmente a nivel de los Estados miembros. Debe evitarse la fragmentación derivada de las diferencias entre las normas nacionales, ya que daría lugar a costes de transacción más elevados, falta de transparencia, inseguridad jurídica y foros de conveniencia indeseables. Esto es especialmente importante en todas las situaciones que afectan a los datos en las relaciones entre empresas, incluidas las condiciones contractuales equitativas y las obligaciones de los fabricantes de productos o servicios relacionados de la internet de las cosas, las cuales requieren una homogeneidad del marco en toda la Unión.

Una evaluación de los aspectos transfronterizos de los flujos de datos en el ámbito del intercambio de datos entre empresas y administraciones también demuestra la necesidad de actuar a escala de la Unión. Muchos agentes privados que poseen datos pertinentes son empresas multinacionales, que no deberían tener que enfrentarse a un régimen jurídico fragmentado.

Los servicios de computación en la nube rara vez se ofrecen en un solo Estado miembro. En consonancia con el RGPD y el Reglamento sobre la libre circulación de datos no personales, que permite a los consumidores y a las empresas tratar datos personales y no personales en cualquier lugar de la Unión que deseen, el tratamiento transfronterizo de datos dentro de la Unión es esencial para llevar a cabo actividades empresariales en el mercado interior. Por lo tanto, es fundamental que las disposiciones sobre el cambio de servicios de tratamiento de datos se apliquen a escala de la Unión, a fin de evitar una fragmentación perjudicial en un mercado de servicios de tratamiento de datos que, por lo demás, está unificado.

Solo una acción común a nivel de la Unión puede permitir la consecución de los objetivos establecidos en la presente propuesta, incluida la creación de unas condiciones de competencia equitativas e innovadoras para las empresas basadas en los datos y la capacitación de los ciudadanos. Esta acción común es un firme paso adelante hacia la consecución del objetivo de crear un auténtico mercado interior de datos.

- **Proporcionalidad**

La presente propuesta establece un equilibrio entre los derechos e intereses de las partes interesadas afectadas y el objetivo general de facilitar un uso más amplio de los datos a un extenso abanico de agentes. Crea un marco facilitador que no va más allá de lo necesario para alcanzar los objetivos. Aborda los obstáculos existentes para una materialización más completa del valor potencial de los datos entre las empresas, los consumidores y el sector público. También establece un marco para futuras normas sectoriales a fin de evitar la fragmentación y la incertidumbre jurídica. Aclara los derechos existentes y, en caso necesario, otorga derechos de acceso a los datos, contribuyendo así al desarrollo de un mercado interior para el intercambio de datos. La iniciativa ofrece una gran flexibilidad para su aplicación a nivel sectorial.

La presente propuesta generará costes financieros y administrativos, que deberán ser

asumidos principalmente por las autoridades nacionales, los fabricantes y los proveedores de servicios, de modo que cumplan las obligaciones establecidas en el presente Reglamento. Con todo, la exploración de distintas opciones y de los costes y beneficios previstos ha dado lugar a un diseño equilibrado del instrumento. De igual modo, los costes para los usuarios y los titulares de datos se compensarán con el valor que se derivará de la mayor disponibilidad y utilización de datos y de la introducción de servicios innovadores en el mercado.

- **Elección del instrumento**

Se ha elegido un reglamento porque es el mejor mecanismo para cumplir los objetivos políticos más amplios: garantizar que todas las empresas de la Unión estén en condiciones de innovar y competir, que los consumidores estén mejor capacitados para asumir el control de sus datos, y que las instituciones, órganos y organismos de la Unión estén mejor equipados para hacer frente a los principales retos políticos, incluidas las emergencias públicas. Habida cuenta del objetivo de armonización global que persigue la propuesta, es necesario un reglamento para garantizar seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, ofrecer a las personas físicas y jurídicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles, garantizar la coherencia en la aplicación de la legislación en todos los Estados miembros, así como una cooperación eficaz entre las autoridades competentes de los diferentes Estados miembros.

La propuesta reforzará el mercado interior de datos al aumentar la seguridad jurídica y garantizar un marco jurídico uniforme, horizontal y coherente.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Evaluaciones *ex post* / controles de la adecuación de la legislación existente**

La presente propuesta se basa parcialmente en la última evaluación de la Directiva sobre bases de datos y en el estudio de la Comisión que apoya la revisión de la Directiva[44]. La Directiva sobre bases de datos introdujo, entre otras cosas, un derecho *sui generis* específico para proteger las bases de datos si el productor de una base de datos invierte sustancialmente en la obtención, verificación y presentación de los datos. Desde su primera adopción, la Directiva se ha evaluado en dos ocasiones. Ambas evaluaciones se han complementado con comunicaciones de la Comisión sobre un marco político para la economía de los datos[45].

El Tribunal de Justicia de la Unión Europea ha profundizado en la cuestión de las inversiones sustanciales en una base de datos, aclarando que el derecho *sui generis* tiene por objeto proteger las inversiones en la recopilación de datos y no en su creación[46] como subproducto de otra actividad económica. Sin embargo, persiste la incertidumbre en cuanto a la aplicación accidental o no intencionada del derecho *sui generis* a las bases de datos que contienen datos generados por máquinas, es decir, datos generados u obtenidos a partir del uso de productos o servicios conexos. Es necesario equilibrar los objetivos políticos de la protección de la propiedad intelectual e industrial de dichas bases de datos en el contexto de la economía de

[44] COM/2017/09 final. SWD(2018) 146 final, sección 5.4.2.; Estudio de apoyo a una evaluación de impacto para la revisión de la Directiva sobre bases de datos.

[45] COM/2017/09 final; COM/2020/66 final; COM/2020/760 final.

[46] Fixtures Marketing Ltd v. Oy Veikkaus Ab (C-46/02, 9/11/2004), Fixtures Marketing Ltd v. Svenska Spel Ab (C-338/02, 9/11/2004) British Horseracing Board Ltd v. William Hill (C-203/02, 9/11/2004) Fixtures Marketing Ltd v. OPAP (C-444/02, 9/11/2004).

los datos, en la que la exclusividad de los datos como bien no rival se considera, en general, un obstáculo para la innovación. Para garantizar la coherencia con las intervenciones reguladoras presentadas en la presente propuesta, la intervención sobre el derecho *sui generis* aborda específicamente la aplicación problemática del derecho *sui generis* en el contexto de la internet de las cosas. Además, la Comisión también está preparando actualmente la evaluación del Reglamento (UE) 2018/1807, prevista para noviembre de 2022. Los informes iniciales de contratistas externos han mostrado el efecto limitado de los códigos de conducta SWIPO sobre el cambio de proveedor en la nube.

- **Consultas con las partes interesadas**

Durante el mandato de la anterior Comisión se inició un trabajo exhaustivo para identificar los problemas que impiden a la Unión aprovechar todo el potencial de la innovación basada en los datos en la economía. La propuesta se basa en consultas anteriores, como la consulta pública de 2017 en apoyo de la Comunicación de la Comisión «*Construir una economía de los datos*»[47], la consulta pública de 2017 sobre la evaluación de la Directiva sobre bases de datos, la consulta pública de 2018 sobre la revisión de la Directiva relativa a la reutilización de la información del sector público, la consulta de 2018 del panel de pymes sobre los principios y orientaciones para el intercambio de datos entre empresas, y la consulta abierta en línea de la Comisión sobre la Estrategia de Datos[48] de febrero a mayo de 2020.

El 28 de mayo de 2021 se publicó una evaluación inicial de impacto en el portal «Legislar mejor», que quedó abierta a comentarios durante cuatro semanas. La Comisión recibió 91 contribuciones en el portal «Legislar mejor»[49], en su mayoría de empresas.

Posteriormente, el 3 de junio de 2021 se publicó una consulta pública en línea sobre la Ley de Datos, que concluyó el 3 de septiembre de 2021. A través de secciones y preguntas específicas, la consulta abordó los puntos cubiertos por la iniciativa. Estaba dirigida a todas las categorías de partes interesadas, con la intención de recabar información sobre el intercambio de datos, el acceso y el uso en las relaciones entre empresas y entre empresas y administraciones, la capacitación de los consumidores y la portabilidad, el papel potencial de medidas técnicas como los contratos inteligentes, la capacidad del usuario para cambiar de servicios en la nube, los derechos de propiedad intelectual (es decir, la protección de las bases de datos) y las salvaguardias para los datos no personales en el contexto internacional. Tras realizar un análisis en profundidad de las respuestas, la Comisión publicó un informe de síntesis en su sitio web[50].

En total, se recibieron 449 contribuciones de 32 países. El mayor número de contribuciones se recibió de las entidades empresariales, con 122 asociaciones empresariales y 105 empresas/organizaciones empresariales. Además, 100 encuestados eran autoridades públicas y 58 eran particulares. En líneas generales, las respuestas confirmaron que existen multitud de obstáculos para el intercambio eficaz y eficiente de datos en todos los tipos de relaciones.

En las relaciones entre empresas, a pesar de que el intercambio de datos en este contexto es una práctica común, los encuestados que habían experimentado dificultades mencionaron distintos obstáculos como, por ejemplo, de carácter técnico (formatos, falta de normas: 69 %); de denegación total de acceso no vinculada a problemas de competencia (55 %) o de abuso de un desequilibrio contractual (44 %). En cuanto a las cuestiones contractuales, casi la mitad de

47 COM/2017/09 final.

48 Comisión Europea (2020): *Resultado de la consulta en línea sobre la Estrategia Europea de Datos.*

49 *Página web* de la Comisión Europea: *Ley de datos y modificación de las normas sobre la protección jurídica de las bases de datos.*

50 Comisión Europea (2021). *Consulta pública sobre la Ley de datos: informe de síntesis*.

los encuestados se mostraron a favor de un «control de abusividad» (46 %), mientras que más del doble de ellos no estaban a favor (21 %). Las pymes mostraron un fuerte apoyo (50 %) al control de abusividad, y un número significativo de grandes empresas también se manifestó a favor (41 %). Del mismo modo, el 46 % de las partes interesadas de todos los sectores mostraron su apoyo a normas generales de acceso basadas en condiciones justas, razonables y no discriminatorias (46 %). El 60 % de los encuestados, en particular las pymes y las microempresas (78 %), coincidieron en que las condiciones contractuales tipo podrían contribuir a un mayor intercambio de datos. El 70 % de las partes interesadas expresó la opinión de que existe un problema de equidad con los datos generados en el contexto de la internet de las cosas, y de que los fabricantes de productos o servicios relacionados no deben poder decidir unilateralmente qué ocurre con los datos generados por dichos productos. El 79 % de los encuestados consideró que los contratos inteligentes podrían ser una herramienta eficaz para poner técnicamente en marcha el acceso a los datos y su utilización en el contexto de los datos cogenerados de la internet de las cosas.

Según los encuestados, los principales factores que impiden el intercambio de datos entre empresas y administraciones son los obstáculos y la inseguridad jurídica, los desincentivos comerciales y la falta de infraestructuras adecuadas. Casi todas las autoridades públicas consideran que es necesaria una acción (de la Unión o de los Estados miembros) para el intercambio de datos entre empresas, frente al 80 % de las instituciones académicas o de investigación y el 38 % de las empresas y de las organizaciones y asociaciones empresariales. Una clara mayoría de las partes interesadas (en particular, los ciudadanos y las administraciones públicas) también expresó la opinión de que el intercambio de datos entre empresas y administraciones debería ser obligatorio, con salvaguardias claras para los casos de uso específicos con un interés público claro en situaciones de emergencia y a efectos de gestión de crisis, para las estadísticas oficiales, para la protección del medio ambiente y para una sociedad más sana en general.

Los encuestados también confirmaron la utilidad de que las empresas usuarias de servicios de computación en la nube tengan derecho a cambiar de proveedor. En cuanto a las salvaguardias para los datos no personales en contextos internacionales, el 76 % de los encuestados percibe el posible acceso a los datos por parte de autoridades extranjeras sobre la base de legislación extranjera como un riesgo para su organización, y el 19 % indica que se trata de un riesgo importante.

- **Obtención y uso de asesoramiento especializado**

La propuesta fue sustentada por varios estudios, talleres y otras aportaciones de expertos:

– Un **estudio en apoyo de la presente evaluación de impacto sobre la mejora del uso de los datos en Europa**, incluidas entrevistas con determinadas partes interesadas. Se celebraron dos talleres intersectoriales sobre el intercambio de datos entre empresas y entre empresas y las administraciones públicas, y un taller de validación final organizado en la primavera de 2021.

– El **estudio sobre las cláusulas contractuales tipo, el control de la equidad en el intercambio de datos y en los contratos en la nube y sobre los derechos de acceso a los datos**, evaluó, en particular, los aspectos de equidad en las relaciones de intercambio de datos entre empresas e incluyó entrevistas específicas con las partes interesadas y un taller de validación.

– Un **estudio sobre el perjuicio económico derivado de los contratos abusivos y no equilibrados en el ámbito de la computación en la nube**. En este caso se incluía

una encuesta en línea de una muestra de pymes y empresas emergentes que utilizan la computación en la nube para llevar a cabo sus actividades.

– Un **estudio sobre el cambio de proveedor de servicios en la nube**, que incluyó un taller intersectorial en el segundo trimestre de 2017.

– Un **estudio en apoyo de la revisión de la Directiva sobre bases de datos**, acompañado de entrevistas con determinadas partes interesadas. Fue útil para la Comisión en la preparación de la presente evaluación de impacto para acompañar la revisión de la Directiva sobre bases de datos, en el contexto de la Ley de Datos y en la consecución de los objetivos interrelacionados

– **Apoyo metodológico a la evaluación de impacto sobre el uso de datos de titularidad privada en las estadísticas oficiales**. Este ejercicio contribuye a la evaluación del impacto de la reutilización de datos entre las empresas y las administraciones en las estadísticas oficiales mediante el desarrollo de un enfoque metodológico y la descripción de los beneficios y costes de la reutilización de los datos y de los casos de uso seleccionados para diferentes ámbitos estadísticos y diferentes tipos de datos del sector privado. Además, contribuye a la investigación y las deliberaciones en curso para comprender mejor el intercambio de los datos entre empresas y administraciones públicas.

– **Seminarios en línea sobre plataformas de datos personales y plataformas de datos industriales**. Se organizaron tres seminarios en línea los días 6, 7 y 8 de mayo de 2020, que reunieron los proyectos de plataformas de datos relevantes de la asociación público-privada Big Data Value.

– **Informe del Grupo de Expertos de alto nivel sobre intercambio de datos entre empresas y administraciones públicas.** El informe ofrece un análisis de los problemas que plantea el intercambio de datos entre empresas y administraciones públicas en la Unión y ofrece una serie de recomendaciones para garantizar un intercambio de datos de carácter modulable, responsable y sostenible en aras del interés público. Además de la recomendación a la Comisión de estudiar la posibilidad de elaborar un marco jurídico en este ámbito, presenta varias formas de alentar a las empresas privadas a compartir sus datos. Entre ellas, figuran los incentivos monetarios y no monetarios (por ejemplo, los incentivos fiscales), la inversión de fondos públicos para apoyar el desarrollo de herramientas técnicas de confianza y los sistemas de reconocimiento para el intercambio de datos.

– **Taller sobre etiquetas/certificación de proveedores de soluciones técnicas para el intercambio de datos**. Alrededor de un centenar de participantes entre empresas (incluidas pymes), instituciones europeas y universidades asistieron a este seminario en línea el 12 de mayo de 2020. El objetivo era examinar si un sistema de etiquetado o de certificación podría impulsar la aceptación por parte de los intermediarios de datos, aumentando la confianza en el ecosistema de datos.

– **Diez talleres organizados entre julio y noviembre de 2019 contaron con la participación de más de 300 partes interesadas y abarcaron diferentes sectores**. Los talleres debatieron cómo la organización del **intercambio de datos en determinados ámbitos**, como el medio ambiente, la agricultura, la energía o la asistencia sanitaria, podría beneficiar a la sociedad en su conjunto, ayudando a los agentes públicos a diseñar mejores políticas y mejorar los servicios públicos, así como a agentes privados para producir servicios que contribuyan a hacer frente a los retos sociales.

– **Consulta al panel de pymes.** Esta consulta al panel, organizada entre octubre de 2018 y enero de 2019, tenía como finalidad recabar la opinión de las pymes con respecto a los principios del intercambio de datos entre empresas y orientaciones publicados en la Comunicación «*Hacia un espacio común europeo de datos*», que acompaña al documento de trabajo de los servicios de la Comisión de 25 de abril de 2018[51].

– **El último Eurobarómetro sobre el impacto de la digitalización.** Esta encuesta general sobre la vida cotidiana de los europeos incluye preguntas sobre el control que tienen las personas de sus datos personales y de su difusión. Se publicó el 5 de marzo de 2020, y ofrece información sobre la predisposición de los ciudadanos europeos a compartir información personal y bajo qué condiciones.

– **El dictamen del Supervisor Europeo de Protección de Datos** (SEPD) sobre la Estrategia Europea de Datos[52]. El 16 de junio de 2020, el SEPD adoptó el Dictamen 3/2020 sobre la Estrategia Europea de Datos. El SEPD acogió con satisfacción la estrategia, y consideró su aplicación como una oportunidad para ejemplarizar un modelo alternativo de economía de los datos.

• **Evaluación de impacto**

La propuesta va acompañada de una evaluación de impacto[53], presentada al Comité de Control Reglamentario (CCR) el 29 de septiembre de 2021 y el 13 de diciembre de 2021. El 21 de enero de 2022, el Comité emitió un dictamen positivo con reservas.

• **Adecuación regulatoria y simplificación**

Al aclarar que el derecho *sui generis* previsto en la Directiva sobre bases de datos (Directiva 96/9/CE) no se aplica a las bases de datos que contengan datos obtenidos o generados por el uso de un producto o un servicio relacionado, la propuesta garantiza que el derecho *sui generis* no interferirá con los derechos de las empresas y los consumidores a acceder a los datos y utilizarlos y a compartir los datos en aplicación del presente Reglamento. Esta aclaración ajustará la aplicación del derecho *sui generis* al objetivo de la propuesta legislativa, y tendrá un impacto positivo en la aplicación uniforme de las normas en el mercado interior y en la economía de los datos.

Favoreciendo el acceso y utilización de los datos, la Ley de Datos debería reducir las cargas, tanto en el sector público como para las empresas, principalmente por la reducción de los costes de transacción y el aumento de la eficiencia. En línea con el principio de compensación de cargas administrativas[54], que tiene como objetivo minimizar, para los ciudadanos y las empresas, las cargas relacionadas con las implicaciones y los costes de la aplicación de la legislación, la carga administrativa neta estimada de la Ley de Datos, basada en la evaluación de impacto, tiene en cuenta beneficios que probablemente no solo compensen, sino que superen con creces los costes administrativos asociados.

• **Derechos fundamentales**

La propuesta se ajusta a la legislación de la Unión sobre la protección de los datos personales y la privacidad de las comunicaciones y los equipos terminales, y prevé salvaguardias adicionales en lo que respecta al acceso a los datos personales, incluidos los casos sujetos a

51 COM/2018/232 final. SWD(2018) 125 final, de 25 de abril de 2018.
52 Dictamen 3/2020 del SEPD sobre la Estrategia Europea de Datos.
53 **[Añádanse los enlaces al documento final y al resumen].**
54 SWD(2021) 305 final.

derechos de propiedad intelectual.

En el capítulo II, se refuerza el ya elevado nivel de protección del consumidor con un nuevo derecho de acceso a los datos generados en situaciones que anteriormente no estaban cubiertas por la legislación comunitaria. El derecho a utilizar y disponer de los bienes adquiridos legalmente se refuerza con un derecho de acceso a los datos generados por el uso de un objeto de la internet de las cosas. De esta forma, el propietario puede beneficiarse de una mejor experiencia de usuario y de una gama más amplia de, por ejemplo, servicios de reparación y mantenimiento. En el contexto de la protección de los consumidores, los derechos de los menores, en cuanto consumidores vulnerables, merecen una atención específica, y las normas de la Ley de Datos contribuirán a aportar claridad con respecto al acceso a los datos y las situaciones de utilización.

El derecho de acceso de terceros a los datos de la internet de las cosas a petición del usuario limita la libertad de empresa y la libertad contractual del fabricante o diseñador de un producto o servicio relacionado. Esta limitación se justifica en cuanto refuerza la protección de los consumidores, en especial al promover sus intereses económicos. Normalmente, el fabricante o diseñador de un producto o servicio relacionado tiene el control exclusivo del uso de los datos generados por el uso de un producto o servicio relacionado, por lo que contribuye a los efectos de dependencia y obstaculiza la entrada en el mercado de los agentes que ofrecen servicios posventa. El derecho de acceso a los datos de la internet de las cosas toma en cuenta esta situación al capacitar a los consumidores que utilizan productos o servicios relacionados para que puedan controlar de manera significativa cómo se utilizan los datos generados por su uso del producto o del servicio relacionado, y permitiendo la innovación por parte de más agentes del mercado. Por lo tanto, los consumidores pueden beneficiarse de una mayor variedad de servicios posventa, como la reparación y el mantenimiento, y ya no dependerán únicamente de los servicios del fabricante. La propuesta facilita la portabilidad de los datos del usuario a terceros y permite una oferta competitiva de servicios posventa, así como una innovación basada en datos más amplia y el desarrollo de productos o servicios no relacionados con los adquiridos o suscritos inicialmente por el usuario.

La limitación de la libertad de contratación y de empresa del fabricante o diseñador es proporcionada y se ve atenuada por la capacidad no afectada del fabricante o diseñador de utilizar también los datos, en la medida en que esté en consonancia con la legislación aplicable y el acuerdo con el usuario. Además, el fabricante o diseñador también se beneficiará del derecho a exigir una compensación por permitir el acceso de terceros. El derecho de acceso se entiende sin perjuicio de los derechos de acceso y portabilidad existentes para los interesados en virtud del RGPD. Las salvaguardias adicionales garantizan un uso proporcionado de los datos por parte de un tercero.

En el capítulo IV, un sistema justo y eficaz de protección contra las cláusulas contractuales abusivas en el intercambio de datos permitirá que las microempresas y las pequeñas y medianas empresas puedan llevar a cabo su actividad empresarial. Esta disposición restringe la libertad contractual de las empresas que recaen dentro del ámbito de aplicación de manera limitada, ya que solo se aplica a las cláusulas contractuales abusivas relativas al acceso a los datos y su utilización impuestas unilateralmente por una parte contratante a una microempresa, o una pequeña o mediana empresa. La disposición se justifica en cuanto las pymes suelen encontrarse en una posición negociadora más débil y a menudo no tienen más opción que aceptar cláusulas contractuales de «lo tomas o lo dejas». La libertad contractual no se ve afectada en gran medida, ya que solo se invalidan las cláusulas excesivas y abusivas, y el contrato celebrado, en la medida de lo posible, sigue siendo válido sin las cláusulas abusivas. Además, las partes todavía pueden negociar individualmente una cláusula

contractual específica[55].

En el capítulo V, las disposiciones relativas al intercambio de datos entre empresas y administraciones públicas por motivos excepcionales mejorarán la capacidad de las autoridades públicas de tomar decisiones en pro del bien común, como en el caso de la respuesta, prevención o ayuda en la recuperación tras una emergencia pública. El sector privado también se beneficia de la racionalización de los procedimientos de solicitud de datos.

En el capítulo VI, las disposiciones relativas al cambio de proveedor de servicios de tratamiento de datos refuerzan la posición de los clientes empresariales y salvaguardan su decisión de cambiar de proveedor. La limitación del derecho de empresa de los proveedores de servicios de tratamiento de datos se justifica en cuanto las nuevas normas abordan la cuestión del efecto de dependencia en el mercado de los servicios en la nube y el borde, y mejoran las posibilidades de elección de los servicios de tratamiento de datos por parte de los particulares y los usuarios empresariales.

En el capítulo X, la intervención en el derecho *sui generis* de la Directiva sobre bases de datos no limita la protección de la propiedad intelectual. Contribuye más bien a la seguridad jurídica en los casos en que la protección del derecho *sui generis* no estaba clara anteriormente.

4. REPERCUSIONES PRESUPUESTARIAS

La presente iniciativa no conlleva repercusión presupuestaria alguna.

5. OTROS ELEMENTOS

- **Planes de ejecución y modalidades de seguimiento, evaluación e información**

A nivel sectorial y macroeconómico, el estudio de seguimiento del mercado de datos en curso ayudará a supervisar el impacto económico de la presente propuesta en el crecimiento del mercado de datos en la Unión.

El impacto en las pymes, es decir, su percepción de los problemas relacionados con el acceso a los datos y su utilización, se evaluará mediante una consulta al panel de pymes cinco años después de la adopción de la Ley de Datos.

Habida cuenta del papel central que desempeñan los espacios comunes europeos de datos en la aplicación de la estrategia europea de datos, muchos de los efectos de esta iniciativa serán objeto de seguimiento a través de los espacios de datos sectoriales y de la información recopilada por el Centro de Apoyo a los espacios de datos que se financiará en el marco del programa Europa Digital. La interacción periódica entre los servicios de la Comisión, el Centro de Ayuda y el Comité Europeo de Innovación en materia de Datos (que se establecerá tras la entrada en vigor de la Ley de Gobernanza) permitirá recabar información fiable que permita evaluar los progresos realizados.

Por último, cuatro años después de la adopción de la Ley de Datos se llevará a cabo una evaluación para valorar la iniciativa y preparar nuevas medidas en caso necesario.

[55] Para más explicaciones sobre el control de abusividad y el principio de libertad contractual, véase la evaluación de impacto, anexo 11.

- **Explicación detallada de las disposiciones específicas de la propuesta**

El capítulo I define el objeto y el ámbito de aplicación del Reglamento y establece las definiciones utilizadas a lo largo del acto.

El capítulo II aumenta la seguridad jurídica para que los consumidores y las empresas accedan a los datos generados por los productos o servicios relacionados de su propiedad, o que alquilan o arrendan. Los fabricantes y diseñadores deben concebir los productos de manera que los datos sean fácilmente accesibles por defecto, y deberán ser transparentes en cuanto a qué datos serán accesibles y cómo acceder a ellos. Las disposiciones de este capítulo no afectarán a la posibilidad de que los fabricantes accedan a los datos de los productos o servicios relacionados que ofrecen y los utilicen, cuando así se acuerde con el usuario. El titular de los datos tiene la obligación de ponerlos a disposición de terceros a petición del usuario. Los usuarios tendrán derecho a autorizar al titular de datos para que den acceso a los datos a terceros proveedores de servicios como, por ejemplo, los proveedores de servicios posventa. Las microempresas y las pequeñas empresas quedan exentas de estas obligaciones.

El capítulo III establece las normas generales aplicables a las obligaciones de puesta a disposición de los datos. Cuando un titular de datos esté obligado a poner datos a disposición de un destinatario de datos en virtud del capítulo II o de otras disposiciones del Derecho de la Unión o de los Estados miembros, el marco general aclara las condiciones en las que se facilitan los datos y la compensación por la puesta a disposición. Cualquier condición deberá ser justa y no discriminatoria, y toda compensación deberá ser razonable, sin impedir que otras disposiciones del Derecho de la Unión o de la legislación nacional por la que se aplique el Derecho de la Unión excluyan la compensación o prevean una compensación inferior por la puesta a disposición de los datos. Cualquier compensación establecida para las pymes no podrá superar los costes incurridos por la puesta a disposición de los datos, a menos que se especifique lo contrario en la legislación sectorial. Los órganos de resolución de litigios certificados por los Estados miembros podrán ayudar a las partes que no estén de acuerdo sobre la indemnización o las condiciones para llegar a un acuerdo.

El capítulo IV aborda el carácter abusivo de las cláusulas contractuales de los contratos de intercambio de datos entre empresas, en situaciones en las que una parte impone unilateralmente una cláusula contractual a una microempresa, o una pequeña o mediana empresa. Este capítulo garantiza que los acuerdos contractuales sobre el acceso y utilización de datos no se aprovechan de los desequilibrios en el poder de negociación entre las partes contratantes. El instrumento del control de abusividad incluye una disposición general que define el carácter abusivo de una cláusula contractual de intercambio de datos, acompañada de una lista de cláusulas que son siempre abusivas o se presume que son abusivas. En las situaciones de desigualdad de poder de negociación, este control protege a la parte más débil a fin de evitar contratos abusivos, ya que dicho carácter abusivo impide el uso de los datos por ambas partes contratantes. De esta forma, las disposiciones garantizan un reparto más justo del valor en la economía de los datos[56]. Las cláusulas contractuales tipo recomendadas por la Comisión pueden ayudar a las partes comerciales a celebrar contratos basados en condiciones equitativas.

El capítulo V crea un marco armonizado para la utilización, por parte de los organismos del sector público y las instituciones, órganos y organismos de la Unión, de los datos que obren en poder de las empresas en situaciones en las que exista una necesidad excepcional de obtener los datos solicitados. El marco se basa en la obligación de poner a disposición los

[56] Para más explicaciones sobre el control de abusividad y su funcionamiento en la práctica, véase la evaluación de impacto, anexo 11.

datos y se aplicaría exclusivamente en caso de emergencia pública o en situaciones en las que los organismos públicos tengan una necesidad excepcional de utilizar determinados datos que no puedan obtenerse en el mercado, mediante la promulgación oportuna de nueva legislación o a través de obligaciones de información existentes. En caso de necesidad excepcional para responder a emergencias públicas, como emergencias de salud pública, o catástrofes naturales o provocadas por el ser humano de carácter grave, los datos se pondrán a disposición de forma gratuita. En otros casos de necesidad excepcional, en particular para prevenir o ayudar a la recuperación tras una emergencia pública, el titular de los datos que los ponga a disposición debe tener derecho a una compensación que incluya los costes relacionados con la puesta a disposición de los datos pertinentes más un margen razonable. Para garantizar que no se abusa del derecho a solicitar datos y que el sector público se hace responsable de su utilización, las solicitudes de datos deben ser proporcionadas, indicar claramente la finalidad que debe alcanzarse y respetar los intereses de la empresa que los pone a disposición. Las autoridades competentes garantizarían la transparencia y la disponibilidad pública de todas las solicitudes. También se encargarían de tramitar las reclamaciones resultantes.

El capítulo VI introduce requisitos reglamentarios mínimos de carácter contractual, comercial y técnico, impuestos a los proveedores de servicios de tratamiento de datos en la nube, el borde y otros servicios de tratamiento de datos, a fin de permitir el cambio entre dichos servicios. En particular, la propuesta garantiza que los clientes mantengan la equivalencia funcional (un nivel mínimo de funcionalidad) del servicio una vez que hayan cambiado a otro proveedor de servicios. La propuesta incluye una excepción para la inviabilidad técnica, pero impone la carga de la prueba en estos casos al proveedor de servicios. La propuesta no exige normas o interfaces técnicas específicas. Sin embargo, exige que los servicios sean compatibles con las normas europeas o las especificaciones técnicas de interoperabilidad abiertas, cuando existan.

El capítulo VII aborda el acceso ilícito de terceros a los datos no personales conservados en la Unión mediante servicios de tratamiento de datos ofrecidos en el mercado de la Unión. La propuesta no afecta a la base jurídica de las solicitudes de acceso a los datos que obren en poder de ciudadanos o empresas de la UE, y se entiende sin perjuicio del marco de protección de datos y privacidad de la Unión. Ofrece salvaguardias específicas, ya que los proveedores tienen que adoptar todas las medidas técnicas, jurídicas y organizativas razonables para evitar un acceso que entre en conflicto con las obligaciones concurrentes de proteger dichos datos en virtud del Derecho de la Unión, a menos que se cumplan condiciones estrictas. El Reglamento cumple los compromisos internacionales de la Unión en el marco de la OMC y en los acuerdos comerciales bilaterales.

El capítulo VIII establece los requisitos esenciales en relación con la interoperabilidad para los operadores de espacios de datos y proveedores de servicios de tratamiento de datos, así como los requisitos esenciales para los contratos inteligentes. Este capítulo también permite que las especificaciones de interoperabilidad abiertas y las normas europeas para la interoperabilidad de los servicios de tratamiento de datos promuevan un entorno de proveedores múltiples en la nube sin interrupciones.

El capítulo IX establece el marco de aplicación y cumplimiento de las autoridades competentes de cada Estado miembro, incluido un mecanismo de denuncia. La Comisión recomendará cláusulas contractuales tipo voluntarias sobre el acceso a los datos y su utilización. Se aplicarán sanciones en caso de infracción del presente Reglamento.

El capítulo X contiene una disposición por la cual el derecho *sui generis* establecido en la Directiva 96/9/CE no se aplicará a las bases de datos que contengan datos obtenidos o

generados por el uso de un producto o un servicio relacionado y obstaculice el ejercicio, por parte de los usuarios, del derecho de acceder a los datos y utilizarlos de conformidad con el artículo 4 del presente Reglamento, ni del derecho a compartir esos datos con terceros de conformidad con el artículo 5 del presente Reglamento.

El capítulo XI permite a la Comisión adoptar actos delegados para introducir un mecanismo de supervisión de las tasas por cambio de proveedor de servicios de tratamiento de datos, para especificar en mayor medida los requisitos esenciales relativos a la interoperabilidad y para publicar la referencia de las especificaciones de interoperabilidad abiertas y las normas europeas para la interoperabilidad de los servicios de tratamiento de datos. También prevé el procedimiento de comité para adoptar actos de ejecución a fin de facilitar la adopción de especificaciones comunes de interoperabilidad y contratos inteligentes cuando no existan normas armonizadas o estas sean insuficientes para garantizar la conformidad con los requisitos esenciales. La propuesta también aclara la relación con otros actos jurídicos de la Unión que regulan los derechos y las obligaciones en materia de intercambio de datos.

2022/0047 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

sobre normas armonizadas para un acceso justo a los datos y su utilización (Ley de Datos)

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[57],

Visto el dictamen del Comité de las Regiones[58],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) En los últimos años, las tecnologías basadas en los datos han tenido efectos transformadores en todos los sectores de la economía. En particular, la proliferación de productos conectados a la internet de las cosas ha aumentado el volumen y el valor potencial de los datos para los consumidores, las empresas y la sociedad. Los datos interoperables y de alta calidad de diferentes ámbitos incrementan la competitividad y la innovación y garantizan un crecimiento económico sostenible. El mismo conjunto de datos puede utilizarse y reutilizarse para diversos fines y de modo ilimitado, sin pérdida de calidad o cantidad.

(2) Los obstáculos al intercambio de datos impiden una asignación óptima de los datos en beneficio de la sociedad. Estos obstáculos incluyen la falta de incentivos para que los titulares de datos suscriban voluntariamente acuerdos sobre el intercambio de datos, la incertidumbre sobre los derechos y las obligaciones en relación con los datos, los costes de contratación y aplicación de interfaces técnicas, el elevado nivel de fragmentación de la información en los silos de datos, la mala gestión de metadatos, la ausencia de normas para la interoperabilidad semántica y técnica, los cuellos de botella que impiden el acceso a los datos, la falta de prácticas comunes para el intercambio de datos y el abuso de los desequilibrios contractuales en relación con el acceso a los datos y su utilización.

(3) En sectores caracterizados por la presencia de microempresas y pequeñas y medianas empresas, a menudo escasean las capacidades y competencias digitales necesarias para recopilar, analizar y utilizar datos, y el acceso a estos queda limitado con frecuencia

[57] DO C […] de […], p. […].
[58] DO C […] de […], p. […].

cuando un único agente los conserva en el sistema o debido a la falta de interoperabilidad entre datos, entre servicios de datos o a través de las fronteras.

(4) Con el fin de responder a las necesidades de la economía digital y eliminar los obstáculos al buen funcionamiento del mercado interior de datos, es necesario establecer un marco armonizado que especifique quién, aparte del fabricante u otro titular de datos, tiene derecho a acceder a los datos generados por los productos o servicios relacionados, en qué condiciones y sobre qué base. Por consiguiente, los Estados miembros no deben adoptar ni mantener requisitos nacionales adicionales sobre las cuestiones que entran en el ámbito de aplicación del presente Reglamento, salvo que así se disponga explícitamente en él, ya que ello afectaría a su aplicación directa y uniforme.

(5) El presente Reglamento garantiza que los usuarios de un producto o servicio relacionado en la Unión puedan acceder oportunamente a los datos generados por el uso de dicho producto o servicio relacionado y que puedan utilizarlos e incluso compartirlos con terceros de su elección. El presente Reglamento impone al titular de datos la obligación de poner los datos a disposición de los usuarios y de terceros designados por los usuarios en determinadas circunstancias. También garantiza que los titulares de datos pongan los datos a disposición de los destinatarios de datos en la Unión en condiciones justas, razonables y no discriminatorias y de manera transparente. Las normas de Derecho privado son fundamentales en el marco general del intercambio de datos. Por lo tanto, el presente Reglamento adapta las normas de Derecho contractual e impide la explotación de los desequilibrios contractuales que dificultan el acceso y la utilización equitativos de los datos para las microempresas y las pequeñas y medianas empresas en el sentido de la Recomendación 2003/361/CE. El presente Reglamento también garantiza que, cuando exista una necesidad excepcional, los titulares de datos pongan a disposición de los organismos del sector público de los Estados miembros y de las instituciones, órganos u organismos de la Unión los datos necesarios para el desempeño de las tareas realizadas en interés público. Además, el presente Reglamento pretende facilitar el cambio entre servicios de tratamiento de datos y mejorar la interoperabilidad de los datos y de los mecanismos y servicios de intercambio de datos en la Unión. El presente Reglamento no debe interpretarse como el reconocimiento o la creación de una base jurídica para que el titular de datos conserve los datos, tenga acceso a ellos o los trate, ni como la concesión de un nuevo derecho del titular de datos a utilizar los datos generados por el uso de un producto o servicio relacionado. En cambio, el presente Reglamento toma como punto de partida el control de que el titular de los datos efectivamente disfruta, de hecho o de derecho, sobre los datos generados por productos o servicios relacionados.

(6) La generación de datos es el resultado de las acciones de al menos dos agentes: el diseñador o fabricante de un producto y el usuario de dicho producto. La generación de datos plantea cuestiones de equidad en la economía digital, ya que los datos registrados por los productos o servicios relacionados constituyen una información importante para los servicios de posventa, los servicios auxiliares y otros servicios. Con el fin de aprovechar los importantes beneficios económicos de los datos como un bien no exclusivo para la economía y la sociedad, es preferible adoptar un enfoque general para asignar los derechos de acceso y utilización de los datos frente a la concesión de derechos exclusivos.

(7) El derecho fundamental a la protección de los datos personales está salvaguardado, en particular, por el Reglamento (UE) 2016/679 y el Reglamento (UE) 2018/1725.

Además, la Directiva 2002/58/CE protege la vida privada y la confidencialidad de las comunicaciones, incluso mediante el establecimiento de condiciones para el almacenamiento de datos personales y no personales en los equipos terminales, y el acceso desde estos. Los mencionados instrumentos constituyen la base para un tratamiento de datos sostenible y responsable, incluso cuando los conjuntos de datos contienen una combinación de datos personales y no personales. El presente Reglamento complementa el Derecho de la Unión y se entiende sin perjuicio del mismo en materia de protección de datos y privacidad, en particular, en lo que se refiere al Reglamento (UE) 2016/679 y la Directiva 2002/58/CE. Ninguna disposición del presente Reglamento debe aplicarse o interpretarse de manera que se reduzca o limite el derecho a la protección de los datos personales o el derecho a la intimidad y la confidencialidad de las comunicaciones.

(8) Los principios de minimización y protección de datos desde el diseño y por defecto son esenciales cuando el tratamiento implica riesgos significativos para los derechos fundamentales de las personas. Teniendo en cuenta los últimos avances técnicos, todas las partes en el intercambio de datos, incluso cuando estén dentro del ámbito de aplicación del presente Reglamento, deben aplicar medidas técnicas y organizativas para proteger estos derechos. Dichas medidas incluyen no solo la seudonimización y el cifrado, sino también el uso de una tecnología cada vez más utilizada que permita introducir algoritmos en los datos y obtener información valiosa sin que sea necesaria la transmisión entre las partes ni la copia superflua de los datos brutos o estructurados.

(9) El presente Reglamento complementa el Derecho de la Unión —y se entiende sin perjuicio del mismo— cuyo objetivo sea promover los intereses de los consumidores y garantizar un elevado nivel de protección de los consumidores, así como proteger su salud, su seguridad y sus intereses económicos, en particular la Directiva 2005/29/CE del Parlamento Europeo y del Consejo[59], la Directiva 2011/83/UE del Parlamento Europeo y del Consejo[60] y la Directiva 93/13/CEE del Parlamento Europeo y del Consejo[61].

(10) El presente Reglamento se entiende sin perjuicio de los actos jurídicos de la Unión que dispongan el intercambio de datos, el acceso a los mismos y su utilización con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, o a efectos aduaneros y fiscales, con independencia de la base jurídica en la que se hayan adoptado en virtud del Tratado de Funcionamiento de la Unión Europea. Dichos actos incluyen el Reglamento (UE) 2021/784 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, sobre la lucha contra la difusión de contenidos terroristas en línea, las [propuestas sobre pruebas electrónicas,

[59] Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) n.º 2006/2004 del Parlamento Europeo y del Consejo («Directiva sobre las prácticas comerciales desleales») (DO L 149 de 11.6.2005, p. 22).

[60] Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo.

[61] Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores. Directiva (UE) 2019/2161 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, por la que se modifica la Directiva 93/13/CEE del Consejo y las Directivas 98/6/CE, 2005/29/CE y 2011/83/UE del Parlamento Europeo y del Consejo, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión.

COM(2018) 225 y 226, una vez adoptadas], la [Propuesta de] Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE, así como la cooperación internacional en este contexto, en particular sobre la base del Convenio del Consejo de Europa sobre la Ciberdelincuencia («Convenio de Budapest») de 2001. El presente Reglamento se entiende sin perjuicio de las competencias de los Estados miembros en relación con las actividades de seguridad pública, defensa y seguridad nacional de conformidad con el Derecho de la Unión, y con las actividades de las aduanas en materia de gestión de riesgos y, en general, de verificación del cumplimiento del código aduanero por parte de los operadores económicos.

(11) El presente Reglamento no debe afectar a la legislación de la Unión que establece requisitos en materia de diseño físico y datos para los productos que se introduzcan en el mercado de la Unión.

(12) El presente Reglamento complementa el Derecho de la Unión —y se entiende sin perjuicio del mismo— que tenga como objetivo establecer requisitos de accesibilidad para determinados productos y servicios, en particular la Directiva 2019/882[62].

(13) El presente Reglamento se entiende sin perjuicio de las competencias de los Estados miembros en relación con las actividades de seguridad pública, defensa y seguridad nacional de conformidad con el Derecho de la Unión, y con las actividades de las aduanas en materia de gestión de riesgos y, en general, de verificación del cumplimiento del código aduanero por parte de los operadores económicos.

(14) Los productos físicos que, a través de sus componentes, obtengan, generen o recopilen datos relativos a su rendimiento, uso o entorno y que puedan comunicar dichos datos mediante un servicio de comunicaciones electrónicas disponible para el público (a menudo denominado «internet de las cosas») deben estar cubiertos por el presente Reglamento. Los servicios de comunicaciones electrónicas incluyen las redes telefónicas terrestres, las redes de televisión por cable, las redes basadas en satélites y las redes de comunicación de campo cercano. Dichos productos pueden incluir vehículos, equipos domésticos y bienes de consumo, productos médicos y sanitarios o maquinaria agrícola e industrial. Los datos representan la digitalización de las acciones y eventos de los usuarios y, en consecuencia, deben ser accesibles para el usuario, mientras que la información derivada o inferida a partir de estos datos, cuando se posea legalmente, no debe considerarse dentro del ámbito de aplicación del presente Reglamento. Estos datos pueden ser valiosos para el usuario y apoyan la innovación y el desarrollo de servicios digitales y de otros tipos que protegen el medio ambiente, la salud y la economía circular, en particular porque facilitan el mantenimiento y la reparación de los productos en cuestión.

(15) En cambio, algunos productos diseñados principalmente para mostrar o reproducir contenidos, o para grabarlos y transmitirlos (por ejemplo, para su utilización por un servicio en línea), no deben estar cubiertos por el presente Reglamento. Estos productos incluyen, entre otros, ordenadores personales, servidores, tabletas y teléfonos inteligentes, cámaras, cámaras web, sistemas de grabación de sonido y escáneres de texto. Son productos que requieren la intervención humana para producir diversas formas de contenido, como documentos de texto, archivos de sonido, archivos de vídeo, juegos y mapas digitales.

---

[62] Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios (DO L 151 de 7.6.2019).

(16) Es necesario establecer normas aplicables a los productos conectados que incorporen un servicio, o estén interconectados con este, de tal manera que la ausencia de dicho servicio impediría que el producto desempeñara sus funciones. Estos servicios relacionados pueden formar parte del acuerdo de venta, alquiler o arrendamiento, o prestarse normalmente para productos del mismo tipo; y el usuario, de manera razonable, podría esperar que se presten dichos servicios, dado el carácter del producto y teniendo en cuenta cualquier declaración pública realizada por el vendedor, arrendador u otras personas (o en nombre de estos) en fases previas de la cadena de transacciones, incluido el fabricante. Estos servicios relacionados pueden generar, por sí mismos, datos valiosos para el usuario, independientemente de la capacidad de recopilación de datos del producto con el que estén interconectados. El presente Reglamento debe ser aplicable asimismo a los servicios relacionados no prestados por el propio vendedor o arrendador, sino por un tercero, en virtud del contrato de venta, alquiler o arrendamiento. En caso de duda sobre si la prestación del servicio forma parte del contrato de venta, alquiler o arrendamiento, debe aplicarse el presente Reglamento.

(17) Los datos generados por el uso de un producto o servicio relacionado incluyen los datos registrados por el usuario de manera intencionada. Estos datos incluyen también los generados como subproducto de la intervención del usuario (como los datos de diagnóstico), y los generados sin intervención del usuario (por ejemplo, cuando el producto se encuentra en «modo de espera»), así como los registrados durante los períodos en que el producto esté apagado. Estos datos deben contener los datos en la forma y el formato en que son generados por el producto, pero no los resultantes de ningún proceso de *software* que calcule datos derivados a partir de dichos datos, ya que este proceso puede estar sujeto a derechos de propiedad intelectual.

(18) Por usuario de un producto debe entenderse la persona física o jurídica, como una empresa o un consumidor, que ha comprado, alquilado o arrendado el producto. En función del título jurídico con el que dicho usuario use el producto, este asumirá los riesgos y aprovechará las ventajas de utilizar el producto conectado y también deberá poder acceder a los datos que genere. Por lo tanto, el usuario debe tener derecho a aprovechar los datos generados por dicho producto y cualquier servicio relacionado.

(19) En la práctica, no todos los datos generados por productos o servicios relacionados son fácilmente accesibles para sus usuarios, y a menudo existen pocas opciones de portabilidad de los datos generados por productos conectados a la internet de las cosas. Los usuarios no pueden obtener los datos necesarios para recurrir a proveedores de servicios de reparación y otros servicios, y las empresas no pueden poner en marcha servicios innovadores, más eficientes y prácticos. En muchos sectores, los fabricantes, aunque no tengan derecho legal a los datos, a menudo pueden determinar, a través del control del diseño técnico del producto o de los servicios relacionados, qué datos se generan y cómo se puede acceder a ellos. Por lo tanto, es necesario garantizar que los productos se diseñen y fabriquen de manera que los datos generados por su uso sean fácilmente accesibles para el usuario en todo momento, y que los servicios relacionados se presten de esa misma manera.

(20) En caso de que varias personas o entidades posean un producto o sean parte en un acuerdo de arrendamiento o alquiler y tengan acceso a un servicio relacionado, a la hora de diseñar el producto, el servicio relacionado o la interfaz pertinente, debe hacerse lo posible por que todas las personas puedan tener acceso a los datos que generan. Por lo general, se requiere a los usuarios de productos que generan datos la creación de una cuenta de usuario. Esta cuenta permite la identificación del usuario

por parte del fabricante, y es un medio para comunicarse con vistas a realizar y tratar las solicitudes de acceso a datos. Los fabricantes o diseñadores de un producto que suelen utilizar varias personas deben establecer el mecanismo necesario que permita crear cuentas de usuario separadas para personas concretas, cuando proceda, o que varias personas puedan utilizar la misma cuenta de usuario. Debe concederse acceso al usuario mediante mecanismos de solicitud sencillos, de ejecución automática, que no requieran un examen o autorización por parte del fabricante o del titular de datos. Esto significa que los datos solo deben ponerse a disposición cuando el usuario lo desee realmente. Cuando no sea posible realizar la solicitud de acceso a los datos de manera automatizada, por ejemplo a través de una cuenta de usuario o de una aplicación móvil que acompañe al producto o servicio, el fabricante deberá informar al usuario de cómo puede acceder a los datos.

(21) Los productos pueden diseñarse para que determinados datos estén directamente disponibles a partir de un almacenamiento de datos en el dispositivo o de un servidor remoto al que se comuniquen los datos. El acceso al almacenamiento de datos en el dispositivo podrá habilitarse a través de redes de área local por cable o inalámbricas conectadas a un servicio de comunicaciones electrónicas disponible al público o a una red móvil. El servidor puede estar integrado en la capacidad del servidor local del fabricante o en la de un tercero o un proveedor de servicios en la nube que actúe como titular de datos. Pueden estar diseñados para permitir al usuario o a un tercero tratar los datos del producto o de una instancia informática del fabricante.

(22) Los asistentes virtuales desempeñan un papel cada vez más importante en la digitalización de los entornos de consumo y son una interfaz fácil de utilizar que sirve para reproducir contenidos, buscar información o activar objetos físicos conectados a la internet de las cosas. Los asistentes virtuales pueden funcionar como una pasarela única, por ejemplo en un entorno doméstico inteligente, y registrar cantidades significativas de datos pertinentes sobre cómo interactúan los usuarios con productos conectados a la internet de las cosas, incluso los fabricados por otras partes, y pueden sustituir a las interfaces proporcionadas por el fabricante, como pantallas táctiles o aplicaciones para teléfonos inteligentes. Es posible que el usuario desee poner dichos datos a disposición de fabricantes terceros para permitir el desarrollo de servicios innovadores destinados a hogares inteligentes. Estos asistentes virtuales deben estar cubiertos por el derecho de acceso a los datos contemplado en el presente Reglamento, también en lo que respecta a los datos registrados antes de la activación del asistente virtual mediante la palabra de activación y a los datos generados cuando un usuario interactúa con un producto a través de un asistente virtual facilitado por una entidad distinta del fabricante del producto. Sin embargo, solo entran en el ámbito de aplicación del presente Reglamento los datos derivados de la interacción entre el usuario y el producto a través del asistente virtual. Los datos producidos por el asistente virtual que no estén relacionados con el uso de un producto no son objeto del presente Reglamento.

(23) Antes de celebrar un contrato de compra, alquiler o arrendamiento de un producto o la prestación de un servicio relacionado, debe facilitarse al usuario información clara y suficiente sobre cómo acceder a los datos generados. Esta obligación aporta transparencia sobre los datos generados y mejora la facilidad de acceso para el usuario. Esta obligación de informar no afecta a la obligación del responsable del tratamiento de facilitar información al interesado de conformidad con los artículos 12, 13 y 14 del Reglamento (UE) 2016/679.

(24) El presente Reglamento impone a los titulares de datos la obligación de poner a disposición los datos en determinadas circunstancias. En la medida en que se traten datos personales, el titular de datos debe ser responsable del tratamiento con arreglo al Reglamento (UE) 2016/679. Cuando el usuario sea un interesado, los titulares de datos deben estar obligados a proporcionarle acceso a sus datos y a ponerlos a disposición de terceros elegidos por el usuario de conformidad con el presente Reglamento. Sin embargo, el presente Reglamento no crea una base jurídica en virtud del Reglamento (UE) 2016/679 para que el titular de datos facilite el acceso a los datos personales o los ponga a disposición de un tercero cuando así lo solicite un usuario que no un interesado, y no debe entenderse que concede ningún nuevo derecho al titular de datos a utilizar los datos generados por el uso de un producto o de un servicio relacionado. Esto se aplica, en particular, cuando el fabricante es el titular de datos. En tal caso, la base para que el fabricante utilice datos no personales debe ser un acuerdo contractual entre el fabricante y el usuario. Dicho acuerdo podrá formar parte del contrato de venta, alquiler o arrendamiento del producto. Toda cláusula contractual del acuerdo que estipule que el titular de datos puede utilizar los datos generados por el usuario de un producto o servicio relacionado debe ser transparente para el usuario, incluso en lo que respecta a la finalidad para la que el titular de datos pretenda utilizar los datos. El presente Reglamento no debe impedir las condiciones contractuales cuyo efecto sea excluir o limitar la utilización de los datos, o de determinadas categorías de los mismos, por parte del titular de datos. El presente Reglamento tampoco debe impedir los requisitos reglamentarios sectoriales específicos en virtud del Derecho de la Unión, o del Derecho interno compatible con el Derecho de la Unión, que excluirían o limitarían la utilización de determinados datos por parte del titular de datos por razones de orden público bien definidas.

(25) En los sectores caracterizados por la concentración de un pequeño número de fabricantes que abastecen a los usuarios finales, los usuarios disponen de opciones limitadas en lo que respecta al intercambio de datos con dichos fabricantes. En tales circunstancias, los acuerdos contractuales pueden resultar insuficientes para alcanzar el objetivo de la capacitación de los usuarios. Los datos suelen permanecer bajo el control de los fabricantes, lo que dificulta a los usuarios obtener valor a partir de los datos generados por los equipos que compran o arriendan. Por consiguiente, existe un potencial limitado para que las pequeñas empresas innovadoras ofrezcan soluciones basadas en datos de manera competitiva y para alcanzar una economía de los datos diversa en Europa. Por lo tanto, el presente Reglamento debe basarse en los últimos avances en sectores específicos, como el Código de conducta sobre el intercambio de datos agrícolas mediante acuerdo contractual. La legislación sectorial puede utilizarse para abordar las necesidades y objetivos específicos del sector. Además, el titular de datos no debe utilizar ningún dato generado por el uso del producto o servicio relacionado con el fin de obtener información sobre la situación económica del usuario, sus activos o métodos de producción o para cualquier otro fin que pueda socavar la posición comercial del usuario en los mercados en los que opera. Esto implicaría, por ejemplo, el uso de la información sobre el rendimiento global de una empresa, o de una explotación agrícola, en las negociaciones contractuales con el usuario sobre la posible adquisición de los productos, o de los productos agrícolas, del usuario en su propio detrimento, o para alimentar bases de datos más amplias de determinados mercados (por ejemplo, las bases de datos sobre el rendimiento de los cultivos para la próxima temporada de cosecha), ya que tal uso podría afectar negativamente al usuario de manera indirecta. El usuario debe disponer de la interfaz técnica necesaria para gestionar los permisos, preferiblemente con opciones de

permiso detalladas (como «permitir una vez» o «permitir cuando se utilice esta aplicación o servicio»), incluida la opción de retirar el permiso.

(26) En los contratos entre un titular de datos y un consumidor como usuario de un producto o servicio relacionado que genera datos, la Directiva 93/13/CEE se aplica a las cláusulas del contrato para garantizar que el consumidor no esté sujeto a cláusulas contractuales abusivas. En el caso de las cláusulas contractuales abusivas impuestas unilateralmente a microempresas o a pequeñas o medianas empresas, tal como se definen en el artículo 2 del anexo de la Recomendación 2003/361/CE[63], el presente Reglamento establece que dichas cláusulas abusivas no deben ser vinculantes para dichas empresas.

(27) El titular de datos podrá exigir una identificación adecuada del usuario para verificar el derecho de acceso a los datos por parte del usuario. En el caso de los datos personales tratados por un encargado del tratamiento en nombre del responsable del tratamiento, el titular de datos debe garantizar que el encargado del tratamiento reciba y tramite la solicitud de acceso.

(28) El usuario debe ser libre de utilizar los datos para cualquier fin lícito, lo que incluye que el usuario, en el ejercicio del derecho reconocido en el presente Reglamento, pueda facilitar los datos que haya recibido a un tercero que ofrezca un servicio posventa que pueda estar en competencia con un servicio prestado por el titular de datos, o dar instrucciones al titular de datos para que lo haga. El titular de datos debe garantizar que los datos puestos a disposición del tercero sean tan exactos, completos, fiables, pertinentes y actualizados como los datos a los que el propio titular de datos pueda acceder, o a los que tenga derecho a acceder, al utilizar el producto o servicio relacionado. En el tratamiento de los datos deben respetarse los secretos comerciales o de propiedad intelectual. Es importante mantener los incentivos a la inversión en productos con funcionalidades basadas en la utilización de datos procedentes de sensores incorporados a dichos productos. Por consiguiente, debe entenderse que los objetivos del presente Reglamento son fomentar el desarrollo de productos nuevos e innovadores o servicios relacionados, estimular la innovación en los mercados de posventa, y también alentar el desarrollo de servicios totalmente novedosos que utilicen los datos, incluso los basados en datos procedentes de diversos productos o servicios relacionados. Al mismo tiempo, el presente Reglamento pretende evitar la reducción de los incentivos a la inversión para el tipo de producto del que se obtienen los datos, por ejemplo, utilizando los datos para desarrollar un producto competidor.

(29) Un tercero al que se facilitan datos puede ser una empresa, un organismo de investigación o una organización sin ánimo de lucro. Al poner los datos a disposición del tercero, el titular de datos no debe explotar de manera abusiva su posición para buscar una ventaja competitiva en mercados en los que el titular de datos y el tercero puedan estar en competencia directa. Además, el titular de datos no debe utilizar ningún dato generado por el uso del producto o servicio relacionado con el fin de obtener información sobre la situación económica del tercero, sus activos o métodos de producción o para cualquier otro fin que pueda socavar la posición comercial del tercero en los mercados en los que opera.

(30) El uso de un producto o servicio relacionado puede generar datos relativos a una persona física identificada o identificable (el interesado), en particular cuando el usuario sea una persona física. El tratamiento de dichos datos está sujeto a las normas

[63] Recomendación de la Comisión 2003/361/CE, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

establecidas en virtud del Reglamento (UE) 2016/679, incluso cuando los datos personales y no personales de un conjunto de datos estén indisolublemente vinculados[64]. El interesado puede ser el usuario u otra persona física. Los datos personales solo podrán ser solicitados por un responsable del tratamiento o un interesado. Un usuario que sea el interesado tiene derecho, en determinadas circunstancias, en virtud del Reglamento (UE) 2016/679, a acceder a los datos personales que le incumban, derecho que no se ve afectado por el presente Reglamento. En virtud del presente Reglamento, el usuario que sea una persona física tiene también derecho a acceder a todos los datos generados por el producto, tanto personales como no personales. Cuando el usuario no sea el interesado sino una empresa, incluido un empresario individual, y no en los casos de uso doméstico compartido del producto, el usuario será responsable del tratamiento en el sentido del Reglamento (UE) 2016/679. Por consiguiente, dicho usuario, como responsable del tratamiento que desea solicitar datos personales generados por el uso de un producto o un servicio relacionado, debe tener una base jurídica para el tratamiento de los datos con arreglo al artículo 6, apartado 1, del Reglamento (UE) 2016/679, como el consentimiento del interesado o el interés legítimo. Dicho usuario debe garantizar que el interesado esté debidamente informado de los fines especificados, explícitos y legítimos del tratamiento de dichos datos, y de la manera en que el interesado puede ejercer efectivamente sus derechos. Cuando el titular de datos y el usuario sean corresponsables del tratamiento en el sentido del artículo 26 del Reglamento (UE) 2016/679, están obligados a determinar, de manera transparente y mediante un acuerdo entre ellos, sus responsabilidades respectivas para garantizar el cumplimiento de dicho Reglamento. Debe entenderse que dicho usuario, una vez que los datos se hayan puesto a disposición, puede convertirse en titular de datos si cumple los criterios establecidos en el presente Reglamento y, por tanto, estar sujeto a la obligación de poner a disposición los datos en virtud del presente Reglamento.

(31) Los datos generados por el uso de un producto o servicio relacionado solo deben ponerse a disposición de un tercero a petición del usuario. Por lo tanto, el presente Reglamento complementa el derecho establecido en el artículo 20 del Reglamento (UE) 2016/679. Dicho artículo establece el derecho de los interesados a recibir los datos personales que les incumban en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otros responsables del tratamiento, cuando dichos datos se traten sobre la base del artículo 6, apartado 1, letra a), o del artículo 9, apartado 2, letra a), o de un contrato con arreglo al artículo 6, apartado 1, letra b). Los interesados también tienen derecho a que los datos personales se transmitan directamente de responsable a responsable, pero solo cuando sea técnicamente posible. El artículo 20 especifica que se trata de los datos facilitados por el interesado, pero no especifica si ello requiere un comportamiento activo por parte del interesado o si también es aplicable cuando un producto o servicio relacionado, por su diseño, observa el comportamiento de un interesado u otra información relacionada con un interesado de manera pasiva. El derecho establecido por el presente Reglamento complementa el derecho a la recepción y la portabilidad de datos personales en virtud del artículo 20 del Reglamento (UE) 2016/679 de varias maneras. Concede a los usuarios el derecho a acceder y poner a disposición de terceros cualquier dato generado por el uso de un producto o servicio relacionado, independientemente de que sean de carácter personal, de la distinción entre datos facilitados activamente u observados pasivamente y de la base jurídica del tratamiento. A diferencia de las obligaciones técnicas establecidas en

64 DO L 303 de 28.11.2018, p. 59.

el artículo 20 del Reglamento (UE) 2016/679, el presente Reglamento exige y garantiza la viabilidad técnica del acceso de terceros a todos los tipos de datos incluidos en su ámbito de aplicación, ya sean personales o no personales. El presente Reglamento también permite al titular de datos establecer una compensación razonable a cargo de terceros, pero no del usuario, por cualquier coste en que se incurra al proporcionar acceso directo a los datos generados por el producto del usuario. Si el titular de datos y un tercero no pueden acordar las condiciones de dicho acceso directo, no debe impedirse en modo alguno que el interesado ejerza los derechos recogidos en el Reglamento (UE) 2016/679, incluido el derecho a la portabilidad de los datos, buscando vías de recurso de conformidad con dicho Reglamento. En este contexto, debe entenderse que, de conformidad con el Reglamento (UE) 2016/679, un acuerdo contractual no permite el tratamiento de categorías especiales de datos personales por parte del titular de datos o del tercero.

(32) El acceso a todos los datos almacenados en equipos terminales, y a los que se acceda desde estos, está sujeto a la Directiva 2002/58/CE y requiere el consentimiento del abonado o usuario en el sentido de dicha Directiva, a menos que sea estrictamente necesario para prestar un servicio de la sociedad de la información expresamente solicitado por el usuario o el abonado (o únicamente para la transmisión de una comunicación). La Directiva 2002/58/CE («Directiva sobre la privacidad y las comunicaciones electrónicas») y la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas protegen la integridad de los equipos terminales del usuario en lo que respecta al uso de las capacidades de tratamiento y almacenamiento y a la recopilación de información. Los equipos de internet de las cosas se consideran equipos terminales si están directa o indirectamente conectados a una red pública de comunicaciones.

(33) Con el fin de evitar la explotación de los usuarios, los terceros a los que se hayan facilitado datos a petición del usuario solo deben tratar los datos para los fines acordados con el usuario e intercambiarlos con otro tercero solo si ello es necesario para prestar el servicio solicitado por el usuario.

(34) En consonancia con el principio de minimización de datos, el tercero solo debe acceder a la información adicional necesaria para prestar el servicio solicitado por el usuario. Tras haber recibido acceso a los datos, el tercero debe tratarlos exclusivamente para los fines acordados con el usuario, sin injerencia del titular de datos. Para el usuario, debe ser tan fácil denegar o interrumpir el acceso del tercero a los datos como autorizarlo. El tercero no debe coaccionar, engañar o manipular al usuario de ningún modo, perjudicando o socavando la autonomía, la toma de decisiones o las opciones del usuario, o utilizando una interfaz digital con el usuario. En este contexto, los terceros no deben basarse en los denominados «patrones oscuros» a la hora de diseñar sus interfaces digitales. Los «patrones oscuros» son técnicas de diseño que empujan o engañan a los consumidores para que tomen decisiones que conllevan consecuencias negativas para sí mismos. Estas técnicas de manipulación pueden utilizarse para persuadir a los usuarios, en particular a los consumidores más vulnerables, a que incurran en comportamientos no deseados, y para engañarlos induciéndoles a tomar decisiones sobre transacciones de revelación de datos o para influir injustificadamente en la toma de decisiones de los usuarios del servicio, de tal manera que se socave y perjudique su autonomía, su toma de decisiones y su capacidad de elegir entre distintas opciones. Las prácticas comerciales habituales y legítimas que sean conformes con el Derecho de la Unión no deben considerarse por sí mismas como «patrones oscuros». Los terceros deben cumplir sus

obligaciones en virtud del Derecho de la Unión pertinente, en particular los requisitos establecidos en la Directiva 2005/29/CE, la Directiva 2011/83/UE, la Directiva 2000/31/CE y la Directiva 98/6/CE.

(35) Los terceros también deben abstenerse de utilizar los datos para trazar perfiles de personas, a menos que sea estrictamente necesario para prestar el servicio solicitado por el usuario. El requisito de suprimir datos cuando ya no sean necesarios para el fin acordado con el usuario complementa el derecho de supresión del interesado con arreglo al artículo 17 del Reglamento (CE) n.º 2016/679. Cuando el tercero sea un proveedor de un servicio de intermediación de datos en el sentido de la [Ley de Gobernanza de Datos], se aplicarán las garantías para el interesado que establece dicho Reglamento. El tercero puede utilizar los datos para desarrollar un producto o servicio relacionado, nuevo e innovador, pero no para desarrollar un producto competidor.

(36) Las empresas emergentes, las pequeñas y medianas empresas y las empresas de sectores tradicionales con capacidades digitales menos desarrolladas tienen dificultades para acceder a los datos pertinentes. El presente Reglamento tiene por objeto facilitar el acceso de estas entidades a los datos, garantizando al mismo tiempo que las obligaciones correspondientes queden delimitadas de la manera más proporcionada posible para evitar extralimitaciones. Al mismo tiempo, en la economía digital ha surgido un pequeño número de empresas muy grandes con un poder económico considerable gracias a la acumulación y agregación de grandes volúmenes de datos y a la infraestructura tecnológica necesaria para su monetización. Algunas de estas empresas prestan servicios básicos de plataforma que controlan ecosistemas de plataformas enteros en la economía digital, y que los operadores del mercado existentes o nuevos no son capaces de desafiar o disputar. El [Reglamento sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales)] tiene por objeto corregir estas ineficiencias y desequilibrios permitiendo a la Comisión designar a un proveedor como «guardián de acceso», e impone una serie de obligaciones a dichos guardianes de acceso designados, como la prohibición de combinar determinados datos sin consentimiento, o la obligación de garantizar los derechos efectivos a la portabilidad de los datos en virtud del artículo 20 del Reglamento (UE) 2016/679. En consonancia con el [Reglamento sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales)], y habida cuenta de la inigualable capacidad de estas empresas para adquirir datos, la inclusión de dichas empresas guardianas de acceso como beneficiarias del derecho de acceso a los datos no sería necesaria para alcanzar el objetivo del presente Reglamento y, por tanto, sería desproporcionada en relación con los titulares de datos sujetos a dichas obligaciones. Esto significa que una empresa que presta servicios básicos de plataforma que ha sido designada como guardián de acceso no puede solicitar ni obtener acceso a los datos de los usuarios generados por el uso de un producto o servicio relacionado o por un asistente virtual sobre la base de las disposiciones del capítulo II del presente Reglamento. Debe entenderse que una empresa que presta servicios básicos de plataforma designada como guardián de acceso con arreglo a la Ley de Mercados Digitales incluye a todas las entidades jurídicas de un grupo de empresas en el que una entidad jurídica presta un servicio básico de plataforma. Además, los terceros a los que se faciliten datos a petición del usuario no podrán poner los datos a disposición de un guardián de acceso designado. Por ejemplo, el tercero no puede subcontratar la prestación de servicios a un guardián de acceso. Sin embargo, esto no impide que terceros utilicen servicios de tratamiento de datos ofrecidos por un guardián de acceso designado. Esta exclusión de los guardianes de acceso designados

del ámbito de aplicación del derecho de acceso en virtud del presente Reglamento no impide a estas empresas obtener datos por otros medios legales.

(37) Habida cuenta del estado actual de la tecnología, resulta excesivamente gravoso imponer nuevas obligaciones de diseño en relación con los productos fabricados o diseñados y los servicios relacionados prestados por microempresas y pequeñas empresas. Sin embargo, no sucede así cuando se subcontrata a una microempresa o pequeña empresa para fabricar o diseñar un producto. En estas situaciones, la empresa que haya subcontratado a la microempresa o pequeña empresa puede compensar adecuadamente al subcontratista. No obstante, una microempresa o pequeña empresa puede estar sujeta a los requisitos establecidos en el presente Reglamento como titular de datos, cuando no sea el fabricante del producto o un proveedor de servicios relacionados.

(38) El presente Reglamento contiene normas generales de acceso, siempre que el titular de datos esté obligado por ley a poner los datos a disposición de un destinatario de datos. Dicho acceso debe basarse en condiciones justas, razonables, no discriminatorias y transparentes con el fin de garantizar la coherencia de las prácticas de intercambio de datos en el mercado interior, también entre distintos sectores, y de alentar y promover prácticas equitativas de intercambio de datos, incluso en ámbitos en los que no se concede dicho derecho de acceso a los datos. Estas normas generales de acceso no se aplican a las obligaciones de poner a disposición los datos en virtud del Reglamento (UE) 2016/679. El intercambio voluntario de datos no se ve afectado por estas normas.

(39) Sobre la base del principio de libertad contractual, las partes deben seguir siendo libres de negociar las condiciones precisas para la puesta a disposición de los datos en sus contratos, en el marco de las normas generales de acceso para la puesta a disposición de los datos.

(40) A fin de garantizar que las condiciones de acceso obligatorio a los datos sean equitativas para ambas partes, las normas generales sobre los derechos de acceso a los datos deben hacer referencia a la norma relativa a la necesidad de evitar cláusulas contractuales abusivas.

(41) Para compensar la falta de información sobre las condiciones de los distintos contratos, lo que dificulta que el destinatario de los datos evalúe si las condiciones de puesta a disposición de los datos no son discriminatorias, debe corresponder al titular de datos demostrar que una cláusula contractual no es discriminatoria. No se considera una discriminación ilegal que el titular de datos utilice cláusulas contractuales diferentes para poner a disposición los datos o una compensación diferente, si dichas diferencias están justificadas por razones objetivas. Estas obligaciones se entienden sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679.

(42) Con el fin de incentivar la inversión continua en la generación de datos valiosos, como la inversión en herramientas técnicas pertinentes, el presente Reglamento contiene el principio de que el titular de datos puede solicitar una compensación razonable cuando esté legalmente obligado a poner los datos a disposición del destinatario de los datos. Estas disposiciones no deben entenderse como un pago por los propios datos, sino, en el caso de las microempresas y las pequeñas o medianas empresas, por los costes en que se haya incurrido y las inversiones necesarias para poner los datos a disposición.

(43) En casos justificados, como cuando sea necesario proteger la participación y la competencia de los consumidores o promover la innovación en determinados mercados, el Derecho de la Unión o la legislación nacional que aplica el Derecho de la

Unión pueden imponer una compensación regulada por la puesta a disposición de tipos de datos específicos.

(44) Con el fin de proteger a las microempresas y a las pequeñas y medianas empresas de cargas económicas excesivas que les dificultarían comercialmente el desarrollo y la gestión de modelos de negocio innovadores, la compensación por la puesta a disposición de los datos que pagarían no debe superar el coste directo de la puesta a disposición de los datos y no debe ser discriminatoria.

(45) Los costes directos de la puesta a disposición de los datos son los costes necesarios para la reproducción de los datos, su difusión por medios electrónicos y su almacenamiento, pero no los costes de recopilación o producción de datos. Los costes directos de la puesta a disposición de los datos deben limitarse a la parte atribuible a las solicitudes individuales, teniendo en cuenta que el titular de datos tendrá que establecer permanentemente las interfaces técnicas necesarias o los correspondientes programas informáticos y la conectividad. Los acuerdos a largo plazo entre los titulares de datos y los destinatarios de datos, por ejemplo a través de un modelo de suscripción, podrían reducir los costes relacionados con la puesta a disposición de los datos en transacciones regulares o repetitivas en una relación de negocios.

(46) La intervención no es necesaria cuando el intercambio de datos se realiza entre grandes empresas, ni cuando el titular de datos es una pequeña o mediana empresa y el destinatario de datos es una gran empresa. En tales casos, se considera que las empresas son capaces de negociar cualquier compensación si es razonable, teniendo en cuenta factores como el volumen, el formato, el carácter, la oferta y la demanda de los datos, así como los costes derivados de la recopilación y puesta a disposición del destinatario de datos.

(47) La transparencia es un principio importante a la hora de garantizar que la compensación solicitada por el titular de datos sea razonable o, cuando el destinatario de datos sea una microempresa o una pequeña o mediana empresa, que la compensación no supere los costes directamente relacionados con la puesta a disposición de los datos al destinatario de datos y que sea atribuible a la solicitud individual. A fin de que el destinatario de datos pueda evaluar y verificar que la compensación cumple los requisitos del presente Reglamento, el titular de datos debe facilitar al destinatario de datos la información necesaria para calcular la compensación con un nivel de detalle suficiente.

(48) Garantizar el acceso a formas alternativas de resolución de litigios nacionales y transfronterizos derivados de la puesta a disposición de los datos debe redundar en beneficio de los titulares y destinatarios de datos y, por lo tanto, reforzar la confianza en el intercambio de datos. Cuando las partes no puedan acordar condiciones justas, razonables y no discriminatorias para la puesta a disposición de los datos, los organismos de resolución de litigios deben ofrecer a las partes una solución sencilla, rápida y económica.

(49) A fin de evitar el recurso a dos o más organismos de resolución de litigios para un mismo litigio, en particular en un contexto transfronterizo, un organismo de resolución de litigios debe poder rechazar una solicitud de resolución de un litigio que ya se haya presentado ante otro organismo de resolución de litigios o ante un órgano jurisdiccional de un Estado miembro.

(50) No debe impedirse que las partes en los procedimientos de resolución de litigios ejerzan su derecho fundamental a la tutela judicial efectiva y a un juez imparcial. Por

consiguiente, la decisión de someter un litigio a un organismo de resolución de litigios no debe privar a dichas partes de su derecho a recurrir ante un órgano jurisdiccional de un Estado miembro.

(51) Cuando una de las partes se encuentra en una posición negociadora más fuerte, existe el riesgo de que pueda aprovecharla en detrimento de la otra parte contratante a la hora de negociar y haga que el acceso a los datos sea menos viable desde el punto de vista comercial y, a veces, económicamente prohibitivo. Estos desequilibrios contractuales perjudican especialmente a las microempresas y a las pequeñas y medianas empresas que no cuentan con una capacidad significativa de negociar las condiciones de acceso a los datos, y cuya única opción es aceptar cláusulas contractuales de «o lo tomas o lo dejas». Por lo tanto, las cláusulas contractuales abusivas que regulen el acceso a los datos y su utilización, o la responsabilidad y los recursos en caso de incumplimiento o rescisión de obligaciones relacionadas con los datos no deben ser vinculantes para las microempresas ni para las pequeñas o medianas empresas cuando se les hayan impuesto unilateralmente.

(52) Las normas sobre cláusulas contractuales deben tener en cuenta el principio de libertad contractual como concepto esencial en las relaciones entre empresas. Por lo tanto, no todas las cláusulas contractuales deben someterse a un control del carácter abusivo, sino únicamente las impuestas unilateralmente a las microempresas y a las pequeñas y medianas empresas. Se trata de situaciones del tipo «o lo tomas o lo dejas» en las que una parte presenta una determinada cláusula contractual y la microempresa, pequeña o mediana empresa no puede influir en el contenido de dicha cláusula pese a haber intentado negociarla. Una cláusula contractual que sea planteada simplemente por una de las partes y aceptada por la microempresa o la pequeña o mediana empresa, o una cláusula que se negocie y posteriormente se acuerde de forma modificada entre las partes contratantes no debe considerarse como impuesta unilateralmente.

(53) Además, las normas sobre cláusulas contractuales abusivas solo deben aplicarse a aquellos elementos de un contrato que estén relacionados con la puesta a disposición de datos, es decir, las cláusulas contractuales relativas al acceso a los datos y a su utilización, así como a la responsabilidad o los recursos por incumplimiento y rescisión de las obligaciones relacionadas con los datos. Las secciones del mismo contrato que no guarden relación con la puesta a disposición de datos no deben estar sujetas al control del carácter abusivo establecido en el presente Reglamento.

(54) Los criterios para determinar las cláusulas contractuales abusivas solo deben aplicarse a cláusulas contractuales excesivas cuando se abuse de una posición negociadora más fuerte. La gran mayoría de las cláusulas contractuales que son comercialmente más favorables para una parte que para la otra, incluidas las que son habituales en los contratos entre empresas, constituyen una expresión normal del principio de libertad contractual y seguirán siendo aplicables.

(55) Si una cláusula contractual no está incluida en la lista de cláusulas que siempre se consideran abusivas o que se presumen abusivas, se aplicará la disposición general del carácter abusivo. A este respecto, las cláusulas enumeradas como abusivas deben servir como referencia para interpretar la disposición general del carácter abusivo. Por último, las cláusulas contractuales tipo para los contratos de intercambio de datos entre empresas que la Comisión debe desarrollar y recomendar también pueden ser útiles para las partes comerciales a la hora de negociar contratos.

(56) En casos de necesidad excepcional, puede ser necesario que los organismos del sector público o las instituciones, órganos y organismos de la Unión utilicen datos que obren

en propiedad de una empresa para responder a emergencias públicas o en otros casos excepcionales. Las organizaciones que realizan actividades de investigación y las organizaciones que financian la investigación también se pueden organizar como organismos del sector público u organismos de Derecho público. Con el fin de limitar la carga para las empresas, las microempresas y las pequeñas empresas deben quedar exentas de la obligación de facilitar datos a los organismos del sector público y a las instituciones, órganos y organismos de la Unión en situaciones de necesidad excepcional.

(57) En caso de emergencia pública, ya sea una emergencia de salud pública, una emergencia derivada de la degradación del medio ambiente o de una catástrofe natural grave (incluidas las agravadas por el cambio climático) o una catástrofe grave provocada por el ser humano, como un incidente grave de ciberseguridad, el interés público resultante de la utilización de los datos prevalecerá sobre el interés de los titulares de datos de disponer libremente de los datos que obran en su poder. En tal caso, los titulares de datos deben estar obligados a poner los datos a disposición de los organismos del sector público o de las instituciones, órganos y organismos de la Unión que así lo requieran. La existencia de una emergencia pública se determina con arreglo a los procedimientos respectivos de los Estados miembros o de las organizaciones internacionales pertinentes.

(58) También puede surgir una necesidad excepcional cuando un organismo del sector público pueda demostrar que los datos son necesarios para evitar una emergencia pública o para ayudar a la recuperación tras una emergencia pública, en situaciones razonablemente próximas a la emergencia pública en cuestión. Cuando la necesidad excepcional no esté justificada por la necesidad de responder a una emergencia pública, evitarla o ayudar a la posterior recuperación, el organismo del sector público o la institución, órgano u organismo de la Unión deberá demostrar que la falta de acceso oportuno a los datos solicitados y la utilización de los mismos le impiden cumplir efectivamente una tarea específica de interés público contemplada explícitamente en la legislación. Esta necesidad excepcional también puede surgir en otras situaciones, por ejemplo en relación con la recopilación oportuna de estadísticas oficiales cuando no se disponga de datos de otro modo, o cuando se reduzca la carga de encuestados considerablemente. Al mismo tiempo, cuando no se trate de responder a una emergencia pública, evitarla o ayudar a la posterior recuperación, el organismo del sector público o la institución, órgano u organismo de la Unión deberá demostrar que no existe ningún medio alternativo para obtener los datos solicitados y que estos no pueden obtenerse de manera oportuna mediante el establecimiento de las obligaciones de suministro de datos necesarias en la nueva legislación.

(59) El presente Reglamento no debe aplicarse a los acuerdos voluntarios celebrados con vistas al intercambio de datos entre entidades privadas y públicas, ni debe condicionarlos. El presente Reglamento no debe afectar a las obligaciones impuestas a los titulares de datos de facilitar datos con motivo de necesidades de carácter no excepcional, en particular cuando se conozca la gama de datos y de titulares de datos y cuando la utilización de los datos pueda tener lugar periódicamente, como en el caso de las obligaciones de información y las obligaciones en el mercado interior. Los requisitos de acceso a los datos para verificar el cumplimiento de las normas aplicables, incluso en los casos en que los organismos del sector público asignen la tarea de verificación del cumplimiento a entidades que no sean organismos del sector público, tampoco deben verse afectados por el presente Reglamento.

(60) Para el ejercicio de sus tareas en los ámbitos de la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales y administrativas, la ejecución de sanciones penales y administrativas, así como la recopilación de datos con fines fiscales o aduaneros, los organismos del sector público y las instituciones, órganos y organismos de la Unión deben basarse en sus competencias en virtud de la legislación sectorial. Por consiguiente, el presente Reglamento no afecta a los instrumentos relativos al intercambio, el acceso y la utilización de datos en dichos ámbitos.

(61) Es necesario un marco proporcionado, limitado y predecible a escala de la Unión para que, en caso de necesidades excepcionales, los titulares de datos pongan los datos a disposición de los organismos del sector público y de las instituciones, órganos y organismos de la Unión, tanto para garantizar la seguridad jurídica como para minimizar las cargas administrativas que recaen sobre las empresas. A tal fin, las solicitudes de datos por parte de los organismos del sector público y de las instituciones, órganos y organismos de la Unión a los titulares de datos deben ser transparentes y proporcionadas en cuanto al alcance de su contenido y su granularidad. La finalidad de la solicitud y el uso previsto de los datos solicitados deben ser específicos y explicarse claramente, y permitir al mismo tiempo la flexibilidad necesaria para que la entidad solicitante desempeñe sus tareas en aras del interés público. La solicitud también debe respetar los intereses legítimos de las empresas a las que se dirige. La carga para los titulares de datos debe reducirse al mínimo obligando a las entidades solicitantes a respetar el principio de «solo una vez», que impide que los mismos datos sean solicitados más de una vez por más de un organismo del sector público o una institución, órgano u organismo de la Unión cuando dichos datos sean necesarios para responder a una emergencia pública. A fin de garantizar la transparencia, la entidad que solicite los datos debe hacer públicas sin demora injustificada las solicitudes de datos formuladas por los organismos del sector público y por las instituciones, órganos u organismos de la Unión, y debe garantizarse la disponibilidad pública en línea de todas las solicitudes justificadas por una emergencia pública.

(62) El objetivo de la obligación de facilitar los datos es garantizar que los organismos del sector público y las instituciones, órganos y organismos de la Unión tengan los conocimientos necesarios para responder a emergencias públicas, prevenirlas o recuperarse de ellas, o para mantener la capacidad de desempeñar tareas específicas expresamente contempladas por la ley. Los datos obtenidos por dichas entidades pueden ser sensibles desde el punto de vista comercial. Por consiguiente, la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo[65] no debe aplicarse a los datos facilitados en virtud del presente Reglamento, que no deben considerarse como datos abiertos disponibles para su reutilización por terceros. No obstante, esto no debe afectar a la aplicabilidad de la Directiva (UE) 2019/1024 en lo que se refiere a la reutilización de las estadísticas oficiales para cuya elaboración se hayan utilizado datos obtenidos con arreglo al presente Reglamento, siempre que dicha reutilización no incluya los datos subyacentes. Además, no debe afectar a la posibilidad de intercambiar los datos para llevar a cabo investigaciones o para la compilación de estadísticas oficiales, siempre que se cumplan las condiciones establecidas en el presente Reglamento. Los organismos del sector público también deben poder intercambiar los datos obtenidos en virtud del presente Reglamento con otros

[65] Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (DO L 172 de 26.6.2019, p. 56).

organismos del sector público con el fin de hacer frente a las necesidades excepcionales para las que se han solicitado los datos.

(63) Los titulares de datos deben tener la posibilidad de pedir una modificación de la solicitud presentada por un organismo del sector público o una institución, órgano u organismo de la Unión o su cancelación en un plazo de cinco o quince días hábiles, dependiendo del carácter de la necesidad excepcional invocada en la solicitud. En caso de solicitudes motivadas por una emergencia pública, debe existir una razón justificada para no poner a disposición los datos si puede demostrarse que la solicitud es similar o idéntica a una solicitud presentada previamente con el mismo fin por otro organismo del sector público o por otra institución, órgano u organismo de la Unión. El titular de datos que rechace la solicitud o que exija su modificación debe comunicar la justificación subyacente de la denegación de la solicitud al organismo del sector público o a la institución, órgano u organismo de la Unión que solicite los datos. En caso de que los derechos *sui generis* sobre bases de datos en virtud de la Directiva 96/6/CE del Parlamento Europeo y del Consejo[66] se apliquen en relación con los conjuntos de datos solicitados, los titulares de datos deben ejercer sus derechos de manera que no se impida al organismo del sector público y a las instituciones, órganos y organismos de la Unión obtener los datos o intercambiarlos de conformidad con el presente Reglamento.

(64) Cuando sea estrictamente necesario incluir datos personales en los datos puestos a disposición de un organismo del sector público o de una institución, órgano u organismo de la Unión, deben cumplirse las normas aplicables en materia de protección de datos personales, y la puesta a disposición de los datos y su uso posterior deben ir acompañados de garantías para los derechos e intereses de las personas interesadas por dichos datos. El organismo que solicite los datos debe demostrar la estricta necesidad y los fines específicos y limitados del tratamiento. El titular de datos debe hacer un esfuerzo razonable para anonimizar los datos o, cuando ello resulte imposible, aplicar medios tecnológicos como la seudonimización y la agregación, antes de poner los datos a disposición.

(65) Los datos puestos a disposición de los organismos del sector público y de las instituciones, órganos y organismos de la Unión sobre la base de una necesidad excepcional solo deben utilizarse para el fin para el que se solicitaron, a menos que el titular de datos que los haya facilitado haya acordado expresamente que los datos se utilicen para otros fines. Los datos deben destruirse cuando ya no sean necesarios para el fin indicado en la solicitud, a menos que se acuerde de otro modo, y debe informarse al titular de datos al respecto.

(66) Al reutilizar los datos facilitados por los titulares de datos, los organismos del sector público y las instituciones, órganos y organismos de la Unión deben respetar tanto la legislación vigente aplicable como las obligaciones contractuales a las que esté sujeto el titular de datos. Cuando la divulgación de secretos comerciales del titular de datos a organismos del sector público o a instituciones, órganos y organismos de la Unión sea estrictamente necesaria para cumplir el objetivo para el que se han solicitado los datos, debe garantizarse la confidencialidad de dicha divulgación al titular de datos.

(67) Cuando esté en juego la salvaguardia de un bien público significativo, como en la respuesta a emergencias públicas, no debe esperarse que el organismo del sector público o la institución, órgano u organismo de la Unión compensen a las empresas

[66] Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos (DO L 77 de 27.3.1996, p. 20).

por los datos obtenidos. Las emergencias públicas son acontecimientos inusuales y no todas requieren la utilización de datos que obran en propiedad de las empresas. Por tanto, no es probable que las actividades empresariales de los titulares de datos se vean afectadas negativamente como consecuencia de que los organismos del sector público o las instituciones, órganos u organismos de la Unión puedan acudir al presente Reglamento. No obstante, en los casos de necesidad excepcional distintos de la respuesta a una emergencia pública, que pueden ser más frecuentes e incluyen la prevención o recuperación de una emergencia pública, los titulares de datos deben tener derecho a una compensación razonable que no debe superar los costes técnicos y de organización en que se incurra para satisfacer la solicitud y el margen razonable necesario para poner los datos a disposición del organismo del sector público o de la institución, órgano u organismo de la Unión. La compensación no debe entenderse como un pago por los propios datos, ni como obligatoria.

(68) El organismo del sector público o la institución, órgano u organismo de la Unión podrá intercambiar los datos que haya obtenido en virtud de la solicitud con otras entidades o personas cuando ello sea necesario para llevar a cabo actividades de investigación científica o actividades analíticas que no pueda realizar por sí mismo. Estos datos también podrán intercambiarse en las mismas circunstancias con los institutos nacionales de estadística y Eurostat para compilar estadísticas oficiales. No obstante, estas actividades de investigación deben ser compatibles con la finalidad para la que se solicitaron los datos y el titular de datos debe ser informado del ulterior intercambio de los datos que había facilitado. Las personas u organismos que lleven a cabo actividades de investigación con las que puedan compartirse estos datos deben actuar sin ánimo de lucro o en el contexto de una misión de interés público reconocida por el Estado. Los organismos sobre los que las empresas comerciales tienen una influencia decisiva tal que les permita ejercer un control derivado de situaciones estructurales que podría dar lugar a un acceso preferente a los resultados de la investigación no deben considerarse organismos de investigación a efectos del presente Reglamento.

(69) La capacidad de los clientes de servicios de tratamiento de datos, incluidos los servicios en la nube y en el borde, de cambiar de un servicio de tratamiento de datos a otro, manteniendo al mismo tiempo una funcionalidad mínima del servicio, es una condición clave para lograr un mercado más competitivo con menores barreras de entrada para los nuevos proveedores de servicios.

(70) El Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo anima a los proveedores de servicios a que desarrollen y apliquen eficazmente códigos de conducta autorreguladores que incluyan las mejores prácticas para, entre otras cosas, facilitar el cambio de proveedores de servicios de tratamiento de datos y la portabilidad de datos. Dada la eficacia limitada de los marcos autorreguladores desarrollados como respuesta y la falta general de disponibilidad de normas e interfaces abiertas, es necesario adoptar un conjunto de obligaciones reglamentarias mínimas para los proveedores de servicios de tratamiento de datos a fin de eliminar los obstáculos contractuales, económicos y técnicos al cambio efectivo entre servicios de tratamiento de datos.

(71) Los servicios de tratamiento de datos deben abarcar los servicios que permiten un acceso remoto bajo demanda y amplio a un conjunto modulable y elástico de recursos informáticos distribuidos que se pueden compartir. Esos recursos informáticos incluyen recursos tales como las redes, los servidores u otras infraestructuras virtuales o físicas, sistemas operativos, *software*, en particular herramientas de desarrollo de

software, almacenamiento, aplicaciones y servicios. La capacidad del cliente del servicio de tratamiento de datos de autoabastecerse unilateralmente de capacidades de computación, como, por ejemplo, tiempo de servidor o almacenamiento en red, sin ninguna interacción humana por parte del proveedor de servicios podría describirse como administración bajo demanda. La expresión «acceso remoto amplio» se utiliza para describir que las capacidades de computación se suministran en toda la red y se accede a ellas a través de mecanismos que promueven el uso de plataformas de cliente ligero o pesado heterogéneas (desde navegadores a dispositivos móviles y estaciones de trabajo). El término «modulable» se refiere a los recursos de computación que el proveedor de servicios de tratamiento de datos puede asignar de manera flexible con independencia de la localización geográfica de los recursos para hacer frente a fluctuaciones de la demanda. El término «conjunto elástico» se usa para describir los recursos informáticos de los que se abastece y que se ponen a la venta según la demanda, de modo que se puedan aumentar o reducir con rapidez los recursos disponibles en función de la carga de trabajo. La expresión «que se pueden compartir» se usa para describir recursos informáticos que se proporcionan a múltiples usuarios que comparten un acceso común al servicio pero la tramitación se lleva a cabo por separado para cada usuario, aunque el servicio se preste desde el mismo equipo electrónico. El término «distribuido» se emplea para describir los recursos informáticos que se encuentran ubicados en distintos ordenadores o dispositivos conectados en red y que se comunican y coordinan entre sí intercambiando mensajes. El término «muy distribuido» se emplea para describir servicios de tratamiento de datos que implican tratar los datos más cerca del punto en que los datos se generan o recogen, por ejemplo en un dispositivo de tratamiento de datos conectado. La computación en el borde, que es un ejemplo de este tipo de tratamiento de datos muy distribuido, está previsto que genere nuevos modelos de negocio y de prestación de servicios de computación en nube, que deben ser abiertos e interoperables desde el principio.

(72) El objetivo del presente Reglamento es facilitar el cambio entre servicios de tratamiento de datos, que englobe todas las condiciones y acciones que son necesarias para que un cliente ponga fin a un acuerdo contractual con un servicio de tratamiento de datos, celebre uno o varios contratos nuevos con diferentes proveedores de servicios de tratamiento de datos, transmita todos sus activos digitales, incluidos datos, a los otros proveedores concernidos y continúe utilizándolos en el nuevo entorno, beneficiándose al mismo tiempo de la equivalencia funcional. Por activos digitales se entienden los elementos en formato digital respecto de los cuales el cliente tiene derecho de uso, como los datos, aplicaciones, máquinas virtuales y otras manifestaciones de tecnologías de virtualización, como los contenedores. Por equivalencia funcional se entiende el mantenimiento de un nivel mínimo de funcionalidad de un servicio después del cambio y debe considerarse técnicamente viable siempre que los dos servicios de tratamiento de datos, de origen y de destino, cubran (total o parcialmente) el mismo tipo de servicio. Los metadatos, generados por el uso de un servicio que hace el cliente, deben ser también portables de conformidad con las disposiciones relativas a los cambios del presente Reglamento.

(73) Cuando los proveedores de servicios de tratamiento de datos sean a su vez clientes de servicios de tratamiento de datos prestados por un tercer proveedor, ellos mismos se beneficiarán de cambios más efectivos, aunque estarán inevitablemente vinculados por las obligaciones del presente Reglamento en lo relativo a sus propias ofertas de servicios.

(74) Debe exigirse a los proveedores de servicios de tratamiento de datos que ofrezcan toda la asistencia y apoyo necesarios para que el proceso de cambio se realice con éxito y eficacia, sin exigir a dichos proveedores de servicios de tratamiento de datos que desarrollen nuevas categorías de servicios en el marco o sobre la base de la infraestructura informática de diferentes proveedores de servicios de tratamiento de datos para garantizar la equivalencia funcional en un entorno distinto del de sus propios sistemas. No obstante, los proveedores de servicios tienen obligación de ofrecer toda la asistencia y apoyo necesarios para que el proceso de cambio sea eficaz. Los derechos existentes en relación con la resolución de los contratos, incluidos los introducidos por el Reglamento (UE) 2016/679 y la Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo[67] no deben verse afectados.

(75) Para facilitar el cambio entre servicios de tratamiento de datos, los proveedores de servicios de tratamiento de datos deben considerar el uso de herramientas de ejecución y/o cumplimiento, en particular las publicadas por la Comisión en forma de un Código normativo relativo a los servicios en nube. En particular, las cláusulas contractuales tipo son beneficiosas para incrementar la confianza en los servicios de tratamiento de datos, crear una relación más equilibrada entre usuarios y proveedores de servicios y mejorar la seguridad jurídica sobre las condiciones aplicables para el cambio a otros servicios de tratamiento de datos. En este contexto, los usuarios y los proveedores de servicios deben considerar el uso de cláusulas contractuales tipo elaboradas por organismos o grupos de expertos competentes establecidos con arreglo al Derecho de la Unión.

(76) Las especificaciones y normas de interoperabilidad abiertas desarrolladas de conformidad con el anexo II, apartados 3 y 4, del Reglamento (UE) n.º 1025/2012 en el ámbito de la interoperabilidad y la portabilidad permiten un entorno en la nube multiproveedor sin fisuras, que constituye un requisito clave para la innovación abierta en la economía de los datos europea. Puesto que los procesos centrados en el mercado no han demostrado la capacidad de establecer especificaciones técnicas o normas que faciliten la interoperabilidad efectiva en la nube en los niveles PcS (plataforma como servicio) y ScS (*software* como servicio), la Comisión debe poder pedir a los organismos europeos de normalización, sobre la base del presente Reglamento y de conformidad con el Reglamento (UE) n.º 1025/2012, que elaboren dichas normas, en particular en el caso de los tipos de servicio para los que aún no existen tales normas. Además de ello, la Comisión animará a los actores del mercado a desarrollar las especificaciones de interoperabilidad abiertas pertinentes. La Comisión, mediante actos delegados, puede hacer obligatorio el uso de normas europeas de interoperabilidad o especificaciones de interoperabilidad abiertas para tipos de servicios específicos a través de una referencia en un repositorio central de normas de la Unión para la interoperabilidad de los servicios de tratamiento de datos. Las normas europeas y las especificaciones de interoperabilidad abiertas solo tendrán su referencia si son conformes a los criterios especificados en el presente Reglamento, que tienen el mismo significado que los requisitos de los puntos 3 y 4 del anexo II del Reglamento (UE) n.º 1025/2012 y las facetas de interoperabilidad definidas en la norma ISO/IEC 19941: 2017.

(77) Los terceros países pueden adoptar leyes, reglamentaciones y otros actos jurídicos que tengan por objeto transferir directamente o facilitar el acceso gubernamental a datos no

[67] Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales (DO L 136 de 22.5.2019, p. 1).

personales que se encuentran fuera de sus fronteras, en particular en la Unión. Las sentencias de órganos jurisdiccionales o las decisiones de autoridades judiciales o administrativas de terceros países, incluidas autoridades policiales de terceros países, que requieran dicha transferencia de datos no personales o el acceso a estos deben tener fuerza legal al amparo de un acuerdo internacional, como un tratado de asistencia judicial mutua, en vigor entre el tercer país solicitante y la Unión o un Estado miembro. En otros casos, pueden darse situaciones en las que una solicitud de transferir o dar acceso a datos no personales derivada de la legislación de un tercer país entre en conflicto con una obligación de proteger dichos datos en virtud de la legislación nacional o de la Unión, en particular en lo que se refiere a la protección de los derechos fundamentales de la persona, como el derecho a la seguridad y el derecho a la tutela judicial efectiva, o los intereses fundamentales de un Estado miembro relacionados con la seguridad o la defensa nacionales, así como la protección de los datos sensibles desde el punto de vista comercial, incluida la protección de los secretos comerciales, y la protección de los derechos de propiedad intelectual e industrial, y especialmente sus compromisos contractuales en materia de confidencialidad conforme a dicha legislación. Cuando no existan acuerdos internacionales que regulen estas cuestiones, la transferencia o el acceso solo han de permitirse si el ordenamiento jurídico del tercer país exige que se establezcan los motivos y la proporcionalidad de la decisión, que la resolución judicial o la decisión revista un carácter específico, y que la oposición motivada del destinatario sea revisada por un órgano jurisdiccional competente del tercer país, facultado para tomar debidamente en cuenta los intereses jurídicos pertinentes del proveedor de los datos. Cuando sea posible con arreglo a las condiciones de la solicitud de acceso a los datos de la autoridad del tercer país, el proveedor de servicios de tratamiento de datos debe poder informar al cliente cuyos datos se solicitan a fin de verificar la existencia de un conflicto potencial de dicho acceso con la normativa de la Unión o nacional, como la relativa a la protección de datos sensibles desde el punto de vista comercial, incluida la protección de los secretos comerciales, los derechos de propiedad intelectual e industrial y los compromisos contractuales en materia de confidencialidad.

(78) Para impulsar la confianza en los datos es esencial que las salvaguardas relativas a los ciudadanos, el sector público y las empresas de la Unión se apliquen en la medida de lo posible para garantizar que se ejerce control sobre sus datos. Además, deben respetarse el Derecho, los valores y las normas de la Unión en cuanto a la seguridad, la protección de los datos y de la vida privada, y la protección de los consumidores, entre otros aspectos. Con el fin de evitar el acceso ilícito a datos no personales, los proveedores de servicios de tratamiento de datos sujetos a este instrumento, como los servicios en la nube y en el borde, deben adoptar todas las medidas razonables para impedir el acceso a los sistemas en los que se almacenen datos no personales, incluso, cuando proceda, mediante el cifrado de datos, la sujeción frecuente a auditorías, el respeto verificado de los pertinentes sistemas de certificación de garantías de seguridad y la modificación de las políticas de empresa.

(79) La normalización y la interoperabilidad semántica deben desempeñar un papel clave para proporcionar soluciones técnicas que garanticen la interoperabilidad. A fin de facilitar la conformidad con los requisitos para la interoperabilidad es necesario establecer una presunción de conformidad para soluciones de interoperabilidad que cumplan las normas armonizadas o partes de las mismas de conformidad con el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo. La Comisión debe adoptar especificaciones comunes en ámbitos en los que no existan normas armonizadas o sean insuficientes para seguir mejorando la interoperabilidad de los

espacios comunes europeos de datos, las interfaces de programación de aplicaciones, el cambio de nube y los contratos inteligentes. Por otra parte, podrían quedar por adoptar especificaciones comunes en los distintos sectores, de conformidad con la legislación sectorial nacional o de la Unión, sobre la base de las necesidades específicas de dichos sectores. Estructuras y modelos de datos reutilizables (en forma de vocabularios básicos), ontologías, perfil de aplicación de metadatos, datos de referencia en forma de vocabulario básico, taxonomías, listas de códigos, cuadros de autoridades y tesauros también deben formar parte de las especificaciones técnicas de interoperabilidad semántica. Por otra parte, la Comisión debe estar facultada para hacer obligatorio el desarrollo de normas armonizadas para la interoperabilidad de los servicios de tratamiento de datos.

(80) A fin de promover la interoperabilidad de los contratos inteligentes en las aplicaciones de intercambio de datos, es necesario establecer requisitos esenciales para los contratos inteligentes para los profesionales que creen contratos inteligentes para terceros o integren dichos contratos inteligentes en aplicaciones que apoyen la ejecución de acuerdos de intercambio de datos. A fin de facilitar la conformidad de ese tipo de contratos inteligentes con dichos requisitos esenciales, es necesario establecer una presunción de conformidad para contratos inteligentes que cumplan las normas armonizadas o partes de las mismas de conformidad con el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo.

(81) A fin de garantizar la aplicación eficaz del presente Reglamento, los Estados miembros deben designar una o más autoridades competentes. Si un Estado miembro designa más de una autoridad competente, debe designar también una autoridad competente de coordinación. Es preciso que las autoridades competentes cooperen entre sí. Las autoridades responsables de la supervisión del cumplimiento de la protección de datos y las autoridades competentes designadas con arreglo a la legislación sectorial serán responsables de la aplicación del presente Reglamento en sus ámbitos de competencia.

(82) A fin de hacer valer sus derechos en virtud del presente Reglamento, las personas físicas y jurídicas deben tener derecho a solicitar reparación por la vulneración de sus derechos en virtud del presente Reglamento presentando denuncias ante las autoridades competentes. Dichas autoridades deben ser obligadas a cooperar para garantizar que la denuncia se gestione y resuelva adecuadamente. A fin de aprovechar el mecanismo de la red de cooperación en materia de protección de los consumidores y facilitar las acciones de representación, el presente Reglamento modifica los anexos del Reglamento (UE) 2017/2394 del Parlamento Europeo y del Consejo[68] y de la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo[69].

(83) Las autoridades competentes de los Estados miembros deben garantizar que el incumplimiento de las obligaciones establecidas en el presente Reglamento sea penalizado con sanciones. Al hacerlo, deben tener en cuenta la naturaleza, gravedad, reincidencia y duración de la infracción, atendiendo al interés público en juego, el

---

68 Reglamento (UE) 2017/2394 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2017, sobre la cooperación entre las autoridades nacionales responsables de la aplicación de la legislación en materia de protección de los consumidores y por el que se deroga el Reglamento (CE) n.º 2006/2004 (DO L 345 de 27.12.2017, p. 1).

69 Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020, relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, y por la que se deroga la Directiva 2009/22/CE (DO L 409 de 4.12.2020, p. 1).

alcance y el tipo de actividades realizadas, así como la capacidad económica del infractor. Deben tener en cuenta si el infractor incumple sistemática o repetidamente las obligaciones que le incumben en virtud del presente Reglamento. Con el fin de ayudar a las empresas a redactar y negociar contratos, la Comisión debe desarrollar y recomendar modelos de cláusulas contractuales no obligatorias para los contratos de intercambio de datos entre empresas, teniendo en cuenta, en su caso, las condiciones de sectores específicos y las prácticas existentes con mecanismos voluntarios de intercambio de datos. Estas cláusulas contractuales tipo serán principalmente una herramienta práctica para ayudar en particular a las empresas pequeñas a celebrar un contrato. Cuando se utilicen de forma generalizada e integral, estas cláusulas contractuales tipo también deben tener el efecto beneficioso de influir en el diseño de los contratos sobre el acceso y uso de datos y, por tanto, deben conducir en general a unas relaciones contractuales más justas a la hora de acceder a los datos y compartirlos.

(84) Con el fin de eliminar el riesgo de que titulares de datos que están en bases de datos obtenidos o generados por medio de componentes físicos, como sensores, de un producto conectado y de un servicio relacionado reclamen el derecho *sui generis* en virtud del artículo 7 de la Directiva 96/9/CE cuando dichas bases de datos no pueden acogerse al derecho *sui generis*, obstaculizando de este modo el ejercicio efectivo del derecho de los usuarios a acceder y utilizar los datos y el derecho a compartir datos con terceros en virtud del presente Reglamento, el presente Reglamento debe aclarar que el derecho *sui generis* no es aplicable a dichas bases de datos, ya que no se cumplirían los requisitos de protección.

(85) Con el fin de tener en cuenta los aspectos técnicos de los servicios de tratamiento de datos, los poderes para adoptar actos con arreglo al artículo 290 del TFUE deben delegarse en la Comisión por lo que respecta a complementar el presente Reglamento a fin de introducir un mecanismo de supervisión de las tasas por cambio impuestas por los proveedores de servicios de tratamiento de datos en el mercado, especificar más detalladamente los requisitos esenciales para los operadores de espacios de datos y los proveedores de servicios de tratamiento de datos en materia de interoperabilidad, y publicar la referencia de las especificaciones abiertas de interoperabilidad y las normas europeas para la interoperabilidad de los servicios de tratamiento de datos. Es particularmente importante que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que dichas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación, de 13 de abril de 2016[70]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(86) Con objeto de garantizar condiciones uniformes para la ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución en lo relativo a completar el presente Reglamento para adoptar especificaciones comunes que garanticen la interoperabilidad de espacios comunes europeos de datos y el intercambio de datos, el cambio entre servicios de tratamiento de datos, la interoperabilidad de los contratos inteligentes, así como para medios técnicos, como

[70] DO L 123 de 12.5.2016, p. 1.

las interfaces de programación de aplicaciones, para permitir la transmisión de datos entre las partes, también de forma continua o en tiempo real, y para vocabularios básicos de interoperabilidad semántica, así como para adoptar especificaciones comunes para los contratos inteligentes. Dichas competencias deberán ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo[71].

(87) El presente Reglamento no debe afectar a las disposiciones específicas de los actos de la Unión adoptados en el ámbito del intercambio de datos entre empresas, entre empresas y consumidores y entre empresas y organismos del sector público que fueran adoptados antes de la fecha de adopción del presente Reglamento. Para garantizar la coherencia y el buen funcionamiento del mercado interior, la Comisión debe evaluar, cuando proceda, la situación relativa a la relación entre el presente Reglamento y los actos adoptados antes de la fecha de adopción del presente Reglamento que regulan el intercambio de datos, a fin de evaluar la necesidad de adaptar dichas disposiciones específicas al presente Reglamento. El presente Reglamento debe entenderse sin perjuicio de las normas que aborden necesidades específicas de sectores o ámbitos de interés público concretos. Dichas normas pueden incluir requisitos adicionales sobre los aspectos técnicos del acceso a datos, como las interfaces para el acceso a datos, o sobre la forma de facilitar el acceso a datos, por ejemplo, directamente desde el producto o a través de servicios de intermediación de datos. Dichas normas también pueden incluir límites a los derechos de los titulares de datos a acceder a los datos de los usuarios o a utilizarlos, u otros aspectos que vayan más allá del acceso y el uso de datos, como los relacionados con la gobernanza. El presente Reglamento debe entenderse también sin perjuicio de normas más específicas en el contexto del desarrollo de espacios comunes europeos de datos.

(88) El presente Reglamento no debe afectar a la aplicación de las normas de competencia, en particular los artículos 101 y 102 del Tratado. Las medidas establecidas en el presente Reglamento no deben utilizarse para restringir la competencia de forma contraria al Tratado.

(89) Con el fin de permitir a los agentes económicos adaptarse a las nuevas normas establecidas en el presente Reglamento, estas deben ser aplicables en el plazo de un año a partir de la entrada en vigor del Reglamento.

(90) El Supervisor Europeo de Protección de Datos y el Comité Europeo de Protección de Datos, a los que se consultó de conformidad con el artículo 42, del Reglamento (UE) 2018/1725, emitieron un dictamen conjunto el [XX XX 2022].

[71] Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1
Objeto y ámbito de aplicación

1. El presente Reglamento establece normas armonizadas sobre la puesta a disposición de los datos generados por el uso de un producto o servicio relacionado para el usuario de dicho producto o servicio, sobre la puesta a disposición de datos por parte de los titulares de datos para los destinatarios de datos, y sobre la puesta a disposición de datos por parte de los titulares de datos para organismos del sector público o instituciones, organismos y órganos de la Unión, cuando exista una necesidad excepcional, para el desempeño de una misión realizada en interés público:

2. El presente Reglamento se aplica a:

   a) los fabricantes de productos y proveedores de servicios relacionados introducidos en el mercado de la Unión y los usuarios de dichos productos o servicios;

   b) titulares de datos que pongan datos a disposición de los destinatarios de datos de la Unión;

   c) destinatarios de datos de la Unión para los cuales se ponen a disposición datos;

   d) organismos del sector público e instituciones, organismos u órganos de la Unión que soliciten a los titulares de datos que pongan a disposición datos cuando exista una necesidad excepcional de esos datos para el cumplimiento de un cometido realizado en interés público y de los titulares de datos que faciliten esos datos en respuesta a dicha solicitud;

   e) proveedores de servicios de tratamiento de datos que ofrezcan dichos servicios a clientes de la Unión.

3. La legislación de la Unión en materia de protección de datos personales, protección de la vida privada y confidencialidad de las comunicaciones e integridad de los equipos terminales se aplicará a los datos personales tratados en relación con los derechos y obligaciones establecidos en el presente Reglamento. El presente Reglamento no afectará a la aplicabilidad del Derecho de la Unión relativo a la protección de datos personales, en particular del Reglamento (UE) 2016/679 y la Directiva 2002/58/CE, incluidos los poderes y competencias de las autoridades de control. En lo tocante a los derechos establecidos en el capítulo II del presente Reglamento, y cuando los usuarios sean los interesados de los datos personales sujetos a los derechos y obligaciones en virtud de dicho capítulo, las disposiciones del presente Reglamento complementarán el derecho a la portabilidad de los datos con arreglo al artículo 20 del Reglamento (UE) 2016/679.

4. El presente Reglamento no afectará a los actos jurídicos de la Unión y nacionales que contemplen el intercambio, el acceso y la utilización de datos con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluido el Reglamento (UE) 2021/784 del

Parlamento Europeo y del Consejo[72] y las [propuestas sobre pruebas electrónicas COM(2018) 225 y 226] una vez adoptadas, ni tampoco a la cooperación internacional en dicho ámbito. El presente Reglamento no afectará a la recogida, intercambio, acceso y utilización de datos en virtud de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, ni del Reglamento (UE) 2015/847 del Parlamento Europeo y del Consejo, relativo a la información que acompaña a las transferencias de fondos. El presente Reglamento no afectará a las competencias de los Estados miembros en relación con actividades relativas a la seguridad pública, la defensa, la seguridad nacional, las aduanas y la administración fiscal, ni a la salud y seguridad de los ciudadanos de conformidad con el Derecho de la Unión.

Artículo 2
Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «datos», cualquier representación digital de actos, hechos o información y cualquier compilación de tales actos, hechos o información, incluso en forma de grabación sonora, visual o audiovisual;

2) «producto», un bien mueble tangible, incluso incorporado en un bien inmueble, que obtiene, genera o recoge datos relativos a su uso o entorno y que puede comunicar datos a través de un servicio de comunicaciones electrónicas disponible para el público y cuya función primaria no es el almacenamiento ni el tratamiento de datos;

3) «servicio relacionado», un servicio digital, incluido el *software*, que está incorporado en un producto o interconectado con él de tal manera que su ausencia impediría al producto realizar una de sus funciones;

4) «asistentes virtuales», *software* que puede procesar peticiones, tareas o preguntas, incluso a partir de material de audio, material escrito, gestos o movimientos, y basándose en dichas peticiones, tareas o preguntas, acceder a servicios propios o de terceros o controlar dispositivos propios o de terceros;

5) «usuario», una persona física o jurídica que posee, alquila o arrienda un producto o recibe un servicio;

6) «titular de datos», una persona física o jurídica que tiene el derecho o la obligación, en virtud del presente Reglamento, del Derecho de la Unión aplicable o de la legislación nacional de ejecución del Derecho de la Unión, de poner a disposición determinados datos, o que, en el caso de los datos no personales y a través del control del diseño técnico del producto o servicios relacionados, tiene la capacidad de poner a disposición determinados datos;

7) «destinatario de datos», una persona física o jurídica que actúa con un propósito relacionado con su actividad comercial, empresa, oficio o profesión, distinta del usuario de un producto o servicio relacionado, a disposición de la cual el titular de datos pone los datos, incluso un tercero previa solicitud del usuario al titular de datos o de conformidad con una obligación legal en virtud del Derecho de la Unión o de la legislación nacional de ejecución del Derecho de la Unión;

[72] Reglamento (UE) 2021/784 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, sobre la lucha contra la difusión de contenidos terroristas en línea (DO L 172 de 17.5.2021, p. 79)

8) «empresa», una persona física o jurídica que, en relación con los contratos y prácticas contemplados por el presente Reglamento, actúa con fines relacionados con su actividad comercial, empresa, oficio o profesión;

9) «organismo del sector público», las autoridades nacionales, regionales o locales de los Estados miembros y las entidades de derecho público de los Estados miembros, o las asociaciones constituidas por una o más de dichas autoridades o por una o más de dichas entidades;

10) «emergencia pública», una situación excepcional que afecta negativamente a la población de la Unión, de un Estado miembro o de una parte de él, que entraña un riesgo de repercusiones graves y duraderas en las condiciones de vida o la estabilidad económica, o la degradación sustancial de los activos económicos de la Unión o del Estado miembro en cuestión;

11) «tratamiento», toda operación o conjunto de operaciones que se efectúa sobre datos o conjuntos de datos en formato electrónico, por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de puesta a disposición, alineación o interconexión, limitación, supresión o destrucción;

12) «servicio de tratamiento de datos», un servicio digital distinto de un servicio de contenidos en línea tal como se define en el artículo 2, apartado 5, del Reglamento (UE) 2017/1128, prestado a un cliente, que hace posible la administración bajo demanda y un acceso remoto amplio a un conjunto modulable y elástico de recursos informáticos que se pueden compartir, de carácter centralizado, distribuido o muy distribuido;

13) «tipo de servicio», un conjunto de servicios de tratamiento de datos que comparten el mismo objetivo primario y el modelo básico de servicio de tratamiento de datos;

14) «equivalencia funcional», el mantenimiento de un nivel mínimo de funcionalidad en el entorno de un nuevo servicio de tratamiento de datos tras el proceso de cambio, de tal manera que, en respuesta a una acción de entrada por parte del usuario en elementos esenciales del servicio, el servicio de destino suministra el mismo resultado con el mismo rendimiento y con el mismo nivel de seguridad, resiliencia operativa y calidad del servicio que el servicio de origen en el momento de la resolución del contrato;

15) «especificaciones de interoperabilidad abiertas», especificaciones técnicas de TIC, tal como se definen en el Reglamento (UE) n.º 1025/2012, que están orientadas, en función de los resultados, hacia la interoperabilidad entre servicios de tratamiento de datos;

16) «contrato inteligente», programa informático almacenado en un sistema de registro electrónico en el que el resultado de la ejecución del programa se registra en el libro mayor electrónico;

17) «libro mayor electrónico», un libro mayor electrónico en el sentido del artículo 3, punto 53, del Reglamento (UE) n.º 910/2014;

18) «especificaciones comunes», un documento, distinto de una norma, con soluciones técnicas que proponen una forma de cumplir determinados requisitos y obligaciones establecidos en el presente Reglamento;

19) «interoperabilidad», la capacidad de dos o más espacios de datos o redes, sistemas, productos, aplicaciones o componentes de comunicación para intercambiar y utilizar datos con el fin de desempeñar sus funciones;

20) «norma armonizada», una norma armonizada tal como se define en el artículo 2, punto 1, letra c), del Reglamento (UE) n.º 1025/2012.

CAPÍTULO II
INTERCAMBIO DE DATOS DE EMPRESA A CONSUMIDOR Y DE EMPRESA A EMPRESA

Artículo 3
Obligación de hacer accesibles los datos generados por el uso de productos o servicios relacionados

1. Los productos se diseñarán y fabricarán, y los servicios relacionados se prestarán, de manera tal que los datos generados por su uso sean, por defecto, accesibles para el usuario con facilidad, con seguridad, y cuando sea pertinente y proceda, directamente.

2. Antes de celebrar un contrato de compra, alquiler o arrendamiento de un producto o de un servicio relacionado, se facilitará al usuario como mínimo la siguiente información, en un formato claro y comprensible:

   a) el carácter y el volumen de los datos que probablemente genere el uso del producto o servicio relacionado;

   b) la probabilidad o no de que los datos se generen de forma continua y en tiempo real;

   c) el modo en que el usuario puede acceder a esos datos;

   d) si el fabricante que suministra el producto o el proveedor de servicios que presta el servicio relacionado tiene intención de usar los datos él mismo o de permitir a un tercero el uso de los datos y, de ser así, los fines para los que se utilizarán dichos datos;

   e) si el vendedor, o el arrendador, son el titular de los datos y, en caso contrario, la identidad del titular de los datos, como su nombre comercial y la dirección geográfica en la que está establecido;

   f) los medios de comunicación que permitan al usuario ponerse rápidamente en contacto con el titular de datos y comunicarse con él de manera eficiente;

   g) el modo en que el usuario puede solicitar que los datos se compartan con un tercero;

   h) el derecho del usuario a presentar una reclamación relativa a la infracción de las disposiciones del presente capítulo ante la autoridad competente a que se refiere el artículo 31.

Artículo 4

Derecho de los usuarios a acceder y utilizar datos generados por el uso de productos o servicios relacionados

1. Cuando el usuario no pueda acceder directamente a los datos desde el producto, el titular de datos pondrá a disposición del usuario los datos generados por su uso de un producto o servicio relacionado sin demora indebida, gratuitamente y, cuando proceda, de forma continua y en tiempo real. Esto se hará sobre la base de una simple solicitud por medios electrónicos cuando sea técnicamente viable.

2. El titular de datos no exigirá al usuario que facilite ninguna información que vaya más allá de lo necesario para verificar su condición de usuario con arreglo al apartado 1. El titular de datos no conservará ninguna información sobre el acceso del usuario a los datos solicitados más allá de lo necesario para la correcta ejecución de la solicitud de acceso del usuario y para la seguridad y el mantenimiento de la infraestructura de datos.

3. Los secretos comerciales solo se desvelarán a condición de que se adopten todas las medidas específicas necesarias para preservar la confidencialidad de los secretos comerciales, en particular con respecto a terceros. El titular de datos y el usuario pueden acordar medidas para preservar la confidencialidad de los datos compartidos, en particular en relación con terceros.

4. El usuario no utilizará los datos obtenidos con arreglo a una solicitud contemplada en el apartado 1 para desarrollar un producto que compita con el producto del que proceden los datos.

5. Cuando el usuario no sea un interesado, el titular de datos solo pondrá a disposición del usuario los datos personales generados por el uso de un producto o servicio relacionado cuando exista una base jurídica válida con arreglo al artículo 6, apartado 1, del Reglamento (UE) 2016/679 y, en su caso, se cumplan las condiciones del artículo 9 del Reglamento (UE) 2016/679.

6. El titular de datos solo utilizará los datos no personales generados por el uso de un producto o servicio relacionado sobre la base de un acuerdo contractual con el usuario. El titular de datos no utilizará dichos datos generados por el uso del producto o servicio relacionado para obtener información sobre la situación económica, los activos y los métodos de producción del usuario, ni sobre el uso por parte de este, susceptible de socavar la posición comercial del usuario en los mercados en los que el usuario opera.

Artículo 5

Derecho a compartir datos con terceros

1. A petición de un usuario o de una parte que actúe en nombre de un usuario, el titular de datos pondrá a disposición de un tercero los datos generados por el uso de un producto o servicio relacionado, sin demora indebida y gratuitamente para el usuario, con la misma calidad que está a disposición del titular de datos y, en su caso, de forma continua y en tiempo real.

2. Ninguna empresa que preste servicios básicos de plataforma respecto de la cual uno o más de dichos servicios hayan sido designados guardianes de acceso, de conformidad con el artículo [...] del [Reglamento XXX sobre mercados disputables y

equitativos en el sector digital (Ley de Mercados Digitales)[73]], podrá ser un tercero elegible en virtud del presente artículo y, por tanto, no podrá:

a) instar o incentivar comercialmente a un usuario de ninguna manera, incluso ofreciendo una compensación monetaria o de otro tipo, para que ponga a disposición de uno de sus servicios datos que el usuario haya obtenido en virtud de una solicitud con arreglo al artículo 4, apartado 1;

b) instar o incentivar comercialmente a un usuario para que solicite al titular de datos que ponga a disposición de uno de sus servicios datos en virtud del apartado 1 del presente artículo;

c) recibir datos de un usuario que este haya obtenido en virtud de una solicitud con arreglo al artículo 4, apartado 1.

3. No se exigirá al usuario ni al tercero que faciliten ninguna información que vaya más allá de lo necesario para verificar su condición de usuario o de tercero con arreglo al apartado 1. El titular de datos no conservará ninguna información sobre el acceso del tercero a los datos solicitados más allá de lo necesario para la correcta ejecución de la solicitud de acceso del tercero y para la seguridad y el mantenimiento de la infraestructura de datos.

4. El tercero no usará medios coercitivos ni abusará de las lagunas evidentes de la infraestructura técnica del titular de datos diseñada para proteger los datos con el fin de obtener acceso a los datos.

5. El titular de datos no utilizará ningún dato no personal generado por el uso del producto o servicio relacionado con el fin de obtener información sobre la situación económica, los activos o los métodos de producción del tercero, ni sobre el uso por parte de este, que pueda socavar la posición comercial del tercero en los mercados en los que opera, a menos que el tercero haya dado su consentimiento para tal uso y tenga la posibilidad técnica de retirar dicho consentimiento en cualquier momento.

6. Cuando el usuario no sea un interesado, los datos personales generados por el uso de un producto o servicio relacionado solo podrán ponerse a disposición cuando exista una base jurídica válida con arreglo al artículo 6, apartado 1, del Reglamento (UE) 2016/679 y, en su caso, se cumplan las condiciones del artículo 9 del Reglamento (UE) 2016/679.

7. El hecho de que el titular de datos y el tercero no lleguen a un acuerdo sobre las modalidades de transmisión de los datos no obstaculizará, evitará ni interferirá en el ejercicio de los derechos del interesado en virtud del Reglamento (UE) 2016/679 y, en particular, en el derecho a la portabilidad de los datos con arreglo al artículo 20 de dicho Reglamento.

8. Los secretos comerciales solo se desvelarán a terceros en la medida en que sea estrictamente necesario para cumplir el objetivo acordado entre el usuario y el tercero, y el tercero adopte todas las medidas específicas necesarias acordadas entre el titular de datos y el tercero para preservar la confidencialidad del secreto comercial. En tal caso, la consideración de los datos como secretos comerciales y las medidas para preservar la confidencialidad se especificarán en el acuerdo entre el titular de datos y el tercero.

[73] DO […].

9. El derecho a que se refiere el apartado 1 no afectará negativamente a los derechos de protección de datos de otras partes.

Artículo 6

Obligaciones de terceros que reciben datos a petición del usuario

1. Los terceros tratarán los datos que se pongan a su disposición con arreglo al artículo 5 únicamente para los fines y en las condiciones acordadas con el usuario, y sin perjuicio de los derechos del interesado en lo que respecta a los datos personales, y suprimirán los datos cuando ya no sean necesarios para la finalidad acordada.

2. El tercero no podrá:

   a) coaccionar, engañar o manipular al usuario de ningún modo, perjudicando o socavando la autonomía, la toma de decisiones o las opciones del usuario, ni tampoco utilizar una interfaz digital con el usuario;

   b) utilizar los datos que reciba para la elaboración de perfiles de personas físicas en el sentido del artículo 4, apartado 4, del Reglamento (UE) 2016/679, a menos que sea necesario para prestar el servicio solicitado por el usuario;

   c) poner los datos que reciba a disposición de otro tercero, en formato sin procesar, agregado o derivado, a menos que sea necesario para prestar el servicio solicitado por el usuario;

   d) poner los datos que reciba a disposición de una empresa que preste servicios básicos de plataforma respecto de la cual uno o más de dichos servicios hayan sido designados guardianes de acceso con arreglo al artículo [...] del [Reglamento sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales)];

   e) utilizar los datos que reciba para desarrollar un producto que compita con el producto del que proceden los datos a los que ha accedido ni compartir los datos con otro tercero con tal finalidad;

   f) impedir al usuario, en particular mediante compromisos contractuales, poner los datos que reciba a disposición de otras partes.

Artículo 7

Ámbito de aplicación de las obligaciones de intercambio de datos de empresa a consumidor y de empresa a empresa

1. Las obligaciones del presente capítulo no se aplicarán a los datos generados por el uso de productos fabricados o servicios relacionados prestados por empresas que se consideren microempresas o pequeñas empresas, tal como se definen en el artículo 2 del anexo de la Recomendación 2003/361/CE, siempre que dichas empresas no tengan empresas asociadas o empresas vinculadas, según la definición del artículo 3 del anexo de la Recomendación 2003/361/CE, que no puedan considerarse microempresas o pequeñas empresas.

2. Cuando el presente Reglamento se refiera a productos o servicios relacionados, se entenderá que dicha referencia incluye también a los asistentes virtuales, en la medida en que se utilicen para acceder a un producto o servicio relacionado o para controlarlo.

CAPÍTULO III
OBLIGACIONES DE LOS TITULARES DE DATOS LEGALMENTE OBLIGADOS A PONER LOS DATOS A DISPOSICIÓN

Artículo 8
Condiciones en las que los titulares de datos ponen datos a disposición de los destinatarios de datos

1. Cuando un titular de datos esté obligado a poner datos a disposición de un destinatario de datos en virtud del artículo 5 o de otra normativa de la Unión o de legislación nacional de ejecución del Derecho de la Unión, lo hará en condiciones justas, razonables y no discriminatorias y de una forma transparente, de conformidad con lo dispuesto en el presente capítulo y en el capítulo IV.

2. El titular de datos acordará con el destinatario de datos las condiciones para la puesta a disposición de los datos. Ninguna cláusula contractual sobre el acceso a los datos y su utilización o sobre la responsabilidad y las vías de recurso por incumplimiento o resolución de obligaciones relativas a datos será vinculante si cumple las condiciones del artículo 13 o si excluye la aplicación, establece excepciones o modifica los derechos del usuario en virtud del capítulo II.

3. El titular de los datos no discriminará entre categorías comparables de destinatarios de datos, incluidas las empresas asociadas o las empresas vinculadas, tal como se definen en el artículo 3 del anexo de la Recomendación 2003/361/CE, del titular de los datos, cuando se pongan a disposición los datos. Cuando un destinatario de datos considere que las condiciones en las que se han puesto a su disposición los datos son discriminatorias, corresponderá al titular de los datos demostrar que no ha habido discriminación.

4. El titular de los datos no pondrá los datos a disposición de un destinatario de datos con carácter exclusivo a menos que lo solicite el usuario con arreglo al capítulo II.

5. Los titulares de datos y los destinatarios de datos no estarán obligados a facilitar ninguna información que vaya más allá de lo necesario para verificar el cumplimiento de las condiciones contractuales acordadas para la puesta a disposición de los datos o de sus obligaciones en virtud del presente Reglamento o de otra legislación de la Unión aplicable o de legislación nacional de ejecución del Derecho de la Unión.

6. Salvo disposición en contrario del Derecho de la Unión, incluido el artículo 6 del presente Reglamento, o de legislación nacional de ejecución del Derecho de la Unión, la obligación de poner los datos a disposición de un destinatario de datos no obligará a la divulgación de secretos comerciales en el sentido de la Directiva (UE) 2016/943.

Artículo 9
Compensación por la puesta a disposición de los datos

1. Toda compensación acordada entre un titular de datos y un destinatario de datos por la puesta a disposición de los datos deberá ser razonable.

2. Cuando el destinatario de datos sea una microempresa o una pequeña o mediana empresa, conforme a la definición del artículo 2 del anexo de la Recomendación 2003/361/CE, toda compensación que se acuerde no deberá superar los costes directamente relacionados con la puesta a disposición del destinatario de los mismos y que sean atribuibles a la solicitud. El artículo 8, apartado 3, será de aplicación a estos efectos.

3. El presente artículo no será óbice para que otra legislación de la Unión u otra legislación nacional de ejecución del Derecho de la Unión excluyan la compensación por la puesta a disposición de datos o prevean una indemnización inferior.

4. El titular de datos facilitará al destinatario de datos información que contenga la base para el cálculo de la compensación con el suficiente detalle para que el destinatario de datos pueda verificar que se cumplen los requisitos del apartado 1 y, en su caso, del apartado 2.

Artículo 10
Resolución de litigios

1. Los titulares de datos y los destinatarios de datos tendrán acceso a órganos de resolución de litigios, certificados de conformidad con el apartado 2 del presente artículo, para resolver litigios en relación con la determinación de condiciones justas, razonables y no discriminatorias para poner los datos a disposición y de la forma transparente de hacerlo, de conformidad con los artículos 8 y 9.

2. A petición del órgano de resolución de litigios, el Estado miembro en el que esté establecido dicho órgano lo certificará, siempre que el órgano haya demostrado que cumple todas las condiciones siguientes:

   a) es imparcial e independiente, y dictará sus resoluciones con arreglo a unas normas de procedimiento claras y justas;

   b) dispone de los conocimientos técnicos necesarios relativos a la determinación de condiciones justas, razonables y no discriminatorias aplicables a la puesta a disposición de datos y la manera de hacerlo con transparencia, que permiten que el órgano pueda determinar efectivamente dichas condiciones;

   c) es fácilmente accesible a través de tecnologías de comunicación electrónicas;

   d) es capaz de adoptar sus decisiones de manera rápida, eficiente y rentable y al menos en una de las lenguas oficiales de la Unión.

   Si a más tardar el [fecha de aplicación del Reglamento] no hay ningún órgano de resolución de litigios certificado en un Estado miembro, dicho Estado miembro deberá constituir y certificar un órgano de resolución de litigios que cumpla las condiciones establecidas en las letras a) a d) del presente apartado.

3. Los Estados miembros notificarán a la Comisión los órganos de resolución de litigios certificados de conformidad con el apartado 2. La Comisión publicará la lista de dichos órganos en un sitio web específico y la mantendrá actualizada.

4. Los órganos de resolución de litigios darán a conocer las tasas, o los mecanismos utilizados para determinar las tasas, a las partes afectadas antes de que estas soliciten una decisión.

5. Los órganos de resolución de litigios rechazarán tratar cualquier solicitud de resolución de un litigio que ya se haya presentado ante otro órgano de resolución de litigios o ante un órgano jurisdiccional de un Estado miembro.

6. Los órganos de resolución de litigios brindarán a las partes la posibilidad de expresar, en un plazo razonable, su punto de vista sobre los asuntos que esas partes hayan sometido a dichos órganos. En ese contexto, los órganos de resolución de litigios facilitarán a dichas partes las observaciones de la otra parte y cualquier declaración realizada por expertos. Dichos órganos brindarán a las partes la posibilidad de presentar comentarios sobre dichas observaciones y declaraciones.

7. Los órganos de resolución de litigios emitirán su decisión sobre los asuntos que les sean remitidos a más tardar 90 días después de que se haya formulado la solicitud de decisión. Dichas decisiones se formularán por escrito o en un soporte duradero y se apoyarán mediante una exposición de motivos que justifique la decisión.

8. La decisión del órgano de resolución de litigios solo será vinculante para las partes si estas han dado su consentimiento explícito a su carácter vinculante antes del inicio del procedimiento de resolución de litigios.

9. El presente artículo no afectará al derecho de las partes a interponer un recurso efectivo ante un órgano jurisdiccional de un Estado miembro.

Artículo 11

Medidas técnicas de protección y disposiciones sobre la utilización o divulgación no autorizadas de datos

1. El titular de datos podrá aplicar medidas técnicas de protección adecuadas, incluidos contratos inteligentes, para impedir el acceso no autorizado a los datos y garantizar el cumplimiento de los artículos 5, 6, 9 y 10, así como de las condiciones contractuales acordadas para la puesta a disposición de los datos. Dichas medidas técnicas de protección no se utilizarán como medio para obstaculizar el derecho del usuario a facilitar datos a terceros de manera efectiva de conformidad con el artículo 5 ni ningún derecho de un tercero en virtud del Derecho de la Unión o de legislación nacional de ejecución del Derecho de la Unión a que se refiere el artículo 8, apartado 1.

2. Un destinatario de datos que, con el fin de obtener datos, haya facilitado información inexacta o falsa al titular de datos, haya utilizado medios engañosos o coercitivos o haya abusado de lagunas evidentes en la infraestructura técnica del titular de datos destinada a proteger los datos, haya utilizado los datos puestos a disposición con fines no autorizados o haya desvelado dichos datos a otra parte sin la autorización del titular de datos, deberá, sin demora indebida, a menos que el titular de datos o el usuario instruya otra cosa:

   a) destruir los datos puestos a disposición por el titular de datos y cualquier copia de los mismos;

   b) poner fin a la producción, la oferta, la puesta en el mercado o el uso de bienes, datos derivados o servicios producidos sobre la base de los conocimientos obtenidos a través de dichos datos, o a la importación, exportación o almacenamiento de mercancías infractoras con esos fines, y destruir cualquier mercancía infractora.

3. El apartado 2, letra b), no será aplicable en ninguno de los casos siguientes:

a) el uso de los datos no ha causado un perjuicio significativo al titular de datos;

b) la aplicación de las disposiciones previstas sería desproporcionada a la luz de los intereses del titular de datos.

Artículo 12
Ámbito de aplicación de las obligaciones de los titulares de datos legalmente obligados a poner los datos a disposición

1. El presente capítulo se aplicará cuando el titular de datos esté obligado, en virtud del artículo 5, o en virtud del Derecho de la Unión o de legislación nacional de ejecución del Derecho de la Unión, a poner los datos a disposición de un destinatario de datos.

2. Ninguna cláusula contractual de un acuerdo de intercambio de datos que, en detrimento de una de las partes o, en su caso, en detrimento del usuario, excluya la aplicación del presente capítulo, establezca excepciones al mismo o modifique sus efectos, será vinculante para esa parte.

3. El presente capítulo solo se aplicará en relación con las obligaciones de puesta a disposición de los datos en virtud del Derecho de la Unión o de legislación nacional de ejecución del Derecho de la Unión, que entren en vigor después del [fecha de aplicación del Reglamento].

CAPÍTULO IV
CLÁUSULAS ABUSIVAS ENTRE EMPRESAS EN RELACIÓN CON EL ACCESO A LOS DATOS Y SU UTILIZACIÓN

Artículo 13
Cláusulas contractuales abusivas impuestas unilateralmente a microempresas, pequeñas o medianas empresas

1. Las cláusulas contractuales sobre el acceso a los datos y su utilización o sobre la responsabilidad y las vías de recurso por incumplimiento o resolución de obligaciones relativas a datos que hayan sido impuestas unilateralmente por una empresa a una microempresa o una pequeña o mediana empresa, según la definición del artículo 2 del anexo de la Recomendación 2003/361/CE, no serán vinculantes en caso de ser abusivas.

2. Una cláusula contractual será abusiva si, por su naturaleza, su aplicación se aparta manifiestamente de las buenas prácticas comerciales en materia de acceso a los datos y su utilización, en contravención de los principios de buena fe y comercio justo.

3. A los efectos del presente artículo, una cláusula contractual será abusiva si tiene por objeto o efecto:

a) excluir o limitar la responsabilidad de la parte que haya impuesto unilateralmente la cláusula en caso de acciones intencionadas o negligencia grave;

b) excluir las vías de recurso de que dispone la parte a la que se haya impuesto unilateralmente la cláusula en caso de incumplimiento de obligaciones contractuales o la responsabilidad de la parte que haya impuesto unilateralmente la cláusula en caso de infracción de dichas obligaciones;

c) otorgar a la parte que haya impuesto unilateralmente la cláusula el derecho exclusivo de determinar si los datos facilitados son acordes con el contrato o de interpretar cualquier cláusula del contrato.

4. A los efectos del presente artículo, se presumirá que una cláusula contractual es abusiva si tiene por objeto o efecto:

a) limitar de forma inadecuada las vías de recurso en caso de incumplimiento de obligaciones contractuales o la responsabilidad en caso de infracción de dichas obligaciones;

b) permitir a la parte que haya impuesto unilateralmente la cláusula acceder a los datos de la otra parte contratante y utilizarlos de manera que cause un grave perjuicio a los intereses legítimos de dicha otra parte;

c) impedir a la parte a la que se haya impuesto unilateralmente la cláusula utilizar los datos que haya aportado o generado durante el período de vigencia del contrato, o limitar la utilización de estos datos en tal medida que esa parte no pueda utilizar, recopilar ni controlar esos datos, ni acceder a ellos, ni explotar su valor de manera proporcionada;

d) impedir a la parte a la que se haya impuesto unilateralmente la cláusula obtener una copia de los datos que haya aportado o generado durante el período de vigencia del contrato o dentro de un plazo razonable tras su resolución;

e) permitir a la parte que haya impuesto unilateralmente la cláusula resolver el contrato con un plazo de preaviso excesivamente corto, habida cuenta de las posibilidades razonables de la otra parte contratante de cambiar a un servicio alternativo y comparable y del perjuicio financiero ocasionado por esa resolución, salvo cuando haya razones fundadas para hacerlo.

5. Se considerará que una cláusula contractual se ha impuesto unilateralmente en la acepción del presente artículo si ha sido aportada por una de las partes contratantes sin que la otra parte contratante haya podido influir en su contenido pese a haber intentado negociarlo. Corresponderá a la parte contratante que haya aportado una cláusula contractual demostrar que no ha sido impuesta unilateralmente.

6. En caso de que la cláusula contractual abusiva sea disociable de las demás cláusulas del contrato, estas seguirán siendo vinculantes.

7. El presente artículo no se aplicará a las cláusulas comerciales del objeto principal del contrato ni a las que determinen el precio a pagar.

8. Las partes de un contrato que entre en el ámbito de aplicación del apartado 1 no podrán excluir la aplicación del presente artículo, establecer excepciones al mismo ni modificar sus efectos.

CAPÍTULO V
PUESTA DE LOS DATOS A DISPOSICIÓN DE LOS ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS INSTITUCIONES, ÓRGANOS U ORGANISMOS DE LA UNIÓN EN RAZÓN DE UNA NECESIDAD EXCEPCIONAL

Artículo 14
Obligación de facilitar datos en razón de una necesidad excepcional

1. Previa solicitud, un titular de datos facilitará datos a un organismo del sector público o de una institución, órgano u organismo de la Unión que demuestre la existencia de una necesidad excepcional de utilizar los datos solicitados.

2. El presente capítulo no será de aplicación a las microempresas ni a las pequeñas empresas, según se definen en el artículo 2 del anexo de la Recomendación 2003/361/CE.

Artículo 15
Necesidad excepcional de utilizar los datos

Se considerará que existe una necesidad excepcional de utilizar los datos en la acepción del presente capítulo en cualquiera de las circunstancias siguientes:

a) cuando los datos solicitados sean necesarios para responder a una emergencia pública;

b) cuando la solicitud de datos esté limitada en el tiempo y en su ámbito de aplicación y sea necesaria para prevenir una emergencia pública o para ayudar a la recuperación tras una emergencia pública;

c) cuando la falta de datos disponibles impida al organismo del sector público o a la institución, órgano u organismo de la Unión desempeñar una tarea específica de interés público que esté explícitamente prevista por ley; y

   1) el organismo del sector público o la institución, órgano u organismo de la Unión no haya podido obtener esos datos por medios alternativos, en particular mediante la compra de datos en el mercado a precios de mercado o apoyándose en obligaciones existentes de facilitar los datos, y la adopción de nuevas medidas legislativas no pueda garantizar la disponibilidad oportuna de los datos; o

   2) la obtención de los datos de acuerdo con el procedimiento establecido en el presente capítulo reduciría en una medida sustancial la carga administrativa para los titulares de datos u otras empresas.

Artículo 16
Relación con otras obligaciones de facilitar datos a organismos del sector público e instituciones, órganos y organismos de la Unión

1. El presente capítulo no afectará a las obligaciones establecidas en el Derecho de la Unión o nacional a efectos de la presentación de informes, el cumplimiento de solicitudes de información o la demostración o verificación del cumplimiento de obligaciones legales.

2. Los organismos del sector público y las instituciones, órganos y organismos de la Unión no ejercerán los derechos contemplados en el presente capítulo con objeto de llevar a cabo actividades para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o administrativas o de ejecución de sanciones penales, ni de administración aduanera o tributaria. El presente capítulo no afecta al Derecho de la Unión y nacional aplicable en materia de prevención, investigación, detección o enjuiciamiento de infracciones penales o administrativas o de ejecución de sanciones penales o administrativas, ni de administración aduanera o tributaria.

Artículo 17
Solicitudes de puesta a disposición de datos

1. Cuando un organismo del sector público o una institución, órgano u organismo de la Unión solicite datos con arreglo al artículo 14, apartado 1, deberá:

   a) especificar qué datos necesita;

   b) demostrar la necesidad excepcional para la que solicita los datos;

   c) explicar el objeto de la solicitud, la utilización prevista de los datos solicitados y la duración de dicha utilización;

   d) indicar la base jurídica que sustenta la solicitud de los datos;

   e) especificar el plazo en que deben facilitarse los datos o en que el titular de datos puede pedir al organismo del sector público o a la institución, órgano u organismo de la Unión que modifique o retire la solicitud.

2. Toda solicitud de datos presentada con arreglo al apartado 1 del presente artículo deberá:

   a) expresarse en un lenguaje claro, conciso y sencillo comprensible para el titular de datos;

   b) guardar proporción con la necesidad excepcional, en cuanto a la granularidad y volumen de los datos solicitados y la frecuencia de acceso a los datos solicitados;

   c) respetar los objetivos legítimos del titular de datos, teniendo en cuenta la protección de los secretos comerciales y el coste y el esfuerzo necesarios para facilitar los datos;

   d) en la medida de lo posible, referirse a datos no personales;

   e) informar al titular de datos de las sanciones que impondrá de conformidad con el artículo 33 una autoridad competente con arreglo al artículo 31 en caso de que no se atienda la solicitud;

   f) ponerse a disposición del público por internet sin demora indebida.

3. Un organismo del sector público o una institución, órgano u organismo de la Unión no facilitará datos obtenidos de conformidad con el presente capítulo para su reutilización en la acepción de la Directiva (UE) 2019/1024. La Directiva (UE) 2019/1024 no será de aplicación a los datos que obren en poder de los organismos del sector público obtenidos conforme al presente capítulo.

4. Lo dispuesto en el apartado 3 no impedirá al organismo del sector público o la institución, órgano u organismo de la Unión intercambiar los datos obtenidos con arreglo al presente capítulo con otro organismo del sector público u otra institución,

órgano u organismo de la Unión con el fin de completar las tareas a que se refiere el artículo 15 ni poner los datos a disposición de un tercero en los casos en que haya externalizado, mediante un acuerdo de acceso público, inspecciones técnicas u otras funciones respecto a ese tercero. Serán de aplicación las obligaciones de los organismos del sector público y las instituciones, órganos u organismos de la Unión previstas en el artículo 19.

Cuando un organismo del sector público o una institución, órgano u organismo de la Unión transmita o facilite datos en aplicación del presente apartado, lo notificará al titular de datos del que haya recibido los datos.

Artículo 18
Cumplimiento de las solicitudes de datos

1. Cuando un titular de datos reciba una solicitud de acceso a los datos con arreglo al presente capítulo, pondrá los datos a disposición del organismo del sector público o la institución, órgano u organismo de la Unión solicitante sin demora indebida.

2. Sin perjuicio de las necesidades específicas en relación con la disponibilidad de datos definidas en la legislación sectorial, el titular de datos podrá denegar la solicitud o pedir su modificación en un plazo de cinco días hábiles a partir de la recepción de la solicitud de los datos necesarios para responder a una emergencia pública, y en el plazo de quince días hábiles en otros casos de necesidad excepcional, basándose en uno de los siguientes motivos:

   a) que los datos no estén disponibles;

   b) que la solicitud no reúna las condiciones establecidas en el artículo 17, apartados 1 y 2.

3. En caso de solicitud de los datos necesarios para responder a una emergencia pública, el titular de datos también podrá denegar la solicitud o pedir su modificación cuando ya haya facilitado los datos solicitados en respuesta a una solicitud presentada previamente con la misma finalidad por otro organismo del sector público u otra institución, órgano u organismo de la Unión y no se haya notificado al titular de datos la destrucción de los datos con arreglo al artículo 19, apartado 1, letra c).

4. En caso de que el titular de datos decida denegar la solicitud o pedir su modificación de conformidad con el apartado 3, indicará la identidad del organismo del sector público o de la institución, órgano u organismo de la Unión que haya presentado previamente una solicitud con la misma finalidad.

5. Cuando el cumplimiento de la solicitud de facilitar datos a un organismo del sector público o a una institución, órgano u organismo de la Unión exija la divulgación de datos personales, el titular de datos hará esfuerzos razonables para seudonimizar los datos, en la medida en que la solicitud pueda ser atendida con datos seudonimizados.

6. Cuando el organismo del sector público o la institución, órgano u organismo de la Unión desee impugnar la negativa del titular de datos a facilitar los datos solicitados, o su petición de modificar la solicitud, o cuando el titular de datos desee impugnar la solicitud, la cuestión será remitida a la autoridad competente contemplada en el artículo 31.

Artículo 19

Obligaciones de los organismos del sector público y de las instituciones, órganos y organismos de la Unión

1. Un organismo del sector público o una institución, órgano u organismo de la Unión que haya recibido datos en respuesta a una solicitud presentada con arreglo al artículo 14:

   a) no podrá utilizar los datos de manera incompatible con la finalidad para la que hayan sido solicitados;

   b) en la medida en que el tratamiento de datos personales resulte necesario, aplicará medidas técnicas y organizativas que protejan los derechos y libertades de los interesados;

   c) destruirá los datos en cuanto dejen de ser necesarios para la finalidad indicada e informará al titular de datos de su destrucción.

2. La divulgación de secretos comerciales o de supuestos secretos comerciales a un organismo del sector público o a una institución, órgano u organismo de la Unión solo se exigirá en la medida en que sea estrictamente necesario para cumplir la finalidad de la solicitud. En ese caso, el organismo del sector público o la institución, órgano u organismo de la Unión adoptará medidas adecuadas para preservar la confidencialidad de dichos secretos comerciales.

Artículo 20

Compensación en caso de necesidad excepcional

1. La puesta a disposición de datos en respuesta a una emergencia pública con arreglo al artículo 15, letra a), será gratuita.

2. Cuando el titular de datos reclame una compensación por facilitar datos en respuesta a una solicitud presentada con arreglo al artículo 15, letras b) o c), la compensación no excederá de los costes técnicos y organizativos soportados para dar cumplimiento a la solicitud, incluidos, en su caso, los costes de anonimización y de adaptación técnica, más un margen razonable. A petición del organismo del sector público o de la institución, órgano u organismo de la Unión que solicite los datos, el titular de datos facilitará información sobre la base de cálculo de los costes y del margen razonable.

Artículo 21

Contribución de los organismos de investigación o institutos de estadística en el contexto de las necesidades excepcionales

1. Un organismo del sector público o una institución, órgano u organismo de la Unión tendrá derecho a compartir con personas físicas u organizaciones los datos recibidos de conformidad con el presente capítulo a fin de llevar a cabo actividades de investigación científica o análisis compatibles con la finalidad para la que se hayan solicitado los datos, o con institutos nacionales de estadística y Eurostat para la recopilación de estadísticas oficiales.

2. Las personas físicas u organizaciones que reciban los datos con arreglo al apartado 1 actuarán sin fines lucrativos o en el contexto de una misión de interés público reconocida en el Derecho de la Unión o del Estado miembro correspondiente. Quedarán excluidas las organizaciones sujetas a una influencia decisiva de empresas

comerciales o que puedan dar a estas un acceso preferente a los resultados de la investigación.

3. Las personas físicas u organizaciones que reciban los datos con arreglo al apartado 1 cumplirán las disposiciones del artículo 17, apartado 3, y del artículo 19.

4. Cuando un organismo del sector público o una institución, órgano u organismo de la Unión transmita o facilite datos en aplicación del apartado 1, lo notificará al titular de datos del que haya recibido los datos.

Artículo 22
Asistencia mutua y cooperación transfronteriza

1. Los organismos del sector público e instituciones, órganos y organismos de la Unión cooperarán y se asistirán mutuamente con el fin de aplicar el presente capítulo de manera coherente.

2. Los datos compartidos en el contexto de la petición y prestación de asistencia con arreglo al apartado 1 no podrán utilizarse de manera incompatible con la finalidad prevista en la petición.

3. Cuando un organismo del sector público prevea solicitar datos a un titular de datos establecido en otro Estado miembro, notificará previamente su intención a la autoridad competente de ese Estado miembro a que se refiere el artículo 31. Este requisito será también de aplicación a las solicitudes de las instituciones, órganos y organismos de la Unión.

4. Tras la notificación de conformidad con el apartado 3, la autoridad competente pertinente asesorará al organismo del sector público solicitante acerca de la necesidad, en su caso, de cooperar con organismos del sector público del Estado miembro en el que esté establecido el titular de datos, con el objetivo de reducir su carga administrativa en relación con el cumplimiento de la solicitud. El organismo del sector público solicitante tendrá en cuenta el asesoramiento de la autoridad competente pertinente.

CAPÍTULO VI

CAMBIO DE PROVEEDOR DE SERVICIOS DE TRATAMIENTO DE DATOS

Artículo 23
Eliminación de los obstáculos a un cambio efectivo de proveedor de servicios de tratamiento de datos

1. Los proveedores de un servicio de tratamiento de datos adoptarán las medidas previstas en los artículos 24, 25 y 26 para garantizar que los clientes de su servicio puedan cambiar a otro servicio de tratamiento de datos que cubra el mismo tipo de servicio, prestado por otro proveedor de servicios. En particular, los proveedores del servicio de tratamiento de datos eliminarán los obstáculos comerciales, técnicos, contractuales y organizativos que impidan a los clientes:

   a) poner término, tras un plazo máximo de preaviso de treinta días naturales, al acuerdo contractual del servicio;

b) celebrar nuevos acuerdos contractuales con otro proveedor de servicios de tratamiento de datos que cubra el mismo tipo de servicio;

c) transferir sus datos, aplicaciones y otros activos digitales a otro proveedor de servicios de tratamiento de datos;

d) mantener la equivalencia funcional de servicio en el entorno informático del otro proveedor o los otros proveedores de servicios de tratamiento de datos que cubran el mismo tipo de servicio, de conformidad con el artículo 26.

2. El apartado 1 solo será aplicable a los obstáculos relacionados con los servicios, los acuerdos contractuales o las prácticas comerciales del proveedor original.

Artículo 24
Cláusulas contractuales relativas al cambio de proveedor de servicios de tratamiento de datos

1. Los derechos del cliente y las obligaciones del proveedor de un servicio de tratamiento de datos en relación con el cambio de proveedor de esos servicios se establecerán con claridad en un contrato escrito. Sin perjuicio de lo dispuesto en la Directiva (UE) 2019/770, ese contrato incluirá al menos los siguientes elementos:

a) cláusulas que permitan al cliente, previa solicitud, cambiar a un servicio de tratamiento de datos ofrecido por otro proveedor de servicios de tratamiento de datos o transferir todos los datos, aplicaciones y activos digitales generados directa o indirectamente por el cliente a un sistema local, concretamente el establecimiento de un período transitorio obligatorio de treinta días naturales como máximo durante el cual el proveedor del servicio de tratamiento de datos:

1) apoyará el proceso de cambio y, cuando sea técnicamente posible, lo completará;

2) velará por la plena continuidad en la prestación de las funciones o servicios respectivos;

b) una especificación exhaustiva de todas las categorías de datos y aplicaciones exportables durante el proceso de cambio, que deberá comprender, como mínimo, todos los datos importados por el cliente al inicio del acuerdo de servicio y todos los datos y metadatos creados por el cliente y por el uso del servicio durante el período en el que se haya prestado el servicio, incluidos, entre otros, los parámetros de configuración, los ajustes de seguridad, los derechos de acceso y los registros de acceso al servicio;

c) un período mínimo para la extracción de datos de al menos treinta días naturales a partir de la expiración del período transitorio acordado entre el cliente y el proveedor del servicio, de conformidad con el apartado 1, letra a), y con el apartado 2.

2. Cuando el período de transición obligatorio definido en el apartado 1, letras a) y c), del presente artículo sea técnicamente inviable, el proveedor de servicios de tratamiento de datos notificará la inviabilidad técnica al cliente dentro de un plazo de siete días hábiles desde que se haya presentado la solicitud de cambio, motivándola debidamente con un informe detallado e indicando un período de transición alternativo, que no podrá exceder de seis meses. De conformidad con el apartado 1 del presente artículo, se garantizará la plena continuidad del servicio durante todo el

período de transición alternativo mediante el pago de la tasa reducida contemplada en el artículo 25, apartado 2.

Artículo 25
Supresión gradual de la tasa por cambio de proveedor

1. A partir del [fecha X + 3 años], los proveedores de servicios de tratamiento de datos no cobrarán al cliente por el proceso de cambio.

2. Desde el [fecha X, fecha de entrada en vigor de la Ley de Datos] hasta el [fecha X + 3 años], los proveedores de servicios de tratamiento de datos podrán cobrar al cliente una tasa reducida por el proceso de cambio.

3. La tasa contemplada en el apartado 2 no excederá de los costes soportados por el proveedor de servicios de tratamiento de datos que tengan una relación directa con el proceso de cambio de que se trate.

4. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, con el fin de completar el presente Reglamento para introducir un mecanismo de seguimiento que permita a la Comisión supervisar la tasa por cambio de proveedor aplicada por los proveedores de servicios de tratamiento de datos en el mercado, con el fin de asegurar su supresión conforme al apartado 1 del presente artículo de acuerdo con el calendario establecido en el mismo apartado.

Artículo 26
Aspectos técnicos del cambio de proveedor

1. Los proveedores de servicios de tratamiento de datos que afectan a recursos informáticos modulables y elásticos limitados a elementos de infraestructura, como los servidores, las redes y los recursos necesarios para explotar la infraestructura, pero que no proporcionan acceso a los servicios operativos, aplicaciones y *software* almacenados, tratados o implantados en esos elementos de infraestructura, garantizarán al cliente, tras cambiar a un servicio ofrecido por otro proveedor de servicios de tratamiento de datos que cubra el mismo tipo de servicio, la equivalencia funcional en el uso del nuevo servicio.

2. En el caso de los servicios de tratamiento de datos distintos de los contemplados en el apartado 1, los proveedores de servicios de tratamiento de datos pondrán las interfaces abiertas a disposición del público de forma gratuita.

3. En el caso de los servicios de tratamiento de datos distintos de los contemplados en el apartado 1, los proveedores de servicios de tratamiento de datos velarán por la compatibilidad con las especificaciones de interoperabilidad abiertas o las normas europeas sobre interoperabilidad definidas de conformidad con el artículo 29, apartado 5, del presente Reglamento.

4. Cuando las especificaciones de interoperabilidad abiertas o las normas europeas a que se refiere el apartado 3 no existan para el tipo de servicio de que se trate, el proveedor de servicios de tratamiento de datos exportará, a petición del cliente, todos los datos generados o cogenerados, incluidos los formatos y estructuras de datos, en un formato estructurado, de uso común y legible por máquina.

CAPÍTULO VII
PROTECCIÓN DE LOS DATOS NO PERSONALES EN CONTEXTOS INTERNACIONALES

Artículo 27
Acceso y transferencia internacionales

1. Los proveedores de servicios de tratamiento de datos personales adoptarán todas las medidas técnicas, jurídicas y organizativas razonables, lo que incluye la celebración de acuerdos contractuales, para impedir la transferencia internacional de datos no personales conservados en la Unión, o el acceso de gobiernos de terceros países a tales datos, cuando la transferencia o el acceso entren en conflicto con el Derecho de la Unión o con el Derecho nacional del Estado miembro de que se trate, sin perjuicio de lo dispuesto en los apartados 2 o 3.

2. Las resoluciones o sentencias de los órganos jurisdiccionales y resoluciones de las autoridades administrativas de terceros países por las que se exija a un proveedor de servicios de tratamiento de datos transferir datos no personales sujetos al presente Reglamento conservados en la Unión, o dar acceso a tales datos, solo podrán reconocerse o ejecutarse de cualquier forma si se basan en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el tercer país solicitante y la Unión o entre el tercer país solicitante y un Estado miembro.

3. En ausencia de tal acuerdo internacional, cuando un proveedor de servicios de tratamiento de datos sea el destinatario de una resolución de un órgano jurisdiccional o de una autoridad administrativa de un tercer país por la que se exija transferir datos no personales sujetos al presente Reglamento conservados en la Unión, o dar acceso a tales datos, y el cumplimiento de dicha resolución pueda poner al destinatario en una situación de conflicto con el Derecho de la Unión o con el Derecho nacional del Estado miembro pertinente, la transferencia de tales datos a esa autoridad del tercer país, o el acceso a los mismos por su parte, únicamente tendrán lugar si:

   a) el sistema del tercer país exige que se expongan los motivos y la proporcionalidad de la resolución o sentencia y que la resolución o sentencia, según el caso, sea de carácter específico, por ejemplo, al establecer un vínculo suficiente con determinadas personas sospechosas o infracciones;

   b) la objeción motivada del destinatario está sujeta a revisión por un órgano jurisdiccional competente del tercer país; y

   c) el Derecho del tercer país faculta al órgano jurisdiccional competente que dicta la resolución o sentencia o revisa la resolución de una autoridad administrativa para tener debidamente en cuenta los intereses jurídicos pertinentes del proveedor de los datos protegidos por el Derecho de la Unión o por el Derecho nacional del Estado miembro pertinente.

El destinatario de la resolución podrá solicitar el dictamen de los organismos o autoridades competentes pertinentes, con arreglo al presente Reglamento, para determinar si se cumplen las condiciones expuestas, especialmente cuando considere que la resolución puede referirse a datos comercialmente sensibles o puede colisionar con los intereses de seguridad nacional o de defensa de la Unión o sus Estados miembros.

El Comité Europeo de Innovación en materia de Datos establecido por el Reglamento [xxx - DGA] asesorará y asistirá a la Comisión en la elaboración de directrices para la evaluación del cumplimiento de esas condiciones.

4. Si se cumplen las condiciones de los apartados 2 o 3, el proveedor de servicios de tratamiento de datos facilitará la cantidad mínima de datos permitida en respuesta a una solicitud, sobre la base de una interpretación razonable de la solicitud.

5. Antes de dar cumplimiento a la solicitud, el proveedor de servicios de tratamiento de datos informará al titular de datos de que una autoridad administrativa de un tercer país ha presentado una solicitud de acceso a sus datos, excepto en los casos en que la solicitud sirva a fines de aplicación de la ley y mientras sea necesario para preservar la eficacia de las actividades correspondientes de aplicación de la ley.

CAPÍTULO VIII
INTEROPERABILIDAD

Artículo 28
Requisitos esenciales en materia de interoperabilidad

1. Los operadores de espacios de datos cumplirán los siguientes requisitos esenciales para facilitar la interoperabilidad de los datos y de los mecanismos y servicios de intercambio de datos:

   a) el contenido del conjunto de datos, las restricciones de uso, las licencias, la metodología de recopilación de datos y la calidad e incertidumbre de los datos se describirán en una medida suficiente para que el destinatario pueda encontrar los datos, acceder a ellos y utilizarlos;

   b) las estructuras de datos, los formatos de datos, los vocabularios, los sistemas de clasificación, las taxonomías y las listas de códigos se describirán de manera que sean de acceso público y coherentes;

   c) los medios técnicos para acceder a los datos, tales como las interfaces de programación de aplicaciones, así como sus condiciones de uso y su calidad de servicio, se describirán en una medida suficiente para permitir el acceso automático a los datos y su transmisión automática entre las partes, de forma continua o en tiempo real, en un formato legible por máquina;

   d) se proporcionarán los medios que permitan la interoperabilidad de los contratos inteligentes en el marco de sus servicios y actividades.

Estos requisitos pueden ser de carácter genérico o referirse a sectores específicos, si bien han de tomar plenamente en consideración la interrelación con requisitos derivados de otras legislaciones sectoriales nacionales o de la Unión.

2. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, con el fin de completar el presente Reglamento precisando en mayor medida los requisitos esenciales contemplados en el apartado 1.

3. Se presumirá que los operadores de espacios de datos que sean conformes con normas armonizadas, o partes de estas normas, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea* son conformes con los requisitos esenciales a que se refiere el apartado 1 del presente artículo, en la medida en que dichas normas contemplen esos requisitos.

4. De conformidad con el artículo 10 del Reglamento (UE) n.º 1025/2012, la Comisión podrá pedir a una o varias organizaciones europeas de normalización que elaboren normas armonizadas que satisfagan los requisitos esenciales contemplados en el apartado 1 del presente artículo.

5. La Comisión, mediante actos de ejecución, adoptará especificaciones comunes en caso de que las normas armonizadas a que se refiere el apartado 4 no existan o cuando considere que las normas armonizadas pertinentes son insuficientes para garantizar la conformidad con los requisitos esenciales del apartado 1 del presente artículo, en su caso, respecto a cualquiera de los requisitos establecidos en el apartado 1 del presente artículo o respecto a todos ellos. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 39, apartado 2.

6. La Comisión podrá adoptar directrices que establezcan especificaciones de interoperabilidad para el funcionamiento de los espacios comunes europeos de datos, tales como disposiciones de aplicación y acuerdos entre las partes para los modelos arquitectónicos y las normas técnicas que fomenten el intercambio de datos, por ejemplo, en lo que respecta a los derechos de acceso y a la traducción técnica del consentimiento o permiso.

Artículo 29
Interoperabilidad de los servicios de tratamiento de datos

1. Las especificaciones de interoperabilidad abiertas y las normas europeas para la interoperabilidad de los servicios de tratamiento de datos deberán:

   a) orientarse, en función de los resultados, hacia la consecución de la interoperabilidad entre distintos servicios de tratamiento de datos que cubran el mismo tipo de servicio;

   b) mejorar la portabilidad de los activos digitales entre distintos servicios de tratamiento de datos que cubran el mismo tipo de servicio;

   c) garantizar, cuando sea técnicamente viable, la equivalencia funcional entre distintos servicios de tratamiento de datos que cubran el mismo tipo de servicio.

2. Las especificaciones de interoperabilidad abiertas y las normas europeas para la interoperabilidad de los servicios de tratamiento de datos abordarán:

   a) los aspectos de la interoperabilidad de la nube en lo que respecta a la interoperabilidad del transporte, la interoperabilidad sintáctica, la interoperabilidad semántica de los datos, la interoperabilidad conductual y la interoperabilidad de los marcos normativos;

   b) los aspectos de la portabilidad de los datos en la nube en lo que respecta a la portabilidad sintáctica de los datos, la portabilidad semántica de los datos y la portabilidad de los marcos normativos relativos a los datos;

   c) los aspectos de las aplicaciones en la nube en lo que respecta a la portabilidad sintáctica de las aplicaciones, la portabilidad de las instrucciones de las aplicaciones, la portabilidad de los metadatos de las aplicaciones, la portabilidad conductual de las aplicaciones y la portabilidad de los marcos normativos de las aplicaciones.

3. Las especificaciones de interoperabilidad abiertas cumplirán lo dispuesto en el anexo II, puntos 3 y 4, del Reglamento (UE) n.º 1025/2012.

4. De conformidad con el artículo 10 del Reglamento (UE) n.º 1025/2012, la Comisión podrá pedir a una o varias organizaciones europeas de normalización que elaboren normas europeas aplicables a tipos específicos de servicios de tratamiento de datos.

5. A los efectos del artículo 26, apartado 3, del presente Reglamento, la Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, con el fin de publicar la referencia de especificaciones de interoperabilidad abiertas y normas europeas para la interoperabilidad de los servicios de tratamiento de datos en el repositorio central de normas de la Unión para la interoperabilidad de los servicios de tratamiento de datos, siempre y cuando esas especificaciones y normas cumplan los criterios establecidos en los apartados 1 y 2 del presente artículo.

Artículo 30

Requisitos esenciales de los contratos inteligentes para el intercambio de datos

1. El proveedor de una aplicación que utilice contratos inteligentes o, en su defecto, la persona cuya actividad comercial, empresarial o profesional implique la utilización de contratos inteligentes para terceros en el contexto de un acuerdo de puesta a disposición de datos cumplirá los siguientes requisitos esenciales:

   a) solidez: velará por que el contrato inteligente se haya diseñado de manera que ofrezca un grado de solidez muy elevado con el fin de evitar errores funcionales y contrarrestar los intentos de manipulación por terceros;

   b) resolución y suspensión seguras: velará por que exista un mecanismo que permita poner fin a la ejecución de transacciones; el contrato inteligente incluirá funciones internas que permitan reinicializar el contrato o darle instrucciones para poner fin a la operación o suspenderla con objeto de evitar futuras ejecuciones (accidentales);

   c) archivo y continuidad de los datos: en caso de que el contrato inteligente deba resolverse o desactivarse, preverá la posibilidad de archivar los datos de las transacciones, así como la lógica y el código del contrato inteligente, con el fin de llevar un registro de las operaciones con datos efectuadas previamente (auditabilidad); y

   d) control de acceso: el contrato inteligente estará protegido mediante rigurosos mecanismos de control de acceso en el nivel de la gobernanza y en el del contrato inteligente.

2. El proveedor del contrato inteligente o, en su defecto, la persona cuya actividad comercial, empresarial o profesional implique la utilización de contratos inteligentes para terceros en el contexto de un acuerdo de puesta a disposición de datos realizará una evaluación de conformidad a efectos del cumplimiento de los requisitos esenciales contemplados en el apartado 1 y expedirá una declaración UE de conformidad respecto a dicho cumplimiento.

3. Al expedir la declaración UE de conformidad, el proveedor de una aplicación que utilice contratos inteligentes o, en su defecto, la persona cuya actividad comercial, empresarial o profesional implique la utilización de contratos inteligentes para terceros en el contexto de un acuerdo de puesta a disposición de datos será

responsable del cumplimiento de los requisitos esenciales contemplados en el apartado 1.

4. Se presumirá que un contrato inteligente que se atenga a las normas armonizadas, o las partes pertinentes de estas normas, elaboradas y publicadas en el *Diario Oficial de la Unión Europea* es conforme con los requisitos esenciales a que se refiere el apartado 1 del presente artículo, en la medida en que dichas normas contemplen esos requisitos.

5. De conformidad con el artículo 10 del Reglamento (UE) n.º 1025/2012, la Comisión podrá pedir a una o varias organizaciones europeas de normalización que elaboren normas armonizadas que satisfagan los requisitos esenciales contemplados en el apartado 1 del presente artículo.

6. En caso de que las normas armonizadas a que se refiere el apartado 4 no existan, o cuando la Comisión considere que las normas armonizadas pertinentes son insuficientes para garantizar la conformidad con los requisitos esenciales del apartado 1 del presente artículo en un contexto transfronterizo, la Comisión, mediante actos de ejecución, podrá adoptar especificaciones comunes respecto a los requisitos esenciales establecidos en el apartado 1 del presente artículo. Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 39, apartado 2.

CAPÍTULO IX
APLICACIÓN Y EJECUCIÓN

Artículo 31
Autoridades competentes

1. Cada Estado miembro designará una o varias autoridades nacionales competentes con el fin de garantizar la aplicación y ejecución del presente Reglamento. Los Estados miembros podrán establecer una o varias autoridades nuevas o recurrir a las autoridades existentes.

2. Sin perjuicio de lo dispuesto en el apartado 1 del presente artículo:

   a) las autoridades de control independientes responsables de supervisar la aplicación del Reglamento (UE) 2016/679 tendrán la responsabilidad de supervisar la aplicación del presente Reglamento en lo que respecta a la protección de los datos personales. Se aplicarán *mutatis mutandis* los capítulos VI y VII del Reglamento (UE) 2016/679; las funciones y competencias de las autoridades de control se ejercerán respecto al tratamiento de datos personales;

   b) para cuestiones específicas del intercambio de datos sectoriales relacionadas con la aplicación del presente Reglamento, se respetará la competencia de las autoridades sectoriales;

   c) la autoridad nacional competente responsable de la aplicación y ejecución del capítulo VI del presente Reglamento tendrá experiencia en el ámbito de los servicios de comunicaciones de datos y electrónicas.

3. Los Estados miembros velarán por que las funciones y competencias de las autoridades competentes designadas con arreglo al apartado 1 del presente artículo estén claramente definidas e incluyan:

a) fomentar la sensibilización entre los usuarios y las entidades que entren en el ámbito de aplicación del presente Reglamento acerca de los derechos y obligaciones previstos en el presente Reglamento;

b) tramitar las denuncias derivadas de supuestas infracciones del presente Reglamento, investigar el objeto de la denuncia en la medida adecuada e informar al denunciante sobre el curso y el resultado de la investigación en un plazo razonable, en particular cuando resulte necesario proseguir la investigación o coordinar actuaciones con otra autoridad competente;

c) llevar a cabo investigaciones sobre asuntos que afecten a la aplicación del presente Reglamento, también sobre la base de información recibida de otra autoridad competente o autoridad pública;

d) imponer, a través de procedimientos administrativos, sanciones económicas disuasorias, que pueden incluir multas coercitivas y multas con efectos retroactivos, o iniciar procedimientos judiciales para la imposición de multas;

e) hacer un seguimiento de los avances tecnológicos pertinentes para la puesta a disposición y utilización de datos;

f) cooperar con las autoridades competentes de otros Estados miembros para garantizar la aplicación coherente del presente Reglamento, lo que incluye el intercambio de toda la información pertinente por medios electrónicos, sin demora indebida;

g) asegurar la disponibilidad pública en línea de las solicitudes de acceso a datos presentadas por organismos del sector público en caso de emergencia pública con arreglo al capítulo V;

h) cooperar con todas las autoridades competentes pertinentes para garantizar que las obligaciones del capítulo VI se cumplan de manera coherente con otra legislación de la Unión y medidas de autorregulación aplicables a los proveedores de servicios de tratamiento de datos;

i) velar por la supresión de la tasa por cambio de proveedor de servicios de tratamiento de datos de conformidad con el artículo 25.

4. Cuando un Estado miembro designe más de una autoridad competente, las autoridades competentes, en el ejercicio de las funciones y competencias que les hayan sido asignadas con arreglo al apartado 3 del presente artículo, cooperarán mutuamente y, cuando proceda, con la autoridad de control responsable del seguimiento de la aplicación del Reglamento (UE) 2016/679, para garantizar la aplicación coherente del presente Reglamento. En esos casos, los Estados miembros en cuestión designarán una autoridad competente coordinadora.

5. Los Estados miembros comunicarán a la Comisión el nombre de las autoridades competentes designadas y sus respectivas funciones y competencias, así como, cuando proceda, el nombre de la autoridad competente coordinadora. La Comisión mantendrá un registro público de dichas autoridades.

6. En el ejercicio de sus funciones y competencias de conformidad con el presente Reglamento, las autoridades competentes no estarán sometidas a ninguna influencia externa, ya sea directa o indirecta, y no solicitarán ni aceptarán instrucciones de ninguna otra autoridad pública o entidad privada.

7. Los Estados miembros velarán por dotar a las autoridades competentes designadas de los recursos necesarios para el ejercicio adecuado de sus funciones de conformidad con el presente Reglamento.

Artículo 32
Derecho a presentar una reclamación ante la autoridad competente

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, toda persona física y jurídica tendrá derecho a presentar una reclamación individual o, cuando proceda, colectiva ante la autoridad competente pertinente del Estado miembro en el que tenga su residencia habitual, su lugar de trabajo o su lugar de establecimiento cuando considere que los derechos que le confiere el presente Reglamento han sido vulnerados.

2. La autoridad competente ante la que se haya presentado la reclamación informará al reclamante sobre el curso del procedimiento y la decisión tomada.

3. Las autoridades competentes cooperarán para tramitar y resolver las reclamaciones, lo que incluirá el intercambio de toda información pertinente por medios electrónicos, sin demora indebida. Dicha cooperación no afectará al mecanismo específico de cooperación previsto en los capítulos VI y VII del Reglamento (UE) 2016/679.

Artículo 33
Sanciones

1. Los Estados miembros adoptarán las normas sobre las sanciones aplicables a las infracciones del presente Reglamento y todas las medidas necesarias para garantizar su aplicación. Esas sanciones serán efectivas, proporcionadas y disuasorias.

2. A más tardar el [fecha de aplicación del Reglamento], los Estados miembros notificarán a la Comisión esas normas y medidas y toda modificación posterior que las afecte.

3. En caso de infracción de las obligaciones establecidas en los capítulos II, III y V del presente Reglamento, las autoridades de control a que se refiere el artículo 51 del Reglamento (UE) 2016/679 podrán, dentro de su ámbito de competencia, imponer multas administrativas acordes con el artículo 83 del Reglamento (UE) 2016/679 y hasta el importe mencionado en el artículo 83, apartado 5, de dicho Reglamento.

4. En caso de infracción de las obligaciones establecidas en el capítulo V del presente Reglamento, la autoridad de control a que se refiere el artículo 52 del Reglamento (UE) 2018/1725 podrá, dentro de su ámbito de competencia, imponer multas administrativas acordes con el artículo 66 del Reglamento (UE) 2018/1725 y hasta el importe mencionado en el artículo 66, apartado 3, de dicho Reglamento.

Artículo 34
Cláusulas contractuales tipo

La Comisión elaborará y recomendará cláusulas contractuales tipo no vinculantes sobre el acceso a los datos y su utilización para ayudar a las partes en la elaboración y negociación de contratos con derechos y obligaciones contractuales equilibrados.

CAPÍTULO X
DERECHO *SUI GENERIS* CON ARREGLO A LA DIRECTIVA 96/9/CE

Artículo 35
Bases de datos que contienen ciertos datos

Con objeto de no obstaculizar el ejercicio, por parte de los usuarios, del derecho de acceder a los datos y utilizarlos de conformidad con el artículo 4 del presente Reglamento, ni del derecho a compartir esos datos con terceros de conformidad con el artículo 5 del presente Reglamento, el derecho *sui generis* establecido en el artículo 7 de la Directiva 96/9/CE no se aplicará a las bases de datos que contengan datos obtenidos o generados por el uso de un producto o un servicio relacionado.

CAPÍTULO XI
DISPOSICIONES FINALES

Artículo 36
Modificación del Reglamento (UE) 2017/2394

En el anexo del Reglamento (UE) 2017/2394, se añade el punto siguiente:

«29. [Reglamento (UE) XXX del Parlamento Europeo y del Consejo (Ley de Datos)].».

Artículo 37
Modificación de la Directiva (UE) 2020/1828

En el anexo de la Directiva (UE) 2020/1828, se añade el punto siguiente:

«67. [Reglamento (UE) XXX del Parlamento Europeo y del Consejo (Ley de Datos)].».

Artículo 38
Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.
2. Los poderes para adoptar actos delegados mencionados en el artículo 25, apartado 4, en el artículo 28, apartado 2, y en el artículo 29, apartado 5, se otorgan a la Comisión por un período de tiempo indefinido a partir del […].
3. La delegación de poderes mencionada en el artículo 25, apartado 4, en el artículo 28, apartado 2, y en el artículo 29, apartado 5, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en ella. No afectará a la validez de los actos delegados que ya estén en vigor.
4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos

en el Acuerdo interinstitucional sobre la mejora de la legislación de 13 de abril de 2016.

5. Tan pronto como la Comisión adopte un acto delegado, lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 25, apartado 4, del artículo 28, apartado 2, y del artículo 29, apartado 5, entrarán en vigor únicamente si, en un plazo de tres meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 39
Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

Artículo 40
Otros actos jurídicos de la Unión que regulan los derechos y obligaciones en materia de acceso a los datos y su utilización

1. No se verán afectadas las obligaciones específicas para la puesta a disposición de datos entre empresas, entre empresas y consumidores y, con carácter excepcional, entre empresas y organismos del sector público establecidas en actos jurídicos de la Unión que hayan entrado en vigor el [xx XXX xxx] o antes de esa fecha, así como en los actos delegados o actos de ejecución basados en dichas normas.

2. El presente Reglamento se entiende sin perjuicio de la legislación de la Unión que, a la luz de las necesidades de un sector, de un espacio común europeo de datos o de un área de interés público, establezca requisitos adicionales, en particular relativos a:

   a) aspectos técnicos del acceso a los datos;

   b) límites a los derechos de los titulares de datos de acceder a determinados datos facilitados por usuarios o de utilizarlos;

   c) aspectos que vayan más allá del acceso a los datos y su utilización.

Artículo 41
Evaluación y revisión

A más tardar el [*dos años desde la fecha de aplicación del presente Reglamento*], la Comisión llevará a cabo una evaluación del presente Reglamento y presentará un informe sobre sus principales conclusiones al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo. En la evaluación se analizarán, en particular:

a) el acceso a otras categorías o tipos de datos;

b) la exclusión de determinadas categorías de empresas como beneficiarias al amparo del artículo 5;

c) otras situaciones que hayan de considerarse necesidades excepcionales a efectos del artículo 15;

d) los cambios en las prácticas contractuales de los proveedores de servicios de tratamiento de datos y si esos cambios se traducen en un cumplimiento suficiente del artículo 24;

e) la reducción de la tasa aplicada por los proveedores de servicios de tratamiento de datos por el proceso de cambio de proveedor, en consonancia con la supresión gradual de esa tasa de conformidad con el artículo 25.

Artículo 42
Entrada en vigor y aplicación

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Será aplicable a partir del [doce meses desde la fecha de entrada en vigor del presente Reglamento].

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
La Presidenta	*El Presidente*