2023/2854

22.12.2023

REGLAMENTO (UE) 2023/2854 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 13 de diciembre de 2023

sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento 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 Banco Central Europeo ([1]),

Visto el dictamen del Comité Económico y Social Europeo ([2]),

Visto el dictamen del Comité de las Regiones ([3]),

De conformidad con el procedimiento legislativo ordinario ([4]),

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 internet 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. Los mismos datos pueden 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. Esos 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, pequeñas empresas y medianas empresas tal como se definen en el artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión ([5]) (pymes), a menudo escasean las capacidades y competencias digitales necesarias para recopilar, analizar y utilizar datos, y el acceso a estos queda limitado con frecuencia 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 tiene derecho a utilizar los datos del producto o los datos del servicio relacionado, en qué condiciones y sobre qué base. Por

([1]) DO C 402 de 19.10.2022, p. 5.
([2]) DO C 365 de 23.9.2022, p. 18.
([3]) DO C 375 de 30.9.2022, p. 112.
([4]) Posición del Parlamento Europeo de 9 de noviembre de 2023 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 27 de noviembre de 2023.
([5]) Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

consiguiente, los Estados miembros no deben adoptar ni mantener requisitos nacionales adicionales relativos a las cuestiones que entran en el ámbito de aplicación del presente Reglamento, salvo que así se disponga expresamente en él, ya que ello afectaría a la aplicación directa y uniforme de este. Además, toda medida a nivel de la Unión debe entenderse sin perjuicio de las obligaciones y los compromisos establecidos en los acuerdos comerciales internacionales celebrados por la Unión.

(5) El presente Reglamento garantiza que los usuarios de un producto conectado o servicio relacionado en la Unión puedan acceder oportunamente a los datos generados por el uso de dicho producto conectado o servicio relacionado y que puedan utilizarlos, entre otros, compartiéndolos con terceros de su elección. El presente Reglamento impone a los titulares de datos la obligación de poner los datos a disposición de los usuarios y de terceros elegidos por el usuario 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 un acceso a los datos y una utilización de estos que sean equitativos. El presente Reglamento también garantiza que, cuando exista una necesidad excepcional, los titulares de datos pongan a disposición de los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión los datos necesarios para el desempeño de alguna tarea específica realizada 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 concesión de un nuevo derecho a los titulares de datos a utilizar los datos generados por el uso de un producto conectado o servicio relacionado.

(6) La generación de datos es el resultado de las acciones de al menos dos agentes, en particular, el diseñador o fabricante de un producto conectado —que en muchos casos podría ser también proveedor de servicios relacionados— y el usuario del producto conectado o servicio relacionado. La generación de datos plantea cuestiones de equidad en la economía digital, ya que los datos registrados por el producto conectado o servicio relacionado 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, también mediante el intercambio de datos sobre la base de acuerdos voluntarios y el desarrollo por las empresas de la Unión de la creación de valor impulsado por los datos, es preferible adoptar un enfoque general para asignar derechos en materia de acceso y utilización de datos frente a la concesión de derechos exclusivos de acceso y utilización. El presente Reglamento establece normas horizontales que podrían ir seguidas de disposiciones de Derecho de la Unión o nacional que regulen la situación específica de los sectores correspondientes.

(7) El derecho fundamental a la protección de los datos personales está salvaguardado, en particular, por los Reglamentos (UE) 2016/679 ([6]) y (UE) 2018/1725 ([7]) del Parlamento Europeo y del Consejo. Además, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([8]) protege la vida privada y la confidencialidad de las comunicaciones, incluso mediante condiciones para el almacenamiento de datos personales y no personales en los equipos terminales, y el acceso desde estos. Dichos actos legislativos de la Unión constituyen la base para un tratamiento de datos sostenible y responsable, incluso cuando los conjuntos de datos contengan una combinación de datos personales y no personales. El presente Reglamento complementa el Derecho de la Unión y se entiende sin perjuicio del Derecho de la Unión en materia de protección de datos personales y de la intimidad (o privacidad), en particular, en lo que se refiere a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 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 privacidad y la confidencialidad de las comunicaciones. Todo tratamiento de datos personales en virtud del presente Reglamento debe cumplir el Derecho

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

([7]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

([8]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

de la Unión en materia de protección de datos, incluido el requisito de una base jurídica válida para el tratamiento con arreglo al artículo 6 del Reglamento (UE) 2016/679 y, cuando proceda, las condiciones del artículo 9 de dicho Reglamento y del artículo 5, apartado 3, de la Directiva 2002/58/CE. El presente Reglamento no constituye una base jurídica para la recogida o generación de datos personales por parte del titular de datos. El presente Reglamento impone a los titulares de datos la obligación de poner los datos personales a disposición de los usuarios o de los terceros elegidos por el usuario, previa petición de dicho usuario. Debe proporcionarse dicho acceso a los datos personales que el titular de datos trate basándose en cualquiera de las bases jurídicas mencionadas en el artículo 6 del Reglamento (UE) 2016/679. Cuando el usuario no sea el interesado, el presente Reglamento no contiene ninguna base jurídica para que se proporcione acceso a los datos personales o estos se pongan a disposición de un tercero, y no debe entenderse que concede ningún nuevo derecho al titular de datos a utilizar los datos personales generados por el uso de un producto conectado o de un servicio relacionado. En esos casos, podría redundar en interés del usuario facilitar el cumplimiento de los requisitos establecidos en el artículo 6 del Reglamento (UE) 2016/679. Dado que el presente Reglamento no debe afectar negativamente a los derechos de protección de datos de los interesados, el titular de datos puede atender las solicitudes en esos casos, entre otros modos, anonimizando los datos personales o, en el caso de que los datos fácilmente disponibles contengan datos personales de varios interesados, transmitiendo únicamente datos personales relativos al usuario.

(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 el intercambio de datos comprendido dentro del ámbito de aplicación del presente Reglamento, deben aplicar medidas técnicas y organizativas para proteger esos derechos. Dichas medidas incluyen no solo la seudonimización y el cifrado, sino también el uso de una tecnología cada vez más disponible que permita llevar los algoritmos a 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) Salvo que se disponga otra cosa en el presente Reglamento, este no afecta a las normas nacionales de Derecho contractual, incluidas las relativas a la celebración, la validez o los efectos de los contratos, ni a las consecuencias de la resolución unilateral de los contratos. El presente Reglamento complementa el Derecho de la Unión —y se entiende sin perjuicio del Derecho de la Unión 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 93/13/CEE del Consejo ([9]) y las Directivas 2005/29/CE ([10]) y 2011/83/UE ([11]) del Parlamento Europeo y del Consejo.

(10) El presente Reglamento se entiende sin perjuicio de los actos jurídicos de la Unión y nacionales que dispongan el intercambio de datos, el acceso a los datos 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 del Tratado de Funcionamiento de la Unión Europea (TFUE) en virtud de la cual se hayan adoptado tales actos jurídicos de la Unión, y sin perjuicio de la cooperación internacional en el ámbito mencionado, en particular, sobre la base del Convenio del Consejo de Europa sobre la Ciberdelincuencia (STE n.º 185), hecho en Budapest el 23 de noviembre de 2001. Dichos actos incluyen los Reglamentos (UE) 2021/784 ([12]) (UE) 2022/2065 ([13]) y (UE) 2023/1543 ([14]) del Parlamento Europeo y del Consejo, y la Directiva

([9]) Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95 de 21.4.1993, p. 29).

([10]) 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).

([11]) 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 (DO L 304 de 22.11.2011, p. 64).

([12]) 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).

([13]) Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (DO L 277 de 27.10.2022, p. 1).

([14]) Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales (DO L 191 de 28.7.2023, p. 118).

(UE) 2023/1544 del Parlamento Europeo y del Consejo ([15]). El presente Reglamento no se aplica a la recopilación, intercambio, acceso o utilización de datos en virtud del Reglamento (UE) 2015/847 del Parlamento Europeo y del Consejo ([16]) y la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo ([17]). El presente Reglamento no se aplica a las actividades que quedan fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, no afecta a las competencias de los Estados miembros en materia de seguridad pública, defensa o seguridad nacional, aduanas y administración fiscal o salud y seguridad ciudadanas, con independencia del tipo de entidad a la que los Estados miembros hayan confiado el desempeño de tareas en relación con dichas competencias.

(11) El presente Reglamento no debe afectar al Derecho 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, salvo que así se disponga expresamente en él.

(12) El presente Reglamento complementa y se entiende sin perjuicio del Derecho de la Unión que establece requisitos de accesibilidad para determinados productos y servicios, en particular, la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo ([18]).

(13) El presente Reglamento se entiende sin perjuicio de los actos jurídicos de la Unión y nacionales de protección de los derechos de propiedad intelectual (que incluye, asimismo, la propiedad industrial), incluidas las Directivas 2001/29/CE ([19]), 2004/48/CE ([20]) y (UE) 2019/790 ([21]) del Parlamento Europeo y del Consejo.

(14) Los productos conectados que, a través de sus componentes o sistemas operativos, obtengan, generen o recopilen datos relativos a su rendimiento, uso o entorno y que puedan comunicar dichos datos mediante un servicio de comunicaciones electrónicas, una conexión física o un acceso en el dispositivo, a menudo denominado «internet de las cosas», deben incluirse en el ámbito de aplicación del presente Reglamento, a excepción de los prototipos. Algunos ejemplos de estos servicios de comunicaciones electrónicas son, en particular, las redes telefónicas terrestres, las redes de televisión por cable, las redes basadas en satélites y las redes de comunicación de campo cercano. Los productos conectados se encuentran en todos los aspectos de la economía y la sociedad, también en infraestructuras privadas, civiles o comerciales, vehículos, equipos sanitarios y de estilo de vida, buques, aeronaves, equipos domésticos y bienes de consumo, productos médicos y sanitarios o maquinaria agrícola e industrial. Las opciones de diseño de los fabricantes y, en su caso, el Derecho de la Unión o nacional que regule las necesidades y los objetivos específicos del sector o las decisiones pertinentes de las autoridades competentes, deben determinar qué datos puede poner a disposición un producto conectado.

(15) Los datos representan la digitalización de las acciones del usuario o de eventos y, en consecuencia, deben ser accesibles para el usuario. Las normas que rigen el acceso a los datos de los productos conectados y los servicios relacionados y su utilización en virtud del presente Reglamento abordan los datos tanto de los productos como de los servicios relacionados. El término «datos del producto» se refiere a los datos generados por el uso de un producto conectado que el fabricante ha diseñado para que sean extraíbles del producto conectado por un usuario, titular de datos o tercero, incluido, cuando proceda, el fabricante. El término «datos del servicio relacionado» se refiere a los datos que representan también la digitalización de las acciones del usuario o de eventos relativos al

([15]) Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales (DO L 191 de 28.7.2023, p. 181).

([16]) Reglamento (UE) 2015/847 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativo a la información que acompaña a las transferencias de fondos y por el que se deroga el Reglamento (CE) n.º 1781/2006 (DO L 141 de 5.6.2015, p. 1).

([17]) Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión (DO L 141 de 5.6.2015, p. 73).

([18]) 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, p. 70).

([19]) Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información (DO L 167 de 22.6.2001, p. 10).

([20]) Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual (DO L 157 de 30.4.2004, p. 45).

([21]) Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE (DO L 130 de 17.5.2019, p. 92).

producto conectado, generados durante la prestación de un servicio relacionado por parte del proveedor. Debe entenderse que los datos generados por el uso de un producto conectado o servicio relacionado abarcan los datos registrados de manera intencionada o los datos resultantes indirectamente de la intervención del usuario, como los datos relativos al entorno o las interacciones del producto conectado. Ello debe incluir los datos relativos a la utilización de un producto conectado generados por una interfaz de usuario o a través de un servicio relacionado, y no debe limitarse a la información de que dicha utilización se ha producido, sino que debe incluir todos los datos generados por el producto conectado como resultado de dicha utilización, tales como los datos generados automáticamente por sensores y los datos registrados por aplicaciones integradas, incluidas las aplicaciones que indican el estado del *hardware* y los fallos de funcionamiento. Ello debe incluir también los datos generados por el producto conectado o servicio relacionado durante los períodos en los que el usuario no interviene, como cuando este decide no utilizar un producto conectado durante un período de tiempo determinado y, en su lugar, mantenerlo en modo de espera o, incluso, apagarlo, dado que el estado de un producto conectado o de sus componentes, por ejemplo, sus pilas o baterías, puede variar cuando el producto conectado se encuentra en modo de espera o apagado. El ámbito de aplicación del presente Reglamento incluye los datos que no se modifican sustancialmente, es decir, los datos brutos, también conocidos como datos fuente o datos primarios, que se refieren a puntos de datos que se generan automáticamente sin ninguna forma de tratamiento posterior, así como los datos que, previamente a su tratamiento y análisis, han sido objeto de un tratamiento destinado a hacerlos comprensibles y que puedan ser utilizados. Tales datos incluyen los datos recogidos a partir de un único sensor o de un grupo conectado de sensores con el fin de hacer comprensibles los datos recogidos para casos de uso más amplios, determinando una cantidad o una calidad física o la modificación de una cantidad física, como la temperatura, la presión, el caudal, el audio, el valor del pH, el nivel líquido, la posición, la aceleración o la velocidad. El término «datos pretratados» no debe interpretarse en el sentido de imponer al titular de datos una obligación de realizar inversiones sustanciales en el limpiado y la transformación de los datos. Los datos que se han de poner a disposición deben incluir los metadatos pertinentes, incluido su contexto básico y su sello de tiempo, necesarios para poder utilizar los datos, combinados con otros datos (por ejemplo, ordenados y clasificados con otros puntos de datos relacionados con ellos) o reformateados en un formato de utilización habitual. Estos datos pueden ser valiosos para el usuario y apoyan la innovación y el desarrollo de servicios digitales y de otro tipo para proteger el medio ambiente, la salud y la economía circular, entre otros, porque facilitan el mantenimiento y la reparación de los productos conectados en cuestión. En cambio, la información que se infiere o se deriva de tales datos, que es el resultado de inversiones adicionales en la asignación de valores o conocimientos que aportan los datos, en particular, mediante algoritmos complejos de propiedad exclusiva, incluidos los que forman parte de programas informáticos de propiedad exclusiva, no debe considerarse incluida en el ámbito de aplicación del presente Reglamento y, por consiguiente, no debe estar sujeta a la obligación del titular de datos de ponerla a disposición de un usuario o un destinatario de datos, a menos que se acuerde otra cosa entre el usuario y el titular de datos. Estos datos podrían incluir, en particular, información derivada de la fusión de sensores, la inferencia o la derivación de datos desde múltiples sensores, recogidos en el producto conectado, utilizando algoritmos complejos de propiedad exclusiva y que podrían estar protegidos por derechos de propiedad intelectual.

(16) El presente Reglamento permite a los usuarios de productos conectados beneficiarse de servicios posventa, servicios auxiliares y otros servicios basados en datos recogidos por sensores integrados en dichos productos, ya que la recopilación de esos datos puede tener un valor para mejorar el rendimiento de los productos conectados. Es importante distinguir, por una parte, entre los mercados de suministro de tales productos conectados dotados de sensores y servicios relacionados y, por otra parte, los mercados de programas informáticos y contenidos no relacionados, como los contenidos textuales, audiovisuales o de audio, a menudo protegidos por derechos de propiedad intelectual. En consecuencia, no debe aplicarse el presente Reglamento a los datos generados por dichos productos conectados dotados de sensores cuando el usuario graba, transmite, muestra o reproduce contenidos, así como los propios contenidos, que a menudo están protegidos por derechos de propiedad intelectual (por ejemplo, para su utilización por un servicio en línea). Tampoco debe aplicarse el presente Reglamento a los datos obtenidos, generados o a los que se haya accedido desde el producto conectado, o que hayan sido transmitidos al producto conectado, con fines de almacenamiento o alguna otra operación de tratamiento en nombre de terceros que no sean el usurario, como pueda ser el caso respecto de los servidores o la infraestructura en la nube que gestionen sus titulares íntegramente en nombre de terceros, entre otros fines, por ejemplo, para su utilización por un servicio en línea.

(17) Es necesario establecer normas relativas a los productos que estén conectados a un servicio relacionado en el momento de la compraventa, alquiler o arrendamiento de tal manera que su ausencia impediría que el producto conectado desempeñe una o varias de sus funciones, o que el fabricante o un tercero conecte posteriormente al producto a fin de aumentar o adaptar la funcionalidad del producto conectado. Dichos servicios relacionados implican la transferencia de datos entre el producto conectado y el proveedor del servicio y debe entenderse que están vinculados expresamente al funcionamiento de las funciones del producto conectado, como servicios que, en su caso, transmiten instrucciones al producto conectado que pueden afectar a su funcionamiento o comportamiento. No deben tener la consideración de servicios relacionados los servicios que no afectan al funcionamiento del producto conectado y no implican la transferencia de datos o instrucciones al producto conectado por parte del proveedor del servicio. Tales servicios podrían incluir, por ejemplo, asesoría auxiliar,

servicios de análisis o financieros o reparaciones y mantenimiento periódicos. Los servicios relacionados pueden ofrecerse como parte del contrato de compraventa, alquiler o arrendamiento. Los servicios relacionados podrían también prestarse para productos del mismo tipo y los usuarios podrían esperar, de manera razonable, que se presten dichos servicios habida cuenta del carácter del producto conectado y 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. Dichos servicios relacionados pueden generar, por sí mismos, datos valiosos para el usuario, independientemente de la capacidad de recopilación de datos del producto conectado 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 caso de duda sobre si el servicio se presta como parte del contrato de compraventa, alquiler o arrendamiento, debe aplicarse el presente Reglamento. Ni el suministro de energía ni la prestación de conectividad deben interpretarse como servicios relacionados en virtud del presente Reglamento.

(18) Por usuario de un producto conectado debe entenderse la persona física o jurídica, como una empresa, un consumidor o un organismo del sector público, que es propietario de un producto conectado, ha recibido determinados derechos temporales, por ejemplo, mediante un contrato de alquiler o arrendamiento, para acceder a los datos obtenidos a partir del producto conectado o utilizarlos, o que recibe servicios relacionados respecto del producto conectado. Estos derechos de acceso no deben obstaculizar ni alterar en modo alguno los derechos de los interesados que puedan estar interactuando con un producto conectado o un servicio relacionado con respecto a los datos personales generados por el producto conectado o durante la prestación del servicio relacionado. El usuario 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 conectado y cualquier servicio relacionado. También debe considerarse usuario a un propietario, alquilador o arrendatario, incluso cuando varias entidades puedan ser consideradas usuarios. En un contexto de múltiples usuarios, cada usuario puede contribuir de manera diferente a la generación de datos y tener interés en varias formas de utilización, como la gestión de la flota para una empresa de arrendamiento o soluciones de movilidad para personas que utilizan un servicio de uso compartido de vehículos.

(19) El término «alfabetización en materia de datos» se refiere a las capacidades, los conocimientos y la comprensión que permiten a usuarios, consumidores y empresas, en particular, las pymes incluidas en el ámbito de aplicación del presente Reglamento, mejorar su concienciación sobre el valor potencial de los datos que generan, producen e intercambian, y les motiva para ofrecer y proporcionar el acceso de conformidad con las normas jurídicas pertinentes. La alfabetización en materia de datos debe ir más allá del aprendizaje sobre herramientas y tecnologías, y debe aspirar a empoderar a los ciudadanos y a las empresas y a dotarlos de la capacidad de beneficiarse de un mercado de datos integrador y justo. La difusión de medidas de alfabetización y la implantación de medidas de seguimiento oportunas podría contribuir a mejorar las condiciones de trabajo y, en última instancia, respaldar la consolidación y la senda de innovación de la economía de los datos en la Unión. Las autoridades competentes deben promover herramientas y adoptar medidas para impulsar las capacidades de alfabetización en materia de datos de los usuarios y entidades incluidos en el ámbito de aplicación del presente Reglamento y su concienciación sobre los derechos y obligaciones que de este se derivan.

(20) En la práctica, no todos los datos generados por productos conectados 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 internet. 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, prácticos y más eficientes. En muchos sectores, los fabricantes, aunque no tengan derecho legal a los datos, pueden determinar, a través del control del diseño técnico de los productos conectados 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 conectados se diseñen y fabriquen —y que los servicios relacionados se diseñen y presten— de manera que los datos de los productos y los datos de los servicios relacionados, incluidos los metadatos asociados necesarios para interpretar y utilizar dichos datos, también a efectos de extraerlos, utilizarlos o compartirlos, siempre sean accesibles para el usuario fácilmente y de forma segura, gratuitamente, en un formato completo, estructurado, de utilización habitual y de lectura mecánica. Se denomina «datos fácilmente disponibles» a los datos del producto y los datos del servicio relacionado que un titular de datos obtiene o puede obtener del producto conectado o servicio relacionado de forma lícita y sin un esfuerzo desproporcionado, por ejemplo, mediante el diseño del producto conectado, el contrato celebrado entre el titular de datos y el usuario para la prestación de servicios relacionados y sus medios técnicos de acceso a los datos. Los datos fácilmente disponibles no incluyen los datos generados por el uso de un producto conectado cuando el diseño del producto conectado no prevea que dichos datos se almacenen o transmitan fuera del componente en que se generan o del producto conectado en su conjunto. Por consiguiente, no

debe entenderse que el presente Reglamento impone la obligación de almacenar datos en la unidad informática central de un producto conectado. La ausencia de tal obligación no debe impedir al fabricante o al titular de datos acordar voluntariamente con el usuario la realización de dichas adaptaciones. Las obligaciones de diseño previstas en el presente Reglamento también se entienden sin perjuicio del principio de minimización de datos establecido en el artículo 5, apartado 1, letra c), del Reglamento (UE) 2016/679 y no deben entenderse en el sentido de que imponen una obligación de diseñar los productos conectados y servicios relacionados de tal manera que almacenen o traten de algún modo datos personales distintos de los necesarios en relación con los fines de su tratamiento. Podrían introducirse disposiciones de Derecho de la Unión o nacional para describir otras especificidades, como los datos del producto que deben ser accesibles desde los productos conectados o los servicios relacionados, dado que dichos datos pueden ser esenciales para el funcionamiento, la reparación o el mantenimiento eficientes de dichos productos conectados o servicios relacionados. Cuando las actualizaciones o modificaciones posteriores de un producto conectado o un servicio relacionado, por parte del fabricante u otra parte, den lugar a datos accesibles adicionales o a una restricción de los datos accesibles inicialmente, esas alteraciones deben comunicarse al usuario en el contexto de la actualización o modificación.

(21) Cuando se considere usuario a varias personas o entidades, por ejemplo en los casos de copropiedad o cuando un propietario, alquilador o arrendatario comparta derechos de acceso a los datos o de utilización de estos, el diseño del producto conectado o servicio relacionado o la interfaz pertinente debe permitir que cada usuario tenga acceso a los datos que genera. Por lo general, el uso de productos conectados que generan datos necesita la creación de una cuenta de usuario. Esta cuenta permite la identificación del usuario por parte del titular de datos, que puede ser el fabricante. También se puede utilizar como medio para comunicarse y para presentar y tramitar las solicitudes de acceso a datos. En caso de que varios fabricantes o proveedores de servicios relacionados hayan vendido, alquilado o arrendado productos conectados o prestado servicios relacionados, integrados entre sí, al mismo usuario, el usuario debe dirigirse a cada una de las partes con las que haya celebrado un contrato. Los fabricantes o diseñadores de un producto conectado que suelen utilizar varias personas deben establecer los mecanismos necesarios para crear cuentas de usuario separadas para personas concretas, cuando proceda, o que varias personas puedan utilizar la misma cuenta de usuario. Las soluciones de cuenta deben permitir al usuario suprimir sus cuentas y los datos relacionados con ellas, y podrían permitirle poner fin al acceso a los datos o a su utilización o intercambio, o presentar solicitudes para ponerle fin, en particular, teniendo en cuenta las situaciones en las que cambia la propiedad o el uso del producto conectado. Debe concederse acceso al usuario mediante un mecanismo de solicitud sencillo, de ejecución automática, que no requiera examen o autorización por parte del fabricante o del titular de datos. Esto significa que los datos deben ponerse a disposición solo cuando el usuario desee el acceso. 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 conectado o servicio relacionado, el fabricante debe informar al usuario de cómo puede acceder a los datos.

(22) Los productos conectados pueden diseñarse para que determinados datos sean directamente accesibles a partir de un almacenamiento de datos en el dispositivo o a partir de un servidor remoto al que se comuniquen los datos. El acceso al almacenamiento de datos en el dispositivo puede habilitarse a través de redes de área local por cable o inalámbricas conectadas a un servicio de comunicaciones electrónicas o red móvil disponibles al público. 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. No se considera que los encargados del tratamiento tal como se definen en el artículo 4, punto 8, del Reglamento (UE) 2016/679 actúan como titulares de datos. Ahora bien, el responsable del tratamiento tal como se define en el artículo 4, punto 7, del Reglamento (UE) 2016/679 les puede encomendar específicamente que pongan datos a disposición. Los productos conectados pueden estar diseñados para permitir al usuario o a un tercero tratar los datos en el producto conectado, en una instancia informática del fabricante o en un entorno de tecnología de la información y las comunicaciones (TIC) elegido por el usuario o el tercero.

(23) Los asistentes virtuales desempeñan un papel cada vez más importante en la digitalización de los entornos de consumo y profesionales y son una interfaz fácil de utilizar que sirve para reproducir contenidos, buscar información o activar productos conectados a internet. 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 internet, 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 inteligentes innovadores. Los derechos de acceso a los datos que establece el presente Reglamento deben ser aplicables a los asistentes virtuales. También deben ser aplicables los derechos de acceso a los datos que establece el presente Reglamento a los datos generados cuando un usuario interactúa con un producto conectado a través de un asistente virtual proporcionado por una entidad distinta del fabricante del producto conectado. Sin embargo, solo deben entrar en el ámbito del presente Reglamento los datos resultantes de la interacción entre el usuario y un producto conectado o servicio relacionado a través del asistente virtual. Los datos producidos por el asistente virtual que no estén relacionados con el uso de un producto conectado o servicio relacionado no se incluyen en el ámbito del presente Reglamento.

(24) Antes de celebrar un contrato de compraventa, alquiler o arrendamiento de un producto conectado, el vendedor o arrendador —que pueden ser el fabricante— deben proporcionar al usuario información sobre los datos del producto que es capaz de generar el producto conectado, incluido el tipo, el formato y el volumen estimado de dichos datos, de manera clara y comprensible. Esto puede incluir información sobre las estructuras de los datos, los formatos de datos, los vocabularios, los sistemas de clasificación, las taxonomías y las listas de códigos, cuando estén disponibles, así como información clara, suficiente y pertinente para el ejercicio de los derechos del usuario sobre cómo pueden almacenarse o extraerse los datos, o cómo se puede acceder a ellos, junto con las descripciones de las condiciones de utilización y la calidad de servicio de las interfaces de programación de aplicaciones o, en su caso, el suministro de paquetes de desarrollo de software. Esa obligación aporta transparencia sobre los datos del producto generados y mejora la facilidad de acceso para el usuario. La obligación de información podría cumplirse, por ejemplo, manteniendo un localizador uniforme de recursos (URL) estable en la web, que puede distribuirse como un enlace web o un código QR, que apunte a la información relevante, que podría ser proporcionado al usuario por el vendedor o arrendador —que puede ser el fabricante— antes de celebrar el contrato de compraventa, alquiler o arrendamiento de un producto conectado. En cualquier caso, resulta necesario que el usuario pueda almacenar la información de manera que sea accesible para su futura consulta y que permita la reproducción inalterada de la información almacenada. No puede esperarse que el titular de datos almacene los datos por tiempo indefinido en vista de las necesidades del usuario del producto conectado, pero debe aplicar, no obstante, una política razonable de conservación de datos, cuando proceda, de conformidad con el principio de limitación del plazo de conservación de conformidad con el artículo 5, apartado 1, letra e), del Reglamento (UE) 2016/679, que permita el ejercicio efectivo de los derechos de acceso a los datos que confiere el presente Reglamento. La obligación de informar no afecta a la obligación del responsable del tratamiento de proporcionar información al interesado de conformidad con los artículos 12, 13 y 14 del Reglamento (UE) 2016/679. La obligación de proporcionar información antes de la celebración de un contrato de prestación de un servicio relacionado debe corresponder al posible titular de datos, con independencia de si el titular de datos celebra un contrato de compraventa, alquiler o arrendamiento de un producto conectado. También debe proporcionarse al usuario la información cuando esta cambie durante la vida útil del producto conectado o el período de vigencia del contrato del servicio relacionado, también cuando la finalidad para la que se utilizarán los datos cambie con respecto a la finalidad especificada inicialmente.

(25) No debe entenderse que el presente Reglamento concede a los titulares de datos ningún nuevo derecho a utilizar los datos del producto o los datos de un servicio relacionado. Cuando el fabricante de un producto conectado sea un titular de datos, la base para que el fabricante utilice datos no personales debe ser un contrato entre el fabricante y el usuario. Dicho contrato podría formar parte de un pacto para la prestación de un servicio relacionado, que podría celebrarse junto con el contrato de compraventa, alquiler o arrendamiento del producto conectado. Toda cláusula contractual que estipule que el titular de datos puede utilizar los datos de un producto o los datos de un servicio relacionado debe ser transparente para el usuario, incluso en lo que respecta a las finalidades para las que el titular de datos pretenda utilizar los datos. Tales finalidades pueden incluir mejorar el funcionamiento del producto conectado o de los servicios relacionados, desarrollar nuevos productos o servicios o agregar datos con el fin de poner a disposición de terceros los datos derivados resultantes, siempre que dichos datos derivados no permitan la identificación de los datos específicos transmitidos al titular de datos desde el producto conectado, ni permitan a un tercero derivarlos del conjunto de datos. Toda modificación del contrato debe depender del consentimiento informado del usuario. El presente Reglamento no impide a las partes pactar cláusulas contractuales cuyo efecto sea excluir o limitar la utilización de datos no personales, o de determinadas categorías de datos no personales, por parte

de un titular de datos. Tampoco impide a las partes pactar la puesta a disposición de terceros de datos del producto o datos del servicio relacionado, de modo directo o indirecto, incluso, en su caso, a través de otro titular de datos. Además, el presente Reglamento no impide requisitos específicos de regulación sectorial en virtud del Derecho de la Unión o del Derecho nacional compatible con el Derecho de la Unión que excluyan o limiten la utilización de determinados datos por parte del titular de datos por razones de políticas públicas bien definidas. El presente Reglamento no impide a los usuarios, en las relaciones entre empresas, poner los datos a disposición de terceros o de titulares de datos con arreglo a cualquier condición contractual lícita, incluso aceptando limitar o restringir el intercambio ulterior de dichos datos, o recibir una compensación proporcional, por ejemplo, a cambio de renunciar a su derecho a utilizar o compartir dichos datos. Aunque el concepto de «titular de datos» generalmente no incluye a los organismos del sector público, puede incluir a empresas públicas.

(26) Para fomentar la aparición de mercados líquidos, equitativos y eficientes de datos no personales, los usuarios de productos conectados deben poder compartir datos con otros, también con fines comerciales, con un mínimo esfuerzo jurídico y técnico. En la actualidad, resulta a menudo difícil para las empresas justificar los costes de personal o informáticos necesarios para preparar conjuntos de datos o productos de datos no personales y ofrecerlos a otras posibles partes a través de servicios de intermediación de datos, incluidos los mercados de datos. Así pues, un obstáculo importante para el intercambio de datos no personales por parte de las empresas dimana de la falta de previsibilidad de los rendimientos económicos derivados de la inversión en la organización y puesta a disposición de conjuntos de datos o productos de datos. A fin de permitir la aparición de mercados líquidos, equitativos y eficientes de datos no personales en la Unión, debe aclararse qué parte tiene derecho a ofrecer dichos datos en un mercado. Por tanto, los usuarios deben tener derecho a compartir datos no personales con destinatarios de datos con fines comerciales y no comerciales. Este intercambio de datos podría ser realizado directamente por el usuario, a través de un titular de datos a petición del usuario, o a través de servicios de intermediación de datos. Los servicios de intermediación de datos, regulados por el Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo ([22]), podrían facilitar la economía de los datos mediante el establecimiento de relaciones comerciales entre los usuarios, los destinatarios de los datos y terceros, y pueden ayudar a los usuarios a ejercer su derecho a utilizar los datos, como, por ejemplo, al garantizar la anonimización de los datos personales o la agregación del acceso a los datos de múltiples usuarios individuales. Cuando los datos estén excluidos de la obligación de un titular de datos de ponerlos a disposición de los usuarios o de terceros, el alcance de dichos datos podría especificarse en el contrato entre el usuario y el titular de datos para la prestación de un servicio relacionado, de manera que los usuarios puedan determinar fácilmente qué datos están a disposición para compartirlos con destinatarios de datos o con terceros. Los titulares de datos no deben poner a disposición de terceros datos no personales del producto con fines comerciales o no comerciales distintos del cumplimiento de su contrato con el usuario, sin perjuicio de los requisitos legales en virtud del Derecho de la Unión o nacional para que un titular de datos los ponga a disposición. Cuando proceda, los titulares de datos deben obligar contractualmente a los terceros a no compartir los datos recibidos de ellos.

(27) En los sectores caracterizados por la concentración de un pequeño número de fabricantes que abastecen de productos conectados a los usuarios finales, los usuarios pueden disponer únicamente de opciones limitadas en lo que respecta al acceso a los datos y a la utilización e intercambio de estos. En tales circunstancias, los contratos pueden resultar insuficientes para alcanzar el objetivo de la capacitación de los usuarios, lo que dificulta a los usuarios obtener valor a partir de los datos generados por el producto conectado que compran, alquilan 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 en la Unión una economía diversa de los datos. 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 agrarios mediante contrato. Pueden adoptarse disposiciones de Derecho de la Unión o nacional para regular las necesidades y objetivos específicos del sector. Además, los titulares de datos no deben utilizar ningún dato fácilmente disponible que constituya un dato no personal, con el fin de obtener información sobre la situación económica del usuario, sus activos o sus métodos de producción o sobre ese uso por

([22]) Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) (DO L 152 de 3.6.2022, p. 1).

el usuario de cualquier otra manera que pueda socavar la posición comercial del usuario en los mercados en los que opera. Esto podría incluir el uso de la información sobre el rendimiento global de una empresa, o de una explotación agraria, en las negociaciones contractuales con el usuario sobre la posible compra 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 tal permiso.

(28) En los contratos entre un titular de datos y un consumidor como usuario de un producto conectado o servicio relacionado que genera datos, se aplica el Derecho de la Unión en materia de protección de los consumidores, en particular las Directivas 93/13/CEE y 2005/29/CE, para garantizar que el consumidor no esté sujeto a cláusulas contractuales abusivas. A efectos del presente Reglamento, las cláusulas contractuales abusivas impuestas unilateralmente a una empresa no deben ser vinculantes para ella.

(29) Los titulares de datos pueden 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 los titulares de datos deben garantizar que el encargado del tratamiento reciba y tramite la solicitud de acceso.

(30) El usuario debe ser libre de utilizar los datos para cualquier fin lícito. Se incluye en ello proporcionar los datos que el usuario haya recibido en el ejercicio de los derechos que le reconoce el presente Reglamento, a un tercero que ofrezca un servicio posventa que pueda estar en competencia con un servicio prestado por un titular de datos, o dar instrucciones al titular de datos para que lo haga. La solicitud debe ser presentada por el usuario o por un tercero autorizado que actúe en nombre del usuario, lo que incluye al proveedor de un servicio de intermediación de datos. Los titulares de datos deben 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 resultantes del uso del producto conectado o servicio relacionado. En el tratamiento de los datos deben respetarse los derechos 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.

(31) La Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo ([23]) establece que la obtención, utilización o revelación de un secreto comercial se consideran lícitas, entre otras cosas, cuando el Derecho de la Unión o nacional exijan o permitan dicha obtención, utilización o revelación. Si bien el presente Reglamento exige a los titulares de datos que divulguen determinados datos a los usuarios o a terceros elegidos por el usuario, incluso cuando dichos datos cumplan los requisitos para ser protegidos como secretos comerciales, debe interpretarse de forma que preserve la protección conferida a los secretos comerciales en virtud de la Directiva (UE) 2016/943. En este contexto, los titulares de datos deben poder exigir al usuario, o a terceros elegidos por el usuario, que preserven la confidencialidad de los datos considerados como secretos comerciales. A tal fin, los titulares de datos deben identificar los secretos comerciales antes de la divulgación y tener la posibilidad de convenir con los usuarios, o con terceros elegidos por el usuario, las medidas necesarias para preservar su confidencialidad, también mediante el uso de cláusulas contractuales tipo, acuerdos de confidencialidad, protocolos de acceso estrictos, normas técnicas y la aplicación de códigos de conducta. Además del uso de cláusulas contractuales tipo que ha de elaborar y recomendar la Comisión, el establecimiento de códigos de conducta y de normas técnicas relativos a la protección de los secretos comerciales en el tratamiento de los datos podría contribuir a la consecución del objetivo del presente Reglamento y debe fomentarse. Cuando no exista un acuerdo sobre las medidas necesarias o cuando el usuario o los terceros elegidos por el usuario no apliquen las medidas convenidas o vulneren la confidencialidad de los secretos comerciales, el titular de datos debe poder retener o suspender el intercambio de los datos identificados como secretos comerciales. En tales casos, el titular de datos debe comunicar la decisión por escrito al usuario o al tercero sin demora indebida y debe notificar a la autoridad competente del Estado miembro en el que el titular de datos esté establecido que ha retenido o suspendido el intercambio de datos e indicar qué medidas no se han convenido o

([23]) Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (DO L 157 de 15.6.2016, p. 1).

aplicado y, en su caso, qué secretos comerciales han visto su confidencialidad comprometida. En principio, los titulares de datos no pueden rechazar una solicitud de acceso a los datos en virtud del presente Reglamento alegando únicamente que determinados datos se consideran secretos comerciales, ya que esto neutralizaría los efectos perseguidos por el presente Reglamento. Sin embargo, en circunstancias excepcionales, un titular de datos que sea un poseedor de un secreto comercial debe poder rechazar, según el caso, una solicitud para los datos específicos en cuestión, si es capaz de demostrar al usuario o al tercero que, a pesar de las medidas técnicas y organizativas tomadas por el usuario o por el tercero, existe una alta probabilidad de que la revelación de dicho secreto comercial ocasione un grave perjuicio económico. Un grave perjuicio económico implica una pérdida económica importante e irreparable. El titular de datos debe, sin demora indebida, motivar debidamente su denegación por escrito al usuario o al tercero y notificarla a la autoridad nacional competente. Dicha motivación debe basarse en elementos objetivos que demuestren el riesgo concreto de grave perjuicio económico que cabe esperar que se derive de una divulgación de datos específica y los motivos por los que las medidas adoptadas para proteger los datos solicitados se consideran insuficientes. En este contexto, puede tenerse en cuenta un posible efecto negativo en la ciberseguridad. Sin perjuicio del derecho a recurrir ante un órgano jurisdiccional de un Estado miembro, cuando el usuario o el tercero deseen impugnar la decisión del titular de datos de denegar, retener o suspender el intercambio de datos, el usuario o el tercero pueden presentar una reclamación ante la autoridad competente, que debe decidir, sin demora indebida, si el intercambio de datos debe iniciarse o reanudarse y en qué condiciones, o pueden convenir con el titular de datos someter la cuestión a un órgano de resolución de litigios. Las excepciones al derecho de acceso a los datos en el presente Reglamento no deben en ningún caso limitar el derecho de acceso y el derecho a la portabilidad de los datos de los interesados en virtud del Reglamento (UE) 2016/679.

(32) El objetivo del presente Reglamento no consiste solo en fomentar el desarrollo de productos conectados o servicios relacionados nuevos e innovadores y estimular la innovación en los mercados de posventa, sino también en estimular el desarrollo de servicios totalmente novedosos que utilicen los datos en cuestión, incluso los basados en datos procedentes de diversos productos conectados o servicios relacionados. Al mismo tiempo, el presente Reglamento pretende evitar la reducción de los incentivos a la inversión para el tipo de producto conectado del que se obtienen datos, por ejemplo, utilizando los datos para desarrollar un producto conectado competidor que los usuarios consideren intercambiable o sustituible atendiendo a sus características, su precio o el uso que se prevea hacer de él. El presente Reglamento no prohíbe el desarrollo de servicios relacionados utilizando datos obtenidos en virtud del presente Reglamento, ya que ello tendría en la innovación un efecto disuasorio no deseable. La prohibición de utilizar los datos a los que se accede en virtud del presente Reglamento para desarrollar un producto conectado competidor protege los esfuerzos de innovación de los titulares de datos. La determinación de si un producto conectado compite con el producto conectado en el que se originan los datos depende de si ambos productos conectados son competidores en el mismo mercado de producto. Esto se debe determinar sobre la base de los principios establecidos en el Derecho de la competencia de la Unión para delimitar el mercado de productos de referencia. No obstante, los fines lícitos para la utilización de los datos podrían incluir la ingeniería inversa, siempre que cumpla los requisitos establecidos en el presente Reglamento y en el Derecho de la Unión o nacional. Este puede ser el caso para la finalidad de reparar o prolongar la vida útil de un producto conectado o de prestar servicios posventa a productos conectados.

(33) Un tercero al que se pongan datos a disposición puede ser una persona física o jurídica, como un consumidor, una empresa, una organización de investigación, una organización sin ánimo de lucro o una entidad que actúe a título profesional. Al poner los datos a disposición del tercero, un 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. Por consiguiente, el titular de datos no debe utilizar ningún dato fácilmente disponible con el fin de obtener información sobre la situación económica, los activos o los métodos de producción del tercero, ni el uso por este de cualquier otra manera que pueda socavar la posición comercial del tercero en los mercados en los que el tercero opera. El usuario debe poder compartir datos no personales con terceros con fines comerciales. Previo acuerdo con el usuario, y con sujeción a lo dispuesto en el presente Reglamento, los terceros deben poder transferir a otros terceros los derechos de acceso a los datos otorgados por el usuario, también a cambio de una compensación. Los intermediarios de datos entre empresas y los sistemas de gestión de información personal, denominados «servicios de intermediación de datos» en el Reglamento (UE) 2022/868, pueden ayudar a los usuarios o los terceros a establecer relaciones comerciales con un número indeterminado de posibles contrapartes para cualquier fin lícito que entre en el ámbito de aplicación del presente Reglamento. Podrían desempeñar un papel fundamental a la hora de agregar el acceso a los datos, de modo que puedan facilitarse los análisis de macrodatos o el aprendizaje automático, siempre que los usuarios mantengan el pleno control de la decisión de proporcionar sus datos a dicha agregación y de las condiciones comerciales en las que se vayan a utilizar sus datos.

(34) El uso de un producto conectado o servicio relacionado puede generar datos relativos al interesado, en particular, cuando el usuario sea una persona física. El tratamiento de dichos datos está sujeto a las normas establecidas en virtud del Reglamento (UE) 2016/679, incluso cuando los datos personales y no personales de un conjunto de datos estén indisolublemente vinculados. El interesado puede ser el usuario u otra persona física. Los datos personales solo pueden 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 uso de un producto conectado, tanto personales como no personales. Cuando el usuario no sea el interesado sino una empresa, incluido un empresario individual, excluidos los casos de uso doméstico compartido del producto conectado, el usuario debe tener la consideración de responsable del tratamiento. Por consiguiente, dicho usuario, que como responsable del tratamiento desea solicitar datos personales generados por el uso de un producto conectado o un servicio relacionado, debe tener una base lícita para el tratamiento de los datos como exige el artículo 6, apartado 1, del Reglamento (UE) 2016/679, como el consentimiento del interesado o la ejecución de un contrato en el que el interesado sea parte. Dicho usuario debe garantizar que el interesado esté debidamente informado de los fines determinados, 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 de mutuo acuerdo, sus responsabilidades respectivas en el cumplimiento de dicho Reglamento. Debe entenderse que dicho usuario, una vez que los datos se hayan puesto a disposición, puede a su vez convertirse en titular de datos si cumple los criterios establecidos en el presente Reglamento y, por tanto, está sujeto a la obligación de poner los datos a disposición en virtud del presente Reglamento.

(35) Los datos del producto o los datos del servicio relacionado solo deben ponerse a disposición de un tercero a petición del usuario. El presente Reglamento complementa en consecuencia el derecho de los interesados, establecido en el artículo 20 del Reglamento (UE) 2016/679, a recibir los datos personales que les incumban en un formato estructurado, de uso habitual y de lectura mecánica, así como a transmitirlos a otro responsable del tratamiento, cuando dichos datos se traten por procedimientos automatizados sobre la base del artículo 6, apartado 1, letra a), o del artículo 9, apartado 2, letra a), o sobre la base de un contrato con arreglo al artículo 6, apartado 1, letra b), de dicho Reglamento. Los interesados también tienen derecho a que los datos personales se transmitan directamente de responsable a responsable, pero solo cuando esto sea técnicamente posible. El artículo 20 del Reglamento (UE) 2016/679 especifica que se trata de los datos proporcionados por el interesado, pero no especifica si ello requiere un comportamiento activo por parte del interesado o si también es aplicable cuando un producto conectado o servicio relacionado, por su diseño, observa el comportamiento de un interesado u otra información relacionada con un interesado de manera pasiva. Los derechos que se derivan del presente Reglamento complementan el derecho a la recepción y la portabilidad de los datos personales en virtud del artículo 20 del Reglamento (UE) 2016/679 de varias maneras. El presente Reglamento concede a los usuarios el derecho a acceder a cualquier dato del producto o dato del servicio relacionado y a ponerlo a disposición de terceros, independientemente de que sea de carácter personal, de la distinción entre datos proporcionados activamente u observados pasivamente y de la base jurídica del tratamiento. A diferencia del 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, asegurando así que los obstáculos técnicos no sigan obstaculizando o impidiendo el acceso a dichos datos. El presente Reglamento también permite a los titulares de datos establecer una compensación razonable a cargo de terceros, pero no del usuario, por los costes en que se incurra al proporcionar acceso directo a los datos generados por el producto conectado 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 establecidos 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 contrato no permite el tratamiento de categorías especiales de datos personales por parte del titular de datos o del tercero.

(36) 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 por el abonado o únicamente para la transmisión de una comunicación. La Directiva 2002/58/CE protege 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 la internet de las cosas se consideran equipos terminales si están directa o indirectamente conectados a una red pública de comunicaciones.

(37) Con el fin de evitar la explotación de los usuarios, los terceros a los que se hayan puesto datos a disposición a petición del usuario deben tratar estos datos solo para la finalidad acordada con el usuario e intercambiarlos con otro tercero solo con el consentimiento del usuario a dicho intercambio.

(38) En consonancia con el principio de minimización de datos, los terceros deben acceder solo a la información necesaria para prestar el servicio solicitado por el usuario. Tras haber recibido acceso a los datos, el tercero debe tratarlos para la finalidad acordada 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. Ni los terceros ni los titulares de datos deben dificultar indebidamente el ejercicio de las opciones o los derechos de los usuarios, tampoco ofreciendo opciones a los usuarios de manera no neutra, o coaccionándolos, engañándolos o manipulándolos de algún modo, o neutralizando o mermando su autonomía, toma de decisiones u opciones, tampoco a través de una interfaz digital de usuario o de una parte de ella. En ese contexto, los terceros o los titulares de datos no deben basarse en los denominados «patrones oscuros» (elementos engañosos) a la hora de diseñar sus interfaces digitales. Los «patrones oscuros» son técnicas de diseño que impulsan 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 vulnerables, de que adopten comportamientos que estos no desean, y para engañarlos induciéndoles a tomar decisiones sobre transacciones de divulgación de datos o para influir injustificadamente en la toma de decisiones de los usuarios del servicio, de tal manera que se neutralice o merme 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 «patrones oscuros». Los terceros y los titulares de datos deben cumplir sus obligaciones en virtud del Derecho de la Unión pertinente, en particular, los requisitos establecidos en las Directivas 98/6/CE ([24]) y 2000/31/CE ([25]) del Parlamento Europeo y del Consejo, y de las Directivas 2005/29/CE y 2011/83/UE.

(39) Los terceros también deben abstenerse de utilizar los datos incluidos en el ámbito de aplicación del presente Reglamento para trazar perfiles de personas, a menos que el tratamiento sea estrictamente necesario para prestar el servicio solicitado por el usuario, incluido en el contexto de las decisiones automatizadas. El requisito de suprimir los datos cuando ya no sean necesarios para el fin acordado con el usuario, salvo que se acuerde otra cosa en relación con los datos no personales, complementa el derecho de supresión del interesado con arreglo al artículo 17 del Reglamento (UE) 2016/679. Cuando un tercero sea un proveedor de un servicio de intermediación de datos se aplican las garantías para el interesado que establece el Reglamento (UE) 2022/868. El tercero puede utilizar los datos para desarrollar un producto conectado o servicio relacionado, nuevo e innovador, pero no para desarrollar un producto conectado competidor.

(40) Las empresas emergentes, las pequeñas empresas, las empresas que se consideran medianas empresas con arreglo al artículo 2 del anexo de la Recomendación 2003/361/CE 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 sean lo más proporcionadas 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. Entre esas empresas muy grandes se cuentan algunas que 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 (UE) 2022/1925 del Parlamento Europeo y del Consejo ([26]) tiene por objeto corregir esas ineficiencias y desequilibrios permitiendo a la Comisión designar a una empresa 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 y la obligación de garantizar los derechos efectivos a la portabilidad de los datos en virtud del artículo 20 del Reglamento (UE) 2016/679. De conformidad con el Reglamento (UE) 2022/1925, y habida cuenta de la inigualable capacidad de esas empresas para adquirir datos, la inclusión de las empresas guardianas de acceso como beneficiarias del

([24]) Directiva 98/6/CE del Parlamento Europeo y del Consejo, de 16 de febrero de 1998, relativa a la protección de los consumidores en materia de indicación de los precios de los productos ofrecidos a los consumidores (DO L 80 de 18.3.1998, p. 27).

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

([26]) Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) (DO L 265 de 12.10.2022, p. 1).

derecho de acceso a los datos no es necesaria para alcanzar el objetivo del presente Reglamento y, por tanto, sería desproporcionada para los titulares de datos sujetos a dichas obligaciones. Esta inclusión también limitaría probablemente los beneficios del presente Reglamento para las pymes, vinculados a la equidad de la distribución del valor de los datos entre los distintos agentes del mercado. Esto significa que una empresa que presta servicios básicos de plataforma que ha sido designada guardián de acceso no puede solicitar ni obtener acceso a los datos de los usuarios generados por el uso de un producto conectado o servicio relacionado o por un asistente virtual sobre la base del presente Reglamento. Además, los terceros a los que se pongan datos a disposición a petición del usuario no pueden poner los datos a disposición de un guardián de acceso. 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. Tampoco impide a esas empresas obtener y utilizar los mismos datos por otros medios lícitos. Los derechos de acceso que confiere el presente Reglamento contribuyen a que los consumidores dispongan de una mayor variedad de servicios. Dado que los acuerdos de carácter voluntario entre guardianes de acceso y titulares de datos no se ven afectados, la limitación de la concesión de acceso a los guardianes de acceso no los excluiría del mercado ni les impediría ofrecer sus servicios.

(41) Habida cuenta del estado actual de la tecnología, resultaría excesivamente gravoso para las microempresas y pequeñas empresas imponer nuevas obligaciones de diseño en relación con los productos conectados fabricados o diseñados que suministran o los servicios relacionados que prestan. Sin embargo, no sucede así cuando, para fabricar o diseñar un producto conectado o para prestar un servicio relacionado, se subcontrata a una microempresa o pequeña empresa que cuenta con una empresa asociada o con una empresa vinculada en el sentido del artículo 3 del anexo de la Recomendación 2003/361/CE que no se considere microempresa o pequeña empresa. En estas situaciones, la empresa que haya subcontratado la fabricación o el diseño a una 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 conectado o un proveedor de servicios relacionados. Se debe aplicar un período transitorio para las empresas que hayan adquirido la condición de medianas empresas menos de un año antes y para los productos conectados durante un año después de la fecha en la que hayan sido introducidos en el mercado por una mediana empresa. Ese período de un año permite a dichas medianas empresas adaptarse y prepararse antes de estar expuestas a la competencia en el mercado de servicios para los productos conectados que fabrican, según los derechos de acceso que confiere el presente Reglamento. Ese período transitorio no se aplica cuando dichas medianas empresas cuenten con una empresa asociada o una empresa vinculada que no tenga la consideración de microempresa o pequeña empresa o cuando dichas medianas empresas hayan sido subcontratadas para fabricar o diseñar el producto conectado o para prestar el servicio relacionado.

(42) Habida cuenta de la variedad de productos conectados que producen datos de distinta naturaleza, volumen y frecuencia, con diferentes niveles de datos y riesgos de ciberseguridad, y que ofrecen oportunidades económicas de diferente valor, y con el fin de garantizar la coherencia de las prácticas de intercambio de datos en el mercado interior, también entre sectores, y de fomentar y promover prácticas justas de intercambio de datos incluso en ámbitos en los que no se conceda tal derecho de acceso a los datos, el presente Reglamento establece normas horizontales sobre las modalidades de acceso a los datos en aquellos supuestos en que un titular de datos esté obligado por el Derecho de la Unión o por la normativa nacional adoptada de conformidad con el Derecho de la Unión a poner los datos a disposición de un destinatario de datos. Dicho acceso debe basarse en condiciones justas, razonables, no discriminatorias y transparentes. Esas normas generales de acceso no se aplican a las obligaciones de poner los datos a disposición en virtud del Reglamento (UE) 2016/679. El intercambio voluntario de datos no se ve afectado por esas normas. Las cláusulas contractuales tipo no vinculantes para el intercambio de datos entre empresas que debe desarrollar y recomendar la Comisión pueden ayudar a las partes a celebrar contratos que incluyan condiciones justas, razonables y no discriminatorias y que se deben aplicar de manera transparente. Sin embargo, la celebración de contratos, que puede incluir las cláusulas contractuales tipo no vinculantes, no debe significar que el derecho a compartir datos con terceros esté condicionado en modo alguno a la existencia de tal contrato. En caso de que las partes no puedan alcanzar un acuerdo contractual sobre el intercambio de datos, ni siquiera con el apoyo de órganos de resolución de litigios, el derecho a compartir datos con terceros es exigible ante los órganos jurisdiccionales nacionales.

(43) 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. Las condiciones de dichos contratos podrían incluir medidas técnicas y organizativas, también en relación con la seguridad de los datos.

(44) A fin de garantizar que las condiciones de acceso obligatorio a los datos sean equitativas para ambas partes de un contrato, 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.

(45) Ningún acuerdo celebrado en las relaciones entre empresas para poner los datos a disposición debe discriminar entre categorías comparables de destinatarios de datos, independientemente de que las partes sean grandes empresas o pymes. Para compensar la falta de información sobre las condiciones que figuran en 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 ser responsabilidad de los titulares 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 los datos a disposición, si dichas diferencias están justificadas por razones objetivas. Esas obligaciones se entienden sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679.

(46) Con el fin de fomentar la inversión continua en la generación y puesta a disposición de datos valiosos, incluidas las inversiones en herramientas técnicas pertinentes, evitando al mismo tiempo cargas excesivas en el acceso a los datos y a su utilización que hagan que el intercambio de datos ya no sea viable desde el punto de vista comercial, el presente Reglamento contiene el principio según el cual, en las relaciones entre empresas, los titulares de datos pueden solicitar una compensación razonable cuando estén obligados con arreglo al Derecho de la Unión o la normativa nacional adoptada de conformidad con el Derecho de la Unión a poner los datos a disposición de un destinatario de datos. Tal compensación no debe entenderse como un pago por los propios datos. La Comisión debe adoptar orientaciones sobre el cálculo que se considera una compensación razonable en la economía de los datos.

(47) En primer lugar, una compensación razonable por el cumplimiento de la obligación en virtud del Derecho de la Unión o la normativa nacional adoptada de conformidad con el Derecho de la Unión para dar cumplimiento a una solicitud de puesta a disposición de datos puede incluir una compensación por los costes en que se haya incurrido al poner los datos a disposición. Esos costes pueden ser técnicos, como los costes necesarios para la reproducción de los datos, su difusión por medios electrónicos y su almacenamiento, pero no para la recopilación o producción de datos. Esos costes técnicos también pueden incluir los costes de tratamiento necesarios para poner los datos a disposición, incluidos los costes asociados al formateo de los datos. Los costes relacionados con la puesta a disposición de datos también pueden incluir los costes destinados a facilitar solicitudes concretas de intercambio de datos. También pueden variar en función del volumen de los datos, así como de las disposiciones adoptadas para ponerlos a disposición. Los acuerdos a largo plazo entre los titulares de datos y los destinatarios de datos, por ejemplo a través de un modelo de suscripción o la utilización de contratos inteligentes, pueden reducir los costes en transacciones periódicas o repetitivas en una relación de negocios. Los costes relacionados con la puesta a disposición de los datos pueden corresponder a una solicitud concreta o ser compartidos con otras solicitudes. En el último caso, un único destinatario de datos no debe pagar la totalidad de los costes de puesta a disposición de los datos. En segundo lugar, una compensación razonable también puede incluir un margen, salvo cuando se trate de pymes y organizaciones de investigación sin ánimo de lucro. El margen puede variar en función de factores relacionados con los propios datos, como el volumen, el formato o la naturaleza de los datos. Puede tener en cuenta los costes de recopilación de los datos. Por lo tanto, un margen puede disminuir cuando el titular de datos haya recopilado los datos para su propia actividad sin inversiones significativas, o puede aumentar cuando las inversiones en la recopilación de datos a efectos de la actividad del titular de datos sean elevadas. Puede limitarse o incluso excluirse en situaciones en las que la utilización de los datos por parte del destinatario de datos no afecte a las propias actividades del titular de datos. El hecho de que los datos sean cogenerados por un producto conectado que sea propiedad, alquilado o arrendado por el usuario también podría reducir el importe de la compensación en comparación con otras situaciones en las que los datos son generados por el titular de datos, por ejemplo durante la prestación de un servicio relacionado.

(48) La intervención no es necesaria cuando el intercambio de datos se realiza entre grandes empresas, ni cuando el titular de datos es una pyme y el destinatario de datos es una gran empresa. En tales casos, se considera que las empresas son capaces de negociar la compensación dentro de los límites de lo que es razonable y no discriminatorio.

(49) Con el fin de proteger a las pymes de cargas económicas excesivas que les dificultarían comercialmente el desarrollo y la gestión de modelos de negocio innovadores, la compensación razonable que pagarían por la puesta a disposición de los datos no debe superar los costes directamente relacionados con la puesta a disposición de los datos. Los costes directamente relacionados son aquellos que son atribuibles a solicitudes individuales, teniendo en cuenta que el titular de los datos debe establecer de forma permanente las interfaces técnicas necesarias o el software y la conectividad necesarios. El mismo régimen debe aplicarse a las organizaciones de investigación sin ánimo de lucro.

(50) En casos debidamente justificados, como cuando sea necesario proteger la participación de los consumidores y la competencia o promover la innovación en determinados mercados, el Derecho de la Unión o la normativa nacional adoptada de conformidad con el Derecho de la Unión pueden disponer que se conceda una compensación regulada por la puesta a disposición de tipos de datos específicos.

(51) La transparencia es un principio importante para garantizar que la compensación solicitada por un titular de datos sea razonable o, si el destinatario de datos es una pyme o una organización de investigación sin ánimo de lucro, 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 de que se trate. A fin de que los destinatarios de datos puedan evaluar y verificar que la compensación cumple los requisitos del presente Reglamento, el titular de datos debe proporcionar al destinatario de datos información con suficiente detalle para calcular la compensación.

(52) 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 unas condiciones justas, razonables y no discriminatorias para la puesta a disposición de los datos, los órganos de resolución de litigios deben ofrecer a las partes una solución sencilla, rápida y económica. Si bien el presente Reglamento solo establece las condiciones que deben cumplir los órganos de resolución de litigios para ser certificados, los Estados miembros son libres de adoptar cualquier norma específica para el procedimiento de certificación, incluida, la expiración o revocación de la certificación. Las disposiciones del presente Reglamento relativas a la resolución de litigios no deben obligar a los Estados miembros a crear órganos de resolución de litigios.

(53) El procedimiento de resolución de litigios en virtud del presente Reglamento es un procedimiento voluntario que permite a los usuarios, titulares de datos y destinatarios de datos acordar someter sus litigios a los órganos de resolución de litigios. Por lo tanto, las partes deben tener libertad para dirigirse a un órgano de resolución de litigios de su elección, ya sea dentro o fuera de los Estados miembros en los que estén establecidas.

(54) A fin de evitar casos de recurso a dos o más órganos de resolución de litigios para un mismo litigio, en particular en una situación transfronteriza, un órgano de resolución de litigios debe poder rechazar la tramitación de una 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.

(55) A fin de garantizar la aplicación uniforme del presente Reglamento, los órganos de resolución de litigios deben tener en cuenta las cláusulas contractuales tipo no vinculantes que debe elaborar y recomendar la Comisión, así como las disposiciones de Derecho de la Unión o nacional que especifiquen las obligaciones de intercambio de datos o las directrices emitidas por las autoridades sectoriales para la aplicación de dichas disposiciones de Derecho.

(56) 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 órgano de resolución de litigios no debe privar a dichas partes de su derecho a recurrir ante un órgano jurisdiccional de un Estado miembro. Los órganos de resolución de litigios deben poner a disposición del público informes anuales de actividad.

(57) Los titulares de datos pueden aplicar medidas técnicas de protección adecuadas para evitar la divulgación y el acceso ilícitos a los datos. Sin embargo, estas medidas no deben discriminar entre destinatarios de datos ni obstaculizar el acceso o la utilización de los datos por los usuarios o destinatarios de datos. En caso de prácticas abusivas por parte de un destinatario de datos, como inducir a error al titular de datos proporcionando información falsa con la intención de utilizar los datos con fines ilícitos, incluido el desarrollo de un producto conectado competidor sobre la base de los datos, el titular de datos y, cuando proceda y no sean la misma persona, el poseedor del secreto comercial o el usuario pueden solicitar al tercero o al destinatario de los datos que aplique medidas correctoras o de reparación sin demora indebida. Toda solicitud de este tipo, y en particular las solicitudes de poner fin a la producción, la oferta o la introducción en el mercado de bienes, datos derivados o servicios, así como las destinadas a poner fin a la importación, la exportación o el almacenamiento de mercancías infractoras o a su destrucción, deben evaluarse a la luz de su proporcionalidad en relación con los intereses del titular de datos, del poseedor del secreto comercial o del usuario.

(58) 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 el acceso a los datos, con el resultado de que dicho acceso sea menos viable desde el punto de vista comercial y, a veces, económicamente prohibitivo. Estos desequilibrios contractuales perjudican a todas las empresas que no cuentan con una capacidad significativa de negociar las condiciones de acceso a los datos, y que podrían no tener otra opción que aceptar cláusulas contractuales de tipo «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 resolución unilateral de obligaciones relacionadas con los datos, no deben ser vinculantes para las empresas cuando dichas condiciones se les hayan impuesto unilateralmente.

(59) 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. Se trata de situaciones del tipo «lo tomas o lo dejas» en las que una parte presenta una determinada cláusula contractual y la otra 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 otra empresa, o una cláusula que se negocie y posteriormente se acuerde de forma modificada entre las partes contratantes no debe considerarse que se haya impuesto unilateralmente.

(60) Además, las normas sobre cláusulas contractuales abusivas deben aplicarse solo 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 resolución unilateral 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.

(61) 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 siguen siendo aplicables. A efectos del presente Reglamento, desviarse manifiestamente de las buenas prácticas comerciales incluiría, entre otras cosas, el menoscabo objetivo de la capacidad de la parte a la que se haya impuesto unilateralmente la cláusula para proteger su interés comercial legítimo en los datos en cuestión.

(62) A fin de garantizar la seguridad jurídica, el presente Reglamento establece una lista de cláusulas que siempre se consideran abusivas y una lista de cláusulas que se presumen abusivas. En este último caso, la empresa que impone la cláusula contractual debe poder refutar la presunción de abuso demostrando que la cláusula contractual enumerada en el presente Reglamento no es abusiva en el caso concreto de que se trate. Si una cláusula contractual no está incluida en la lista de cláusulas que siempre se consideran abusivas o que se presumen abusivas, se aplica la disposición general relativa al carácter abusivo. A este respecto, las cláusulas contractuales enumeradas como abusivas en el presente Reglamento deben servir como referencia para interpretar la disposición general relativa al carácter abusivo. Por último, las cláusulas contractuales tipo no vinculantes 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. Si una cláusula contractual se declara abusiva, el contrato de que se trate debe seguir aplicándose sin ella, a menos que la cláusula contractual abusiva no sea separable de las demás cláusulas del contrato.

(63) En situaciones de necesidad excepcional, puede ser necesario que los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión utilicen en el ejercicio de sus funciones legales de interés público los datos existentes, incluidos, cuando proceda, los metadatos de acompañamiento, para responder a emergencias públicas o en otros casos excepcionales. Las necesidades excepcionales son circunstancias imprevisibles y limitadas en el tiempo, a diferencia de otras circunstancias que podrían planificarse, programarse, ser periódicas o frecuentes. Aunque el concepto de «titular de datos» generalmente no incluye a los organismos del sector público, puede incluir a las empresas públicas. 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. A fin de limitar la carga para las empresas, las microempresas y las pequeñas empresas solo deben estar obligadas a proporcionar datos a los organismos del sector público, a la Comisión, al Banco Central Europeo o a los organismos de la Unión en situaciones de necesidad excepcional en las que se necesiten dichos datos para responder a una emergencia pública y los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión no puedan obtener tales datos por otros medios en tiempo oportuno y de manera efectiva en condiciones equivalentes.

(64) En caso de emergencia pública, ya sea una emergencia de salud pública, una emergencia derivada de una catástrofe natural (incluidas las agravadas por el cambio climático y la degradación del medio ambiente) 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, la Comisión, el Banco Central Europeo o los organismos de la Unión que así lo requieran. La existencia de una emergencia pública debe determinarse o declararse con arreglo al Derecho de la Unión o nacional y sobre la base de los procedimientos pertinentes, incluidos los de las organizaciones internacionales pertinentes. En tales casos, el organismo del sector público debe demostrar que los datos incluidos en el ámbito de la solicitud no podrían obtenerse de otro modo de manera oportuna y eficaz y en condiciones equivalentes, por ejemplo, mediante el suministro voluntario de datos por otra empresa o la consulta de una base de datos pública.

(65) También puede surgir una necesidad excepcional en situaciones en las que no existe emergencia alguna. En tales casos, un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión solo debe poder solicitar datos no personales. El organismo del sector público debe demostrar que los datos son necesarios para la realización de alguna tarea específica desempeñada en interés público que haya sido expresamente prevista por la ley, como la elaboración de estadísticas oficiales o la mitigación o recuperación de una emergencia pública. Además, dicha solicitud solo puede hacerse cuando el organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión haya determinado unos datos específicos que de otro modo no podrían obtenerse de manera oportuna y efectiva y en condiciones equivalentes, y solo si ha agotado todos los demás medios a su disposición para obtener dichos datos, como la obtención de datos mediante acuerdos voluntarios, incluida la compraventa de datos no personales en el mercado mediante la oferta de tarifas de mercado, o el apoyo en las obligaciones existentes de poner datos a disposición o la adopción de nuevas medidas legislativas que puedan garantizar la disponibilidad oportuna de los datos. También deben aplicarse las condiciones y principios aplicables a las solicitudes, como las relacionadas con la limitación de la finalidad, la proporcionalidad, la transparencia y la limitación temporal. En los casos de solicitudes de datos necesarios para la elaboración de estadísticas oficiales, el organismo del sector público solicitante también debe demostrar si el Derecho nacional le permite comprar datos no personales en el mercado.

(66) El presente Reglamento no debe aplicarse ni prejuzgar los acuerdos voluntarios para el intercambio de datos entre entidades públicas y privadas, incluido el suministro de datos por parte de las pymes, y se entiende sin perjuicio de los actos jurídicos de la Unión que prevén solicitudes de información obligatorias de entidades públicas a entidades privadas. El presente Reglamento no debe afectar a las obligaciones impuestas a los titulares de datos de proporcionar datos con motivo de necesidades de carácter no excepcional, en particular, cuando se conozca la gama de datos y de titulares de datos o 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.

(67) El presente Reglamento complementa y se entiende sin perjuicio del Derecho de la Unión y nacional que establezca el acceso a los datos y habilite la utilización de estos con fines estadísticos, en particular, el Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo ([27]), así como los actos jurídicos nacionales relativos a las estadísticas oficiales.

(68) Para el ejercicio de sus funciones en los ámbitos de la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o administrativas, la ejecución de sanciones penales o administrativas, así como la recopilación de datos con fines fiscales o aduaneros, los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión deben basarse en sus competencias en virtud del Derecho de la Unión o nacional. Por consiguiente, el presente Reglamento no afecta a los actos legislativos relativos al intercambio, el acceso y la utilización de datos en dichos ámbitos.

(69) De conformidad con el artículo 6, apartados 1 y 3, del Reglamento (UE) 2016/679, al establecer la base jurídica 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, la Comisión, el Banco Central Europeo o los 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 procedentes de organismos del sector público, la Comisión, el Banco Central Europeo u organismos de la Unión y destinadas a los titulares de datos deben ser específicas, transparentes y proporcionadas en el alcance de su contenido y su granularidad. La finalidad de la solicitud y la utilización prevista de los datos solicitados deben ser específicas y explicarse claramente, y permitir al mismo tiempo la flexibilidad necesaria para que la entidad solicitante desempeñe sus tareas específicas en aras del interés público. La solicitud también debe respetar los intereses legítimos del titular de datos al 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 la Comisión, el Banco Central Europeo o los organismos de la Unión. Para garantizar la transparencia, las solicitudes de datos presentadas por la Comisión, el Banco Central Europeo o los organismos de la Unión deben hacerse públicas sin demora indebida por la entidad que solicita los datos. El Banco Central Europeo y los organismos de la Unión deben informar a la Comisión de sus solicitudes. Si la solicitud de datos la presenta un organismo público, este también debe notificar al coordinador de datos del Estado miembro en el que esté establecido el organismo del sector público. Debe garantizarse la disponibilidad pública en línea de todas las solicitudes. Una vez recibida una notificación de solicitud de datos, la autoridad competente podrá decidir evaluar la legalidad de la solicitud y ejercer sus funciones en relación con el cumplimiento y la aplicación del presente Reglamento. El coordinador de datos debe garantizar la disponibilidad pública en línea de todas las solicitudes presentadas por organismos del sector público.

(70) El objetivo de la obligación de proporcionar los datos es garantizar que los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión tengan los conocimientos necesarios para responder a emergencias públicas, prevenirlas o recuperarse de ellas, o para mantener la capacidad de realizar tareas específicas expresamente previstas por la ley. Los datos obtenidos por dichas entidades pueden ser sensibles desde el punto de vista comercial. Por consiguiente, ni el Reglamento (UE) 2022/868 ni la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo ([28]) deben aplicarse a los datos puestos a disposición en virtud del presente Reglamento, y no deben considerarse 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, siempre que se cumplan las condiciones establecidas en el presente Reglamento, no debe resultar afectada la posibilidad de compartir los datos para llevar a cabo investigaciones o para el desarrollo, la elaboración y la difusión de estadísticas oficiales. Los organismos del sector público también deben poder intercambiar los datos obtenidos en virtud del presente Reglamento con otros organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión con el fin de hacer frente a las necesidades excepcionales para las que se han solicitado los datos.

([27]) Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008 relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) n.º 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas (DO L 87 de 31.3.2009, p. 164).

([28]) 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).

(71) Los titulares de datos deben tener la posibilidad de denegar una solicitud presentada por un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión o pedir su modificación sin demora indebida y, en cualquier caso, en un plazo de cinco o treinta días hábiles, dependiendo del carácter de la necesidad excepcional invocada en la solicitud. Cuando proceda, el titular de datos debe tener esa posibilidad cuando no tenga control sobre los datos solicitados, es decir, cuando no tenga acceso inmediato a los datos y no pueda determinar su disponibilidad. Debe existir una razón válida para no poner los datos a disposición si puede demostrarse que la solicitud es similar a una solicitud presentada previamente con el mismo fin por otro organismo del sector público o la Comisión, el Banco Central Europeo o un organismo de la Unión y no se haya notificado al titular de los datos la supresión de estos con arreglo al presente Reglamento. El titular de datos que deniegue la solicitud o que pida su modificación debe comunicar la justificación subyacente al organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión que solicite los datos. Cuando los derechos *sui generis* sobre bases de datos en virtud de la Directiva 96/9/CE del Parlamento Europeo y del Consejo ([29]) 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, la Comisión, el Banco Central Europeo o un organismo de la Unión obtener los datos o intercambiarlos de conformidad con el presente Reglamento.

(72) Cuando se trate de una necesidad excepcional relacionada con una respuesta a emergencias públicas, los organismos del sector público deben utilizar datos no personales siempre que sea posible. En el caso de solicitudes basadas en una necesidad excepcional no relacionada con una emergencia pública, no pueden solicitarse datos personales. Cuando el alcance de la solicitud incluya datos personales, el titular de los datos debe anonimizarlos. Cuando sea estrictamente necesario incluir datos personales en los datos que deban ponerse a disposición de un organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión, o cuando la anonimización resulte imposible, la entidad que solicite los datos debe demostrar la necesidad estricta y los fines específicos y limitados del tratamiento. Deben cumplirse las normas aplicables en materia de protección de datos personales. La puesta a disposición de los datos y su utilización posterior deben ir acompañadas de garantías para los derechos e intereses de las personas afectadas por dichos datos.

(73) Los datos puestos a disposición de los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión sobre la base de una necesidad excepcional deben utilizarse solo para los fines para los que se solicitaron, a menos que el titular de datos que los haya puesto a disposición haya consentido expresamente que los datos se utilicen para otros fines. Los datos deben suprimirse cuando ya no sean necesarios para los fines indicados en la solicitud, a menos que se acuerde de otro modo, y debe informarse al titular de datos al respecto. El presente Reglamento se basa en los regímenes de acceso existentes en la Unión y en los Estados miembros y no modifica las disposiciones de Derecho nacional en materia de acceso del público a los documentos en el contexto de las obligaciones de transparencia. Los datos deben suprimirse cuando ya no sean necesarios para cumplir dichas obligaciones de transparencia.

(74) Al reutilizar los datos proporcionados por los titulares de datos, los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión deben respetar tanto el vigente Derecho de la Unión o nacional aplicable, como las obligaciones contractuales a las que esté sujeto el titular de datos. Deben abstenerse de desarrollar o mejorar un producto conectado o servicio relacionado que compita con el producto conectado o servicio relacionado del titular de datos, así como de compartir los datos con un tercero para esos fines. Asimismo, deben dar reconocimiento público a los titulares de datos a petición de estos y deben ser responsables de mantener la seguridad de los datos recibidos. Cuando la revelación de secretos comerciales del titular de datos a organismos del sector público, la Comisión, el Banco Central Europeo o los 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 revelación antes de la divulgación de datos.

(75) 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, la Comisión, el Banco Central Europeo o el organismo de la Unión de que se trate compensen a las empresas 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. Al mismo tiempo, la obligación de proporcionar datos podría suponer una carga considerable para las microempresas y las pequeñas empresas. Por lo tanto, deben poder reclamar una compensación incluso en el contexto de la

([29]) 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).

respuesta a emergencias públicas. 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, la Comisión, el Banco Central Europeo o los organismos de la Unión puedan acudir al presente Reglamento. No obstante, en casos de necesidad excepcional distintos de los casos de respuesta a emergencias públicas, que pueden ser más frecuentes, 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, la Comisión, el Banco Central Europeo o el organismo de la Unión. La compensación no debe entenderse como un pago por los propios datos o como obligatoria. Los titulares de datos no deben poder reclamar una compensación cuando el Derecho nacional impida a los institutos nacionales de estadística u otras autoridades nacionales responsables de la elaboración de estadísticas compensar a los titulares de datos por la puesta a disposición de los datos. El organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión de que se trate debe poder impugnar el nivel de compensación solicitado por el titular de datos sometiendo el asunto a la autoridad competente del Estado miembro en el que esté establecido el titular de datos.

(76) Los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión deben tener derecho a intercambiar los datos que hayan 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, siempre y cuando esas actividades sean compatibles con los fines para los que se solicitaron los datos. Debe informar oportunamente al titular de datos de dicho intercambio. Estos datos también pueden intercambiarse en las mismas circunstancias con los institutos nacionales de estadística y Eurostat para desarrollar, elaborar y difundir 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 ha proporcionado. Las personas físicas que lleven a cabo actividades de investigación o las organizaciones de investigación con las que puedan compartirse esos datos deben actuar sin ánimo de lucro o en el contexto de una misión de interés público reconocida por el Estado. Las organizaciones en las que las empresas comerciales tengan una influencia importante, que les permita ejercer un control debido a situaciones estructurales que podría dar lugar a un acceso preferente a los resultados de la investigación, no deben considerarse organizaciones de investigación a efectos del presente Reglamento.

(77) Para hacer frente a una emergencia pública transfronteriza u otra necesidad excepcional, las solicitudes de datos pueden dirigirse a titulares de datos en Estados miembros distintos del organismo del sector público solicitante. En tal caso, el organismo del sector público solicitante debe notificarlo a la autoridad competente del Estado miembro en el que esté establecido el titular de datos para que dicha autoridad pueda examinarla con arreglo a los criterios establecidos en el presente Reglamento. Lo mismo debe aplicarse a las solicitudes presentadas por la Comisión, el Banco Central Europeo o un organismo de la Unión. Cuando se soliciten datos personales, el organismo del sector público debe notificarlo a la autoridad de control responsable de supervisar la aplicación del Reglamento (UE) 2016/679 en el Estado miembro en el que esté establecido el organismo del sector público. La autoridad competente en cuestión debe estar facultada para asesorar al organismo del sector público, a la Comisión, al Banco Central Europeo o al organismo de la Unión para que cooperen con los organismos del sector público del Estado miembro en el que esté establecido el titular de datos en relación con la necesidad de garantizar una carga administrativa mínima para el titular de datos. Cuando la autoridad competente tenga objeciones fundadas respecto de la conformidad de la solicitud con el presente Reglamento, debe rechazar la solicitud del organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión, que deben tener en cuenta dichas objeciones antes de iniciar cualquier acción adicional, incluido volver a presentar la solicitud.

(78) 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 y sin interrupción del servicio, o de utilizar los servicios de varios proveedores simultáneamente sin trabas ni costes indebidos de transferencia de datos, es una condición clave para lograr un mercado más competitivo con menores barreras de entrada para los nuevos proveedores de servicios de tratamiento de datos, y para garantizar una mayor resiliencia para los usuarios de estos servicios. Los clientes que se beneficien de ofertas gratuitas también deben beneficiarse de las disposiciones sobre cambio que se establecen en el presente Reglamento, de modo que esas ofertas no den lugar a una situación de bloqueo para los clientes.

(79) El Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo ([30]) anima a los proveedores de servicios de tratamiento de datos a que desarrollen y apliquen eficazmente códigos de conducta autorreguladores que incluyan las mejores prácticas para, entre otras cosas, facilitar el cambio de proveedor de servicios de tratamiento de datos y la transferencia de datos. Dada la limitada aceptación 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 legales mínimas para los proveedores de servicios de tratamiento de datos a fin de eliminar los obstáculos precomerciales, comerciales, técnicos, contractuales y organizativos, que no se limitan a reducir la velocidad de la transferencia de datos en la salida del cliente, lo que dificulta el cambio efectivo de servicios de tratamiento de datos.

(80) Los servicios de tratamiento de datos deben abarcar los servicios que permiten acceso de red ubicuo y bajo demanda a un conjunto compartido, configurable, modulable y elástico de recursos informáticos distribuidos. Esos recursos informáticos incluyen recursos tales como las redes, los servidores u otras infraestructuras virtuales o físicas, software, incluidas 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 de tratamiento de datos podría describirse como que requiere un esfuerzo mínimo de gestión y conlleva una interacción mínima entre el proveedor y el cliente. El término «ubicuo» se utiliza para describir las capacidades de computación desplegadas en el conjunto de la red y a las que se accede 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 «elástico» se usa para describir los recursos informáticos que se movilizan y liberan 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 «conjunto compartido» se usa para describir recursos informáticos que se proporcionan a múltiples usuarios que comparten un acceso común al servicio, pero en el que el procesamiento 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. Está previsto que la computación en el borde, que es un ejemplo de este tipo de tratamiento de datos muy distribuido, genere nuevos modelos de negocio y de prestación de servicios de computación en nube, que deben ser abiertos e interoperables desde el principio.

(81) El concepto genérico de «servicios de tratamiento de datos» abarca un número considerable de servicios con una gama muy amplia de fines, funcionalidades y estructuras técnicas diferentes. Como generalmente entienden los proveedores y usuarios, y en consonancia con unas normas ampliamente utilizadas, los servicios de tratamiento de datos entran en uno o varios de los tres modelos de prestación de servicios de tratamiento de datos siguientes, a saber, infraestructura como servicio (IaaS, por sus siglas en inglés), plataforma como servicio (PaaS, por sus siglas en inglés) y software como servicio (SaaS, por sus siglas en inglés). Estos modelos de prestación de servicios representan una combinación específica y preestablecida de recursos informáticos ofrecidos por un proveedor de servicios de tratamiento de datos. Esos tres modelos fundamentales de prestación de servicios de tratamiento de datos se complementan con variaciones emergentes, cada una de las cuales consta de una combinación distinta de recursos informáticos, como, por ejemplo, almacenamiento como servicio y base de datos como servicio. Los servicios de tratamiento de datos pueden clasificarse de un modo más detallado y dividirse en una lista no exhaustiva de conjuntos de servicios de tratamiento de datos que comparten el mismo objetivo principal y las mismas funcionalidades principales, así como el mismo tipo de modelos de tratamiento de datos, que no están relacionados con las características operativas del servicio (en lo sucesivo, «mismo tipo de servicio»). Los servicios incluidos en el mismo tipo de servicio pueden compartir el mismo modelo de prestación de servicio de tratamiento de datos; sin embargo, puede parecer que dos bases de datos comparten el mismo objetivo principal, pero, tras considerar su modelo de tratamiento de datos, su modelo de distribución y los casos de utilización a los que se dirigen, dichas bases de datos podrían entrar en una subcategoría más detallada de servicios similares. Los servicios del mismo tipo de servicio pueden tener características diferentes y competidoras, como el rendimiento, la seguridad, la resistencia y la calidad del servicio.

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

(82) Socavar la extracción de los datos exportables que pertenecen al cliente del proveedor de servicios de tratamiento de datos de origen puede impedir el restablecimiento de las funcionalidades del servicio en la infraestructura del proveedor de destino de los servicios de tratamiento de datos. Con el fin de facilitar la estrategia de salida del cliente, evitar tareas innecesarias y gravosas, y garantizar que el cliente no pierda ninguno de sus datos como consecuencia del proceso de cambio, el proveedor de servicios de tratamiento de datos de origen debe informar al cliente previamente del alcance de los datos que puede exportar una vez que el cliente decida cambiar a otro servicio prestado por un proveedor de servicios de tratamiento de datos diferente o a una infraestructura de TIC local. El alcance de los datos exportables debe incluir, como mínimo, los datos de entrada y salida, incluidos los metadatos, generados directa o indirectamente, o cogenerados por el uso del servicio de tratamiento de datos por el cliente, excluidos cualquier activo o dato del proveedor de servicios de tratamiento de datos o de un tercero. Los datos exportables deben excluir cualquier activo o dato del proveedor de servicios de tratamiento de datos o del tercero, que esté protegido por derechos de propiedad intelectual o constituya secreto comercial de dicho proveedor o tercero, o datos relacionados con la integridad y seguridad del servicio, cuya exportación exponga al proveedor de servicios de tratamiento de datos a vulnerabilidades de ciberseguridad. Estas exclusiones no deben impedir ni retrasar el proceso de cambio.

(83) Los activos digitales se refieren a elementos en forma digital para los que el cliente tiene derecho de uso, incluidas las aplicaciones y metadatos relacionados con la configuración de los ajustes, la seguridad y la gestión de los derechos de acceso y control, y otros elementos como las manifestaciones de tecnologías de virtualización, incluidas las máquinas y los contenedores virtuales. Los activos digitales pueden transferirse cuando el cliente tenga derecho de uso independiente de la relación contractual con el servicio de tratamiento de datos del que se propone cambiar. Esos otros elementos son esenciales para la utilización eficaz de los datos y aplicaciones del cliente en el entorno del proveedor de servicios de tratamiento de datos de destino.

(84) El objetivo del presente Reglamento es facilitar el cambio de servicios de tratamiento de datos, que englobe las condiciones y acciones que son necesarias para que un cliente resuelva unilateralmente un contrato de servicio de tratamiento de datos, celebre uno o varios contratos nuevos con diferentes proveedores de servicios de tratamiento de datos y transmita sus datos exportables y activos digitales, y, en su caso, el beneficio de la equivalencia funcional.

(85) El proceso de cambio es una operación impulsada por el cliente que consta de varias fases, incluida la extracción de datos, relativo a la descarga de datos desde el ecosistema del proveedor de servicios de tratamiento de datos de origen; la transformación, cuando los datos se estructuran de modo que no se ajustan al esquema de la ubicación de destino; y la carga de los datos en una nueva ubicación de destino. En una situación específica descrita en el presente Reglamento, la desagregación de un servicio concreto del contrato y su traslado a un proveedor diferente también debe considerarse un cambio. En ocasiones, una entidad tercera gestiona el proceso de cambio en nombre del cliente. En consecuencia, debe entenderse que todos los derechos y obligaciones del cliente establecidos por el presente Reglamento, incluida la obligación de cooperar de buena fe, se aplican a dicha entidad tercera en estas circunstancias. Los proveedores de servicios de tratamiento de datos y los clientes tienen distintos niveles de responsabilidad, en función de las fases del proceso mencionado. Por ejemplo, el proveedor de servicios de tratamiento de datos de origen es responsable de extraer los datos a un formato de lectura mecánica, pero son el cliente y el proveedor de servicios de tratamiento de datos de destino quienes deben cargar los datos en el nuevo entorno, a menos que se haya obtenido un servicio profesional de transición específico. Un cliente que tenga la intención de ejercer los derechos relacionados con el cambio, previstos en el presente Reglamento, debe informar al proveedor de servicios de tratamiento de datos de origen de la decisión de cambiar a un proveedor de servicios de tratamiento de datos diferente, de cambiar a una infraestructura de TIC local o de suprimir los activos y los datos exportables de dicho cliente.

(86) Por equivalencia funcional se entiende restablecer, sobre la base de los datos exportables y los activos digitales del cliente, un nivel mínimo de funcionalidad en el entorno de un nuevo servicio de tratamiento de datos del mismo tipo de servicio después del cambio, cuando el servicio de tratamiento de datos de destino ofrezca un resultado materialmente comparable en respuesta a la misma entrada para características compartidas suministrada al cliente en virtud del contrato. Solo cabe esperar que los proveedores de servicios de tratamiento de datos faciliten la equivalencia funcional de las características que los servicios de tratamiento de datos de origen y de destino ofrecen de forma independiente. El presente Reglamento no constituye una obligación de facilitar la equivalencia funcional para los proveedores de servicios de tratamiento de datos distintos de los que ofrecen servicios del modelo de prestación IaaS.

(87) Los servicios de tratamiento de datos se utilizan en todos los sectores y varían en cuanto a complejidad y tipo de servicio. Esta es una consideración importante con respecto al proceso y a los plazos de transferencia. No obstante, debe poder aplicarse una prórroga del período transitorio por motivos de inviabilidad técnica para permitir la finalización del proceso de cambio en el plazo establecido solo en casos debidamente justificados. La carga de la prueba a este respecto debe recaer plenamente en el proveedor del servicio de tratamiento de datos de que se trate. Esto se entiende sin perjuicio del derecho exclusivo del cliente a prorrogar el período transitorio una vez por un período que el cliente considere más adecuado para sus propios fines. El cliente puede invocar ese derecho a una prórroga antes del período transitorio o durante este, teniendo en cuenta que el contrato sigue siendo aplicable durante el período transitorio.

(88) Los costes por cambio son costes añadidos que exigen los proveedores de tratamiento de datos a sus clientes por el proceso de cambio. Normalmente, estos costes tienen como fin repercutir en el cliente que desee efectuar un cambio los costes en los que pueda incurrir el proveedor de servicios de tratamiento de datos de origen debido al proceso de cambio. Entre los costes por cambio se encuentran los costes relativos al tránsito de los datos de un proveedor de servicios de tratamiento de datos a otro, o hacia un sistema de infraestructura de TIC local (en lo sucesivo, «costes de salida de datos»), o los costes incurridos en acciones de apoyo específicas durante el proceso de cambio. Los costes de salida de datos innecesariamente elevados y otros costes injustificados que no estén relacionados con los costes reales del cambio disuaden a los clientes de cambiar, restringen la libre circulación de datos y pueden limitar la competencia y provocar efectos de bloqueo para los clientes, reduciendo los incentivos para elegir un proveedor de servicios diferente o adicional. Por lo tanto, deben suprimirse los costes por cambio tres años después de la fecha de entrada en vigor del presente Reglamento. Los proveedores de servicios de tratamiento de datos deben poder imponer costes por cambio reducidos hasta esa fecha.

(89) El proveedor de servicios de tratamiento de datos de origen debe poder externalizar determinadas tareas y compensar a entidades terceras con el fin de cumplir las obligaciones establecidas en el presente Reglamento. Un cliente no debe asumir los costes derivados de la externalización de servicios contratada por el proveedor de servicios de tratamiento de datos de origen durante el proceso de cambio, y dichos costes deben considerarse injustificados, a menos que cubran el trabajo realizado por el proveedor de servicios de tratamiento de datos, a petición del cliente, de apoyo adicional en el proceso de cambio que vayan más allá de las obligaciones que el presente Reglamento impone expresamente al proveedor en razón de un cambio. Nada de lo dispuesto en el presente Reglamento impide que un cliente compense a entidades terceras por el apoyo en el proceso de migración, ni que las partes acuerden contratos para servicios de tratamiento de datos de duración determinada, incluidas sanciones proporcionadas por resolución anticipada para cubrir la resolución unilateral anticipada de dichos contratos, de conformidad con el Derecho de la Unión o nacional. Para fomentar la competencia, la supresión gradual de los costes asociados al cambio entre distintos proveedores de servicio de tratamiento de datos debe incluir específicamente los costes de salida de datos impuestos por un proveedor de servicios de tratamiento de datos a un cliente. Los costes estándar del servicio por la prestación de los servicios de tratamiento de datos en sí mismos no constituyen costes por cambio. Esos costes estándar del servicio no pueden ser suprimidos y siguen siendo aplicables hasta que deje de aplicarse el contrato de prestación de los servicios pertinentes. El presente Reglamento permite al cliente solicitar la prestación de servicios adicionales que vayan más allá de las obligaciones que el presente Reglamento impone al proveedor en razón de un cambio. Esos servicios adicionales pueden ser prestados y facturados por el proveedor cuando se presten a petición del cliente y este acepte por adelantado el precio de dichos servicios.

(90) Hace falta un enfoque regulador para la interoperabilidad que sea ambicioso y que inspire la innovación para superar la dependencia de un solo proveedor, que obstaculiza la competencia y el desarrollo de nuevos servicios. La interoperabilidad entre servicios de tratamiento de datos implica múltiples interfaces y niveles de infraestructuras y programas informáticos, y rara vez se limita a una prueba binaria de si se puede lograr o no. Por el contrario, la construcción de dicha interoperabilidad está sujeta a un análisis de costes y beneficios que es necesario para determinar si vale la pena perseguir resultados razonablemente previsibles. La norma ISO/IEC 19941:2017 es una importante norma internacional que constituye una referencia importante para la consecución de los objetivos del presente Reglamento, ya que contiene consideraciones técnicas que aclaran la complejidad de dicho proceso.

(91) 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 sigan vinculados por las obligaciones del presente Reglamento en lo relativo a sus propias ofertas de servicios.

(92) Los proveedores de servicios de tratamiento de datos deben estar obligados a ofrecer toda la asistencia y el apoyo, dentro de su capacidad y en proporción a sus respectivas obligaciones, que se requiere para que el proceso de cambio a un servicio de otro proveedor de servicios de tratamiento de datos sea satisfactorio, eficaz y seguro. El presente Reglamento no exige a los proveedores de servicios de tratamiento de datos que desarrollen nuevas categorías de servicios de tratamiento de datos, tampoco en el marco o sobre la base de la infraestructura informática de diferentes proveedores de servicios de tratamiento de datos con objeto de garantizar la equivalencia funcional en un entorno distinto del de sus propios sistemas. Un proveedor de servicios de tratamiento de datos de origen no tiene acceso ni información sobre el entorno del proveedor de servicios de tratamiento de datos de destino. No debe entenderse que la equivalencia funcional obliga al proveedor de servicios de tratamiento de datos de origen a reconstruir el servicio en cuestión dentro de la infraestructura del proveedor de servicios de tratamiento de datos de destino. En cambio, el proveedor de servicios de tratamiento de datos de origen debe adoptar todas las medidas razonables a su alcance para facilitar el proceso de lograr la equivalencia funcional proporcionando capacidades, información adecuada, documentación, apoyo técnico y, en su caso, las herramientas necesarias.

(93) También debe exigirse a los proveedores de servicios de tratamiento de datos que eliminen los obstáculos existentes y no impongan otros nuevos, también para los clientes que deseen cambiar a una infraestructura de TIC local. Los obstáculos pueden ser, entre otros, de carácter precomercial, comercial, técnico, contractual u organizativo. Los proveedores de servicios de tratamiento de datos también deben estar obligados a eliminar los obstáculos a la desagregación de un servicio concreto de otros servicios de tratamiento de datos prestados en virtud de un contrato y a poner el servicio pertinente a disposición para el cambio, cuando no existan obstáculos técnicos importantes y demostrados que impidan dicha separación.

(94) A lo largo de todo el proceso de cambio debe mantenerse un alto nivel de seguridad. Esto significa que el proveedor de servicios de tratamiento de datos de origen debe ampliar el nivel de seguridad al que se comprometió para el servicio a todas las modalidades técnicas de las que dicho proveedor es responsable durante el proceso de cambio, como las conexiones de red o los dispositivos físicos. Los derechos existentes en relación con la resolución unilateral de los contratos, incluidos los introducidos por el Reglamento (UE) 2016/679 y la Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo ([31]) no deben verse afectados. El presente Reglamento no debe entenderse como que impide a los proveedores de servicios de tratamiento de datos prestar o proporcionar a sus clientes servicios, características y funcionalidades nuevos y mejorados o competir con otros proveedores de servicios de tratamiento de datos sobre esa base.

(95) La información que han de proporcionar los proveedores de servicios de tratamiento de datos a los clientes podría apoyar la estrategia de salida del cliente. Dicha información debe incluir procedimientos para iniciar el cambio del servicio de tratamiento de datos; los formatos de datos de lectura mecánica a los que pueden exportarse los datos del usuario; las herramientas destinadas a exportar datos, incluidas las interfaces abiertas, así como la información sobre compatibilidad con normas armonizadas o especificaciones comunes basadas en especificaciones de interoperabilidad abierta; información sobre las restricciones y limitaciones técnicas conocidas que podrían afectar al proceso de cambio; y el tiempo estimado necesario para completar el proceso de cambio.

(96) Para facilitar la interoperabilidad y el cambio entre servicios de tratamiento de datos, los usuarios y proveedores de servicios de tratamiento de datos deben considerar el uso de herramientas de ejecución y cumplimiento, en particular las publicadas por la Comisión en forma de un código normativo de la UE sobre computación en la nube y unas directrices sobre contratación pública de servicios de tratamiento de datos. En particular, las cláusulas

([31]) 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).

contractuales estándar son beneficiosas porque incrementan la confianza en los servicios de tratamiento de datos, crean una relación más equilibrada entre usuarios y proveedores de servicios de tratamiento de datos y mejoran la seguridad jurídica sobre las condiciones aplicables para el cambio a otros servicios de tratamiento de datos. En ese contexto, los usuarios y proveedores de servicios de tratamiento de datos deben considerar el uso de cláusulas contractuales estándar u otras herramientas autorreguladoras de cumplimiento, siempre que cumplan el presente Reglamento, desarrolladas por los organismos o grupos de expertos pertinentes establecidos en virtud del Derecho de la Unión.

(97) Con el fin de facilitar el cambio entre servicios de tratamiento de datos, todas las partes implicadas, incluidos los proveedores de servicios de tratamiento de datos, tanto de origen como de destino, deben cooperar de buena fe para que el proceso de cambio se haga efectivo, permitir la transferencia segura y oportuna de los datos necesarios en un formato de utilización habitual, de lectura mecánica y mediante interfaces abiertas, al mismo tiempo que se evitan perturbaciones del servicio y se mantiene la continuidad del servicio.

(98) Los servicios de tratamiento de datos que se refieran a servicios la mayor parte de cuyas características principales se hayan desarrollado a medida para responder a las demandas específicas de un cliente concreto o en los que todos los componentes se hayan desarrollado a efectos de un cliente individual deben quedar exentos de algunas de las obligaciones aplicables al cambio de servicio de tratamiento de datos. Esto no debe incluir los servicios que el proveedor de servicios de tratamiento de datos ofrece a gran escala comercial a través de su catálogo de servicios. Una de las obligaciones del proveedor de servicios de tratamiento de datos es informar debidamente a los posibles clientes de tales servicios, antes de la celebración de un contrato, de las obligaciones establecidas en el presente Reglamento que no se aplican a los servicios pertinentes. Nada impide al proveedor de servicios de tratamiento de datos desplegar finalmente dichos servicios a escala, en cuyo caso dicho proveedor tendría que cumplir todas las obligaciones ligadas al cambio establecidas en el presente Reglamento.

(99) En consonancia con el requisito mínimo de permitir el cambio de proveedor de servicios de tratamiento de datos, el presente Reglamento también tiene por objeto mejorar la interoperabilidad para el uso paralelo de múltiples servicios de tratamiento de datos con funcionalidades complementarias. Esto se refiere a situaciones en las que los clientes no ponen fin a un contrato para cambiar a otro proveedor de servicios de tratamiento de datos, sino en las que múltiples servicios de distintos proveedores se utilizan en paralelo, de manera interoperable, para beneficiarse de las funcionalidades complementarias de los diferentes servicios en la configuración del sistema del cliente. Sin embargo, se reconoce que la salida de datos de un proveedor de servicios de tratamiento de datos a otro para facilitar el uso paralelo de los servicios puede ser una actividad continua, a diferencia de la salida puntual requerida como parte del proceso de cambio. Por lo tanto, los proveedores de servicios de tratamiento de datos deben poder seguir cobrando por la salida de datos, sin superar los costes incurridos, para fines de uso paralelo tres años después de la fecha de entrada en vigor del presente Reglamento. Esto es importante, entre otras cosas, para el despliegue eficaz de estrategias multinube, que permiten a los clientes aplicar estrategias informáticas preparadas para el futuro y reducen la dependencia de proveedores concretos de servicios de tratamiento de datos. Facilitar un enfoque multinube para los clientes de servicios de tratamiento de datos también contribuye a aumentar su resiliencia operativa digital, tal como se reconoce para las entidades de servicios financieros en el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo ([32]).

(100) Se espera que las especificaciones y normas de interoperabilidad abiertas desarrolladas de conformidad con el anexo II del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([33]) en el ámbito de la interoperabilidad y la portabilidad permitan un entorno en la nube multiproveedor, que constituye un requisito clave para la innovación abierta en la economía de los datos europea. Dado que la adopción por el mercado de las normas definidas en el marco de la iniciativa de coordinación de la normalización en la nube (CSC), concluida en 2016, ha sido limitada, también es necesario que la Comisión confíe en las partes del mercado para desarrollar las especificaciones de interoperabilidad abiertas pertinentes a fin de seguir el rápido ritmo del desarrollo

([32]) Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 (DO L 333 de 27.12.2022, p. 1).

([33]) Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

tecnológico en este sector. La Comisión puede adoptar entonces estas especificaciones de interoperabilidad abiertas en forma de especificaciones comunes. Además, cuando los procesos centrados en el mercado no hayan demostrado una capacidad de establecer especificaciones comunes o normas que faciliten la interoperabilidad efectiva en la nube en los niveles PaaS y SaaS, 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 para los tipos específicos de servicios para los que aún no existen tales normas. Además de ello, la Comisión va a animar a los actores del mercado a desarrollar las especificaciones de interoperabilidad abiertas pertinentes. Después de consultar a las partes interesadas, la Comisión, mediante actos de ejecución, debe poder hacer obligatorio el uso de normas armonizadas de interoperabilidad o especificaciones comunes para tipos de servicios específicos a través de una referencia en un repositorio central de la Unión de normas para la interoperabilidad de los servicios de tratamiento de datos. Los proveedores de servicios de tratamiento de datos deben garantizar la compatibilidad con dichas normas armonizadas y especificaciones comunes basadas en especificaciones de interoperabilidad abiertas, que no deben afectar negativamente a la seguridad ni a la integridad de los datos. Las normas armonizadas de interoperabilidad de los servicios de tratamiento de datos y las especificaciones comunes basadas en especificaciones de interoperabilidad abiertas tendrán su referencia solo si cumplen los criterios especificados en el presente Reglamento, que tienen el mismo significado que los requisitos del anexo II del Reglamento (UE) n.º 1025/2012 y las facetas de interoperabilidad definidas en la norma internacional ISO/IEC 19941:2017. Además, la normalización debe tener en cuenta las necesidades de las pymes.

(101) Los terceros países pueden adoptar leyes, reglamentaciones y otros actos jurídicos que tengan por objeto transferir directamente o proporcionar el acceso de las administraciones públicas a datos no personales que se encuentran fuera de sus fronteras, también 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 del Derecho de un tercer país entre en conflicto con una obligación de proteger dichos datos en virtud del Derecho de la Unión o del Derecho nacional del Estado miembro que corresponda, 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, incluidos sus compromisos contractuales en materia de confidencialidad conforme a dicho Derecho. Cuando no existan acuerdos internacionales que regulen estas cuestiones, la transferencia o el acceso a datos no personales han de permitirse solo si se ha verificado que 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 esté sujeta a examen por un órgano jurisdiccional competente del tercer país, facultado para tomar debidamente en cuenta los intereses jurídicos pertinentes del proveedor de dichos 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 antes de conceder acceso a dichos datos a fin de verificar la existencia de un conflicto potencial de dicho acceso con el Derecho de la Unión o nacional, como el relativo 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.

(102) Para impulsar la confianza en los datos es esencial que las salvaguardas para garantizar a los ciudadanos, los organismos del sector público y las empresas de la Unión el control de sus datos se apliquen en la medida de lo posible. 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 privacidad, y la protección de los consumidores, entre otros aspectos. Con el fin de evitar el acceso ilícito de las administraciones públicas a datos no personales por parte de las autoridades de terceros países, los proveedores de servicios de tratamiento de datos sujetos al presente Reglamento, 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, el sometimiento frecuente a auditorías, el respeto verificado de los pertinentes sistemas de certificación de garantías de seguridad y la modificación de las políticas de empresa.

(103) La normalización y la interoperabilidad semántica deben desempeñar un papel clave para proporcionar soluciones técnicas que garanticen la interoperabilidad dentro de los espacios comunes europeos de datos, y entre ellos, que son marcos interoperables de normas y prácticas comunes, específicos para un fin o un sector o intersectoriales, con el fin de compartir o tratar conjuntamente los datos para, entre otros, el desarrollo de nuevos productos y servicios, la investigación científica o las iniciativas de la sociedad civil. El presente Reglamento establece determinados requisitos esenciales de interoperabilidad. Los participantes en espacios de datos que ofrezcan datos o servicios basados en datos a otros participantes, que son entidades que facilitan o participan en el intercambio de datos dentro de espacios comunes europeos de datos, incluidos los titulares de datos, deben cumplir esos requisitos en lo que respecta a los elementos que estén bajo su control. El cumplimiento de esas normas se puede garantizar mediante el cumplimiento de los requisitos esenciales establecidos en el presente Reglamento o presuponer mediante el cumplimiento de normas armonizadas o especificaciones comunes a través de una presunción de conformidad. 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 estas de conformidad con el Reglamento (UE) n.º 1025/2012, que representa el marco por defecto para elaborar normas que prevean tales presunciones. La Comisión debe evaluar los obstáculos a la interoperabilidad y dar prioridad a las necesidades de normalización, sobre cuya base puede solicitar a una o varias organizaciones europeas de normalización, de conformidad con el Reglamento (UE) n.º 1025/2012, que elaboren normas armonizadas que satisfagan los requisitos esenciales establecidos en el presente Reglamento. Cuando dichas solicitudes no den lugar a normas armonizadas o dichas normas armonizadas sean insuficientes para garantizar la conformidad con los requisitos esenciales del presente Reglamento, la Comisión debe poder adoptar especificaciones comunes en esos ámbitos, siempre que al hacerlo respete debidamente el papel y las funciones de las organizaciones de normalización. La adopción de especificaciones comunes debe tener lugar únicamente como solución alternativa excepcional para facilitar el cumplimiento de los requisitos esenciales del presente Reglamento o cuando el proceso de normalización esté bloqueado o cuando se produzcan retrasos en el establecimiento de normas armonizadas adecuadas. Cuando dichos retrasos se deban a la complejidad técnica de la norma en cuestión, la Comisión debe tenerlo en cuenta antes de considerar la posibilidad de establecer especificaciones comunes. Las especificaciones comunes se deben elaborar de manera abierta e inclusiva y se debe tener en cuenta, cuando proceda, el asesoramiento del Comité Europeo de Innovación en materia de Datos (CEID) establecido por el Reglamento (UE) 2022/868. Por otra parte, se podrían adoptar especificaciones comunes en distintos sectores, de conformidad con el Derecho de la Unión o nacional, sobre la base de las necesidades específicas de dichos sectores. Además, la Comisión debe estar facultada para hacer obligatorio el desarrollo de normas armonizadas para la interoperabilidad de los servicios de tratamiento de datos.

(104) A fin de promover la interoperabilidad de las herramientas para la ejecución automatizada de los acuerdos de intercambio de datos, es necesario establecer requisitos esenciales para los contratos inteligentes que los profesionales creen para terceros o que se integren en aplicaciones que apoyen la ejecución de acuerdos para el 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 de los contratos inteligentes que cumplan las normas armonizadas o partes de estas de conformidad con el Reglamento (UE) n.º 1025/2012. El concepto de «contrato inteligente» en el presente Reglamento es tecnológicamente neutro. Los contratos inteligentes, por ejemplo, pueden estar conectados a un libro mayor electrónico. Los requisitos esenciales deben aplicarse únicamente a los proveedores de contratos inteligentes, exceptuando cuando desarrollen contratos inteligentes internamente exclusivamente para uso interno. El requisito esencial de garantizar que los contratos inteligentes se puedan interrumpir y resolver unilateralmente implica el consentimiento mutuo de las partes en el acuerdo de intercambio de datos. La aplicabilidad de las normas pertinentes de la normativa civil, contractual y de protección de los consumidores a los acuerdos de intercambio de datos sigue o debe seguir sin verse afectada por el uso de contratos inteligentes para la ejecución automatizada de tales acuerdos.

(105) Para demostrar el cumplimiento de los requisitos esenciales del presente Reglamento, el proveedor de un contrato inteligente o, en su defecto, la persona cuya actividad comercial, empresarial o profesional implique el despliegue de contratos inteligentes para terceros en el contexto de la ejecución total o parcial de un acuerdo de puesta a disposición de datos en el contexto del presente Reglamento, debe realizar una evaluación de conformidad y expedir una declaración UE de conformidad. Dicha evaluación de conformidad debe estar sujeta a los principios generales establecidos en el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo ([34]) y en la Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo ([35]).

([34]) Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

([35]) Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo (DO L 218 de 13.8.2008, p. 82).

(106) Además de obligar a los desarrolladores profesionales de contratos inteligentes a cumplir los requisitos esenciales, también es importante animar a aquellos participantes dentro de espacios de datos que ofrezcan datos o servicios basados en datos a otros participantes dentro de los espacios comunes europeos de datos, y a través de ellos, a apoyar la interoperabilidad de las herramientas para el intercambio de datos, incluidos los contratos inteligentes.

(107) A fin de garantizar la aplicación e implementación 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, a un coordinador de datos entre ellas. Es preciso que las autoridades competentes cooperen entre sí. Mediante el ejercicio de sus poderes de investigación de conformidad con los procedimientos nacionales aplicables, las autoridades competentes deben poder buscar y obtener información, en particular, en relación con las actividades de entidades dentro de sus competencias y, también en el contexto de investigaciones conjuntas, teniendo debidamente en cuenta que las medidas de supervisión y ejecución relativas a una entidad bajo la competencia de otro Estado miembro deben ser adoptadas por la autoridad competente de ese otro Estado miembro, cuando proceda, de conformidad con los procedimientos relativos a la cooperación transfronteriza. Las autoridades competentes deben prestarse asistencia mutua y oportuna, en particular cuando una autoridad competente de un Estado miembro posea información pertinente para una investigación llevada a cabo por las autoridades competentes en otros Estados miembros, o pueda recopilar dicha información a la que las autoridades competentes del Estado miembro en el que esté establecida la entidad no tengan acceso. Las autoridades competentes y los coordinadores de datos deben identificarse en el registro público llevado por la Comisión. El coordinador de datos podría ser un medio adicional para facilitar la cooperación en situaciones transfronterizas, como cuando una autoridad competente de un Estado miembro determinado no sepa a qué autoridad debe dirigirse en el Estado miembro del coordinador de datos, por ejemplo, cuando el caso esté relacionado con más de una autoridad competente o sector. El coordinador de datos debe actuar, entre otras cosas, como punto de contacto único para todas las cuestiones relacionadas con la aplicación del presente Reglamento. Cuando no se haya designado un coordinador de datos, la autoridad competente debe asumir las tareas asignadas al coordinador de datos en virtud del presente Reglamento. Las autoridades responsables de la supervisión del cumplimiento de la normativa en materia de protección de datos y las autoridades competentes designadas con arreglo al Derecho de la Unión o nacional deben ser responsables de la aplicación del presente Reglamento en sus ámbitos de competencia. A fin de evitar conflictos de intereses, las autoridades competentes responsables de la aplicación y ejecución del presente Reglamento en el ámbito de la puesta a disposición de datos a raíz de una solicitud sobre la base de una necesidad excepcional no deben beneficiarse del derecho a presentar dicha solicitud.

(108) 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 reclamaciones. El coordinador de datos debe proporcionar, cuando se le solicite, toda la información necesaria a las personas físicas y jurídicas para la presentación de sus denuncias ante la correspondiente autoridad competente. Dichas autoridades deben ser obligadas a cooperar para garantizar que una denuncia se gestione y resuelva adecuadamente, de manera efectiva y en tiempo oportuno. 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 ([36]) y de la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo ([37]).

(109) Las autoridades competentes deben garantizar que el incumplimiento de las obligaciones establecidas en el presente Reglamento esté sujeto a sanciones. Dichas sanciones podrían consistir en sanciones económicas, advertencias, amonestaciones u órdenes para que las prácticas comerciales se ajusten a las obligaciones impuestas por el presente Reglamento. Las sanciones establecidas por los Estados miembros deben ser efectivas, proporcionadas y disuasorias, y deben tener en cuenta las recomendaciones del CEID, contribuyendo así a lograr el mayor nivel posible de coherencia en el establecimiento y la aplicación de sanciones. Cuando proceda, las autoridades competentes deben recurrir a medidas provisionales para limitar los efectos de una supuesta infracción mientras la investigación de dicha infracción esté en curso. Al hacerlo, deben tener en cuenta, entre otros factores, la naturaleza, gravedad,

([36]) 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).

([37]) 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).

magnitud y duración de la infracción, atendiendo al interés público en juego, el alcance y el tipo de actividades realizadas, así como la capacidad económica del infractor. También deben tener en cuenta si la parte infractora incumple sistemática o repetidamente las obligaciones que le incumben en virtud del presente Reglamento. A fin de garantizar el respeto del principio *non bis in idem* y, en particular, evitar que la misma infracción de las obligaciones establecidas en el presente Reglamento se sancione más de una vez, el Estado miembro que tenga la intención de ejercer su competencia en relación con una parte infractora que no esté establecida en la Unión ni tenga en ella un representante legal debe informar, sin demora indebida, a todos los coordinadores de datos, así como a la Comisión.

(110) El CEID debe asesorar y prestar asistencia a la Comisión en la coordinación de las prácticas y políticas nacionales sobre los temas contemplados por el presente Reglamento, así como en la consecución de sus objetivos en relación con la normalización técnica para mejorar la interoperabilidad. También debe desempeñar un papel clave a la hora de facilitar debates exhaustivos entre las autoridades competentes sobre la aplicación y control del cumplimiento del presente Reglamento. Ese intercambio de información tiene por objeto aumentar el acceso efectivo a la justicia, así como la ejecución y cooperación judicial en toda la Unión. Entre otras funciones, las autoridades competentes deben recurrir al CEID como plataforma para evaluar, coordinar y adoptar recomendaciones sobre el establecimiento de sanciones por infracciones del presente Reglamento. Dicho Comité debe permitir a las autoridades competentes, con la ayuda de la Comisión, a coordinar el enfoque óptimo para determinar e imponer dichas sanciones. Ese enfoque evita la fragmentación, dejando al mismo tiempo flexibilidad a los Estados miembros, y debe dar lugar a recomendaciones eficaces que respalden la aplicación coherente del presente Reglamento. El CEID también debe desempeñar un papel consultivo en los procesos de normalización y en la adopción de especificaciones comunes mediante actos de ejecución, en la adopción de actos delegados para establecer un mecanismo de seguimiento de los costes por cambio impuestos por los proveedores de servicios de tratamiento de datos y para especificar en mayor medida los requisitos esenciales para la interoperabilidad de los datos, de los mecanismos y servicios de intercambio de datos, así como de los espacios comunes europeos de datos. También debe asesorar y prestar asistencia a la Comisión en la adopción de las directrices que establecen especificaciones de interoperabilidad para el funcionamiento de los espacios comunes europeos de datos.

(111) Con el fin de ayudar a las empresas a redactar y negociar contratos, la Comisión debe desarrollar y recomendar cláusulas contractuales tipo no vinculantes 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. Esas cláusulas contractuales tipo serán principalmente una herramienta práctica para ayudar en particular a las pymes a celebrar un contrato. Cuando se utilicen de forma generalizada e integral, esas cláusulas contractuales tipo también deben tener el efecto beneficioso de influir en el diseño de los contratos sobre el acceso y la utilización 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.

(112) 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 u otros datos generados por máquinas, reclamen el derecho *sui generis* en virtud del artículo 7 de la Directiva 96/9/CE obstaculizando de este modo, en particular, 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. Ello no obsta a la posible aplicación del derecho *sui generis* en virtud del artículo 7 de la Directiva 96/9/CE a bases de datos que contengan datos que no entren en el ámbito de aplicación del presente Reglamento, siempre que se cumplan los requisitos de protección en virtud del apartado 1 de dicho artículo.

(113) A fin de tener en cuenta los aspectos técnicos de los servicios de tratamiento de datos, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del TFUE, por lo que respecta a complementar el presente Reglamento a fin de establecer un mecanismo de supervisión de los costes por cambio impuestos por los proveedores de servicios de tratamiento de datos en el mercado y especificar más detalladamente los requisitos esenciales sobre interoperabilidad exigibles a los participantes en espacios de datos que ofrecen datos o servicios de datos a otros participantes. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas

durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación ([38]). 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.

(114) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución en lo relativo a la adopción de especificaciones comunes que garanticen la interoperabilidad de los datos, de los mecanismos y servicios de intercambio de datos, así como de los espacios comunes europeos de datos, de especificaciones comunes para la interoperabilidad de los servicios de tratamiento de datos, y de especificaciones comunes para la interoperabilidad de los contratos inteligentes. También deben conferirse a la Comisión competencias de ejecución con el fin de publicar las referencias de las normas armonizadas y especificaciones comunes para la interoperabilidad de servicios de tratamiento de datos en un repositorio central de la Unión de normas para la interoperabilidad de los servicios de tratamiento de datos. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo ([39]).

(115) 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 proporcionar 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 la utilización de datos, como los relacionados con la gobernanza o los requisitos de seguridad, incluidos los requisitos de ciberseguridad. Asimismo, el presente Reglamento debe entenderse sin perjuicio de normas más específicas en el contexto del desarrollo de espacios comunes europeos de datos o, salvo las excepciones previstas en el presente Reglamento, del Derecho de la Unión y nacional que establezcan el acceso a los datos y autoricen su utilización con fines de investigación científica.

(116) El presente Reglamento no debe afectar a la aplicación de la normativa de competencia, en particular a los artículos 101 y 102 del TFUE. Las disposiciones del presente Reglamento no deben utilizarse para restringir la competencia de forma contraria al TFUE.

(117) Con el fin de permitir a los agentes incluidos en el ámbito de aplicación del presente Reglamento adaptarse a las nuevas normas previstas en él y para adoptar las disposiciones técnicas necesarias, dichas normas deben ser aplicables a partir del 12 de septiembre de 2025.

(118) 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, apartados 1 y 2, del Reglamento (UE) 2018/1725, emitieron su dictamen el 4 de mayo de 2022.

(119) Dado que los objetivos del presente Reglamento, a saber, garantizar la equidad en la asignación del valor de los datos entre los agentes de la economía de los datos y fomentar el acceso equitativo a los datos y su utilización para contribuir al establecimiento de un verdadero mercado interior de datos, no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, debido a las dimensiones o a los efectos de la acción y a la utilización transfronteriza de los datos, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dichos objetivos.

([38]) DO L 123 de 12.5.2016, p. 1.

([39]) 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 lo siguiente, entre otros:

a) la puesta a disposición de datos de productos y de datos de servicios relacionados en favor de los usuarios del producto conectado o servicio relacionado;

b) la puesta a disposición de datos por parte de los titulares de datos en favor de los destinatarios de datos;

c) la puesta a disposición de datos por parte de los titulares de datos en favor de los organismos del sector público, la Comisión, el Banco Central Europeo y los organismos de la Unión, cuando exista una necesidad excepcional de disponer de dichos datos para el desempeño de alguna tarea específica realizada en interés público;

d) la facilitación del cambio entre servicios de tratamiento de datos;

e) la introducción de salvaguardias contra el acceso ilícito de terceros a los datos no personales, y

f) el desarrollo de normas de interoperabilidad para el acceso, la transferencia y la utilización de datos.

2. El presente Reglamento es aplicable a los datos personales y no personales, incluidos los siguientes tipos de datos, en los contextos siguientes:

a) el capítulo II se aplica a los datos, excepto el contenido, relativos al rendimiento, uso y entorno de los productos conectados y los servicios relacionados;

b) el capítulo III se aplica a cualquier dato del sector privado que sea objeto de obligaciones legales de intercambio de datos;

c) el capítulo IV se aplica a cualquier dato del sector privado al que se acceda y que se utilice sobre la base de contratos entre empresas;

d) el capítulo V se aplica a cualquier dato del sector privado, centrándose en los datos no personales;

e) el capítulo VI se aplica a cualquier dato y servicio tratado por los proveedores de servicios de tratamiento de datos;

f) el capítulo VII se aplica a cualquier dato no personal que se encuentre en la Unión por los proveedores de servicios de tratamiento de datos.

3. El presente Reglamento se aplica a:

a) los fabricantes de productos conectados introducidos en el mercado de la Unión y los proveedores de servicios relacionados, independientemente del lugar de establecimiento de dichos fabricantes y proveedores;

b) los usuarios de la Unión de los productos conectados o servicios relacionados a que se refiere la letra a);

c) los titulares de datos, con independencia de su lugar de establecimiento, que pongan datos a disposición de los destinatarios de datos de la Unión;

d) los destinatarios de datos de la Unión a cuya disposición se ponen datos;

e) los organismos del sector público, la Comisión, el Banco Central Europeo o los organismos de la Unión que soliciten a los titulares de datos que pongan datos a su disposición cuando exista una necesidad excepcional de dichos datos para el desempeño de alguna tarea específica realizada en interés público, y a los titulares de datos que proporcionen esos datos en respuesta a dicha solicitud;

f) los proveedores de servicios de tratamiento de datos, con independencia de su lugar de establecimiento, que presten dichos servicios a clientes de la Unión;

g) los participantes en espacios de datos y proveedores de aplicaciones que utilicen contratos inteligentes y personas cuya actividad comercial, empresarial o profesional implique el despliegue de contratos inteligentes para terceros en el contexto de la ejecución de un acuerdo.

4. Cuando el presente Reglamento se refiera a productos conectados o servicios relacionados, se entenderá que incluyen también los asistentes virtuales, en la medida en que interactúen con un producto conectado o servicio relacionado.

5. El presente Reglamento se entenderá sin perjuicio del Derecho de la Unión ni del Derecho nacional en materia de protección de datos personales, de la intimidad y de la confidencialidad de las comunicaciones e integridad de los equipos terminales, que se aplicará a los datos personales tratados en relación con los derechos y obligaciones establecidos en el presente Reglamento, en particular, los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva 2002/58/CE, incluidos los poderes y competencias de las autoridades de control y de los derechos de los interesados. En la medida en que los usuarios tengan la condición de interesados, los derechos establecidos en el capítulo II del presente Reglamento complementarán el derecho de acceso de los interesados y los derechos a la portabilidad de los datos con arreglo a los artículos 15 y 20 del Reglamento (UE) 2016/679. En caso de conflicto entre el presente Reglamento y el Derecho de la Unión en materia de protección de datos personales o de la intimidad, o la normativa nacional adoptada de conformidad con el Derecho de la Unión en la materia, prevalecerá el Derecho aplicable de la Unión o nacional en materia de protección de datos personales o de la intimidad.

6. El presente Reglamento no se aplica a los acuerdos voluntarios celebrados con vistas al intercambio de datos entre entidades privadas y públicas, en particular a los acuerdos voluntarios para el intercambio de datos, ni los condiciona.

El presente Reglamento no afecta a los actos jurídicos de la Unión o 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, o a efectos aduaneros y fiscales, en particular, los Reglamentos (UE) 2021/784, (UE) 2022/2065 y (UE) 2023/1543, y la Directiva (UE) 2023/1544, ni a la cooperación internacional en dicho ámbito. El presente Reglamento no se aplica a la recogida, intercambio, acceso o utilización de datos en virtud del Reglamento (UE) 2015/847 y de la Directiva (UE) 2015/849. El presente Reglamento no se aplica a los ámbitos que queden fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, no afecta a las competencias de los Estados miembros relativas a la seguridad pública, la defensa o la seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan confiado el desempeño de tareas en relación con dichas competencias, o de su facultad para salvaguardar otras funciones esenciales del Estado, incluida la garantía de la integridad territorial del Estado y el mantenimiento del orden público. El presente Reglamento no afecta a las competencias de los Estados miembros en materia de aduanas y administración fiscal, ni a la salud y seguridad ciudadanas.

7. El presente Reglamento complementa el enfoque de autorregulación del Reglamento (UE) 2018/1807 mediante la introducción de obligaciones de aplicabilidad general sobre el cambio de nube.

8. El presente Reglamento se entiende sin perjuicio de los actos jurídicos nacionales y de la Unión por los que se establece la protección de los derechos de propiedad intelectual, en particular, las Directivas 2001/29/CE, 2004/48/CE y (UE) 2019/790.

9. El presente Reglamento complementa y se entiende sin perjuicio del Derecho de la Unión con objeto de 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, las Directivas 93/13/CEE, 2005/29/CE y 2011/83/UE.

10. El presente Reglamento no impide la celebración de contratos lícitos voluntarios de intercambio de datos, incluidos los contratos celebrados sobre la base de la reciprocidad, que cumplan los requisitos establecidos en el presente Reglamento.

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) «metadatos»: una descripción estructurada del contenido o de la utilización de los datos que facilita la búsqueda o la utilización de esos datos;

3) «datos personales»: los datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

4) «datos no personales»: aquellos que no sean datos personales;

5) «producto conectado»: un bien que obtiene, genera, o recoge datos relativos a su uso o entorno y que puede comunicar datos del producto a través de un servicio de comunicaciones electrónicas, una conexión física o un acceso en el dispositivo y cuya función primaria no es el almacenamiento, el tratamiento ni la transmisión de datos en nombre de alguien que no sea el usuario;

6) «servicio relacionado»: un servicio digital, distinto de un servicio de comunicaciones electrónicas, incluido el software, que está conectado con el producto en el momento de la compraventa, el alquiler o el arrendamiento, de tal manera que su ausencia impediría al producto conectado realizar una o varias de sus funciones, o que el fabricante o un tercero conecta posteriormente al producto para añadir, actualizar o adaptar las funciones del producto conectado;

7) «tratamiento»: toda operación o conjunto de operaciones realizadas sobre datos o conjuntos de datos, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, divulgación por transmisión, difusión o cualquier otro medio de puesta a disposición, cotejo o interconexión, limitación, supresión o destrucción;

8) «servicio de tratamiento de datos»: servicio digital que se presta a un cliente y que permite un acceso de red ubicuo y bajo demanda a un conjunto compartido de recursos informáticos configurables, modulables y elásticos de carácter centralizado, distribuido o muy distribuido, que puede movilizarse y liberarse rápidamente con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios;

9) «mismo tipo de servicio»: un conjunto de servicios de tratamiento de datos que comparten el mismo objetivo primario, modelo de servicio de tratamiento de datos y funcionalidades principales;

10) «servicio de intermediación de datos»: un servicio de intermediación de datos tal como se define en el artículo 2, punto 11, del Reglamento (UE) 2022/868;

11) «interesado»: el interesado tal como se indica en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

12) «usuario»: una persona física o jurídica que posee un producto conectado o a la que se le han transferido por contrato derechos temporales de uso de dicho producto conectado, o que recibe servicios relacionados;

13) «titular de datos»: una persona física o jurídica que tiene el derecho o la obligación, con arreglo al presente Reglamento, al Derecho de la Unión aplicable o a la normativa nacional adoptada de conformidad con el Derecho de la Unión, de utilizar y poner a disposición datos, incluidos, cuando se haya pactado contractualmente, los datos del producto o los datos de servicios relacionados que haya extraído o generado durante la prestación de un servicio relacionado;

14) «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 conectado 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 normativa nacional adoptada de conformidad con el Derecho de la Unión;

15) «datos del producto»: datos generados por el uso de un producto conectado que el fabricante ha diseñado para que puedan ser extraídos, a través de un servicio de comunicaciones electrónicas, una conexión física o un acceso en el dispositivo, por un usuario, un titular de los datos o un tercero, incluido, cuando proceda, el fabricante;

16) «datos de servicios relacionados»: datos que representan la digitalización de acciones del usuario o de eventos relacionados con el producto conectado, registrados intencionadamente por el usuario o generados como subproducto de la acción del usuario durante la prestación de un servicio relacionado por el proveedor;

17) «datos fácilmente disponibles»: datos del producto y datos del servicio relacionado que un titular de datos obtiene o puede obtener lícitamente del producto conectado o servicio relacionado, sin un esfuerzo desproporcionado que vaya más allá de una operación simple;

18) «secreto comercial»: un secreto comercial tal como se define en el artículo 2, punto 1, de la Directiva (UE) 2016/943;

19) «poseedor de un secreto comercial»: poseedor de un secreto comercial tal como se define en el artículo 2, punto 2, de la Directiva (UE) 2016/943;

20) «elaboración de perfiles»: la elaboración de perfiles tal como se define en el artículo 4, punto 4, del Reglamento (UE) 2016/679;

21) «comercialización»: todo suministro de un producto conectado para su distribución, consumo o utilización en el mercado de la Unión en el transcurso de una actividad comercial, ya sea a cambio de pago o a título gratuito;

22) «introducción en el mercado»: la primera comercialización de un producto conectado en el mercado de la Unión;

23) «consumidor»: toda persona física que actúe con fines ajenos a su propia actividad comercial, negocio, oficio o profesión;

24) «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;

25) «pequeña empresa»: una pequeña empresa tal como se define en el artículo 2, apartado 2, del anexo de la Recomendación 2003/361/CE;

26) «microempresa»: una microempresa tal como se define en el artículo 2, apartado 3, del anexo de la Recomendación 2003/361/CE;

27) «organismos de la Unión»: los órganos y organismos de la Unión establecidos en virtud de actos adoptados sobre la base del Tratado de la Unión Europea, del TFUE o del Tratado constitutivo de la Comunidad Europea de la Energía Atómica;

28) «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;

29) «emergencia pública»: una situación excepcional, limitada en el tiempo, como una emergencia de salud pública, una emergencia derivada de catástrofes naturales, una catástrofe grave provocada por el hombre, incluido un incidente grave de ciberseguridad, que afecta negativamente a la población de la Unión, del conjunto o de partes de un Estado miembro, que entraña un riesgo de repercusiones graves y duraderas para las condiciones de vida o la estabilidad económica, la estabilidad financiera o la degradación sustancial e inmediata de los activos económicos de la Unión o del Estado miembro en cuestión, y que se determina o declara oficialmente de conformidad con los procedimientos correspondientes en virtud del Derecho de la Unión o nacional;

30) «cliente»: una persona física o jurídica que ha establecido una relación contractual con un proveedor de servicios de tratamiento de datos con el objetivo de utilizar uno o varios servicios de tratamiento de datos;

31) «asistentes virtuales»: software que puede procesar peticiones, tareas o preguntas, incluidas las basadas en material de audio, material escrito, gestos o movimientos, y que, basándose en dichas peticiones, tareas o preguntas, proporciona acceso a otros servicios o controla las funciones de productos conectados;

32) «activos digitales»: elementos en forma digital, incluidas las aplicaciones, para los que el cliente tiene derecho de uso, independientemente de la relación contractual establecida con el servicio de tratamiento de datos del que el cliente se pretende cambiar;

33) «infraestructura de TIC local»: la infraestructura de TIC y de los recursos informáticos propiedad del cliente, alquilados o arrendados por el cliente, situados en el centro de datos del propio cliente y gestionados por el cliente o por un tercero;

34) «cambio»: el proceso en el que intervienen un proveedor de servicios de tratamiento de datos de origen, un cliente de un servicio de tratamiento de datos y, en su caso, un proveedor de servicios de tratamiento de datos de destino, en el que el cliente de un servicio de tratamiento de datos pasa de utilizar un servicio de tratamiento de datos a otro servicio de tratamiento de datos del mismo tipo de servicio, u otro servicio, ofrecido por un proveedor de servicios de tratamiento de datos diferente, o a una infraestructura de TIC local, incluido mediante la extracción, transformación y carga de datos;

35) «costes de salida de datos»: los costes de transferencia de datos cobrados a los clientes por extraer sus datos a través de la red de la infraestructura de las TIC de un proveedor de servicios de tratamiento de datos a los sistemas de un proveedor diferente o a una infraestructura de TIC local;

36) «costes por cambio»: los costes, excluidos los costes de servicio estándar o la sanciones por resolución anticipada, impuestas por un proveedor de servicios de tratamiento de datos a un cliente por las acciones que le exige el presente Reglamento para cambiar al sistema de un proveedor diferente o a una infraestructura de TIC local, incluidos los costes de salida de datos;

37) «equivalencia funcional»: restablecer, sobre la base de los datos exportables y activos digitales del cliente, un nivel mínimo de funcionalidad en el entorno de un nuevo servicio de tratamiento de datos, del mismo tipo de servicio, después del proceso de cambio, cuando el servicio de tratamiento de datos de destino proporcione un resultado materialmente comparable en respuesta a la misma entrada para características compartidas suministrada al cliente en virtud del contrato;

38) «datos exportables»: a efectos de lo dispuesto en los artículos 23 a 31 y en el artículo 35, los datos de entrada y salida, incluidos los metadatos, directa o indirectamente generados o cogenerados por el uso por parte del cliente del servicio de tratamiento de datos, excluidos cualesquiera activos o datos protegidos por derechos de propiedad intelectual, o que constituyan secretos comerciales, de proveedores de servicios de tratamiento de datos o de terceros;

39) «contrato inteligente»: programa informático utilizado para la ejecución automatizada de un acuerdo o de parte de este, que utiliza una secuencia de registros electrónicos de datos y garantiza su integridad y la exactitud de su orden cronológico;

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

41) «especificación de interoperabilidad abierta»: una especificación técnica en el ámbito de las tecnologías de la información y la comunicación, que está orientada a lograr la interoperabilidad entre servicios de tratamiento de datos;

42) «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;

43) «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 para el usuario los datos de los productos y los datos de servicios relacionados

1. Los productos conectados se diseñarán y fabricarán, y los servicios relacionados se diseñarán y prestarán, de manera tal que los datos de los productos y los datos de servicios relacionados, incluidos los metadatos pertinentes necesarios para interpretar y utilizar dichos datos, sean, por defecto, accesibles con facilidad, con seguridad, gratuitamente, en un formato completo, estructurado, de utilización habitual y de lectura mecánica, y, cuando proceda y sea técnicamente viable, accesibles para el usuario directamente.

2. Antes de celebrar un contrato de compraventa, alquiler o arrendamiento de un producto conectado, el vendedor o arrendador, que puede ser el fabricante, proporcionarán al usuario, como mínimo, la siguiente información, de manera clara y comprensible:

a) el tipo, el formato y el volumen estimado de datos del producto que el producto conectado es capaz de generar;

b) si el producto conectado es capaz de generar datos de forma continua y en tiempo real;

c) si el producto conectado es capaz de almacenar datos en el propio dispositivo o en un servidor remoto, incluido, cuando proceda, el período de conservación previsto;

d) el modo en que el usuario puede acceder a los datos, extraerlos o, en su caso, suprimirlos, incluidos los medios técnicos para hacerlo, así como sus condiciones de utilización y calidad del servicio.

3. Antes de celebrar un contrato de prestación de un servicio relacionado, el proveedor de dicho servicio proporcionará al usuario, como mínimo, la siguiente información, de manera clara y comprensible:

a) el carácter, el volumen estimado y la frecuencia de recopilación de los datos del producto que se espera obtenga el posible titular de datos y, cuando proceda, las modalidades mediante las que el usuario puede acceder a estos datos o extraerlos, incluidas las medidas del posible titular de datos relativas al almacenamiento de los datos y la duración de conservación de estos;

b) el carácter y el volumen estimado de los datos del servicio relacionado que vayan a generarse, así como las modalidades mediante las que el usuario puede acceder a estos datos o extraerlos, incluidas las medidas del posible titular de datos relativas al almacenamiento de los datos y la duración de conservación de estos;

c) si el posible titular de datos prevé utilizar él mismo los datos fácilmente disponibles y los fines para los que se utilizarán dichos datos, y si tiene la intención de permitir que uno o varios terceros utilicen los datos para la finalidad acordada con el usuario;

d) la identidad del posible titular de los datos, como su nombre comercial y la dirección geográfica en la que está establecido y, cuando proceda, de otras partes que efectúen tratamiento de datos;

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

f) el modo en que el usuario puede solicitar que los datos se compartan con un tercero y, cuando proceda, dejar de compartir los datos;

g) el derecho del usuario a presentar una reclamación relativa a cualquier infracción de las disposiciones del presente capítulo ante la autoridad competente designada con arreglo al artículo 37;

h) si un posible titular de datos es el poseedor de secretos comerciales contenidos en los datos a los que se pueda acceder desde el producto conectado o generados durante la prestación de un servicio relacionado y, cuando el posible titular de datos no sea el poseedor del secreto comercial, la identidad del poseedor del secreto comercial;

i) la duración del contrato entre el usuario y el posible titular de datos, así como las cláusulas de resolución unilateral del contrato.

Artículo 4

Derechos y obligaciones de los usuarios y titulares de datos respecto del acceso, utilización y puesta a disposición de los datos de productos y de los datos de servicios relacionados

1. Cuando el usuario no pueda acceder directamente a los datos desde el producto conectado, o del servicio relacionado, los titulares de datos facilitarán al usuario el acceso sin demora indebida a los datos fácilmente disponibles, y los correspondientes metadatos necesarios para interpretar y utilizar dichos datos, con la misma calidad disponible para el titular de datos, con facilidad, con seguridad, gratuitamente y en un formato completo, estructurado, de utilización habitual y de lectura mecánica y, cuando proceda y sea técnicamente viable, 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. Los usuarios y los titulares de datos podrán estipular contractualmente limitaciones o prohibiciones del acceso a los datos, de su utilización o su posterior intercambio, si dicho tratamiento puede socavar los requisitos de seguridad del producto conectado, según lo establecido en el Derecho de la Unión o nacional, dando lugar a un efecto adverso grave para la salud, la seguridad o la protección de las personas físicas. Las autoridades sectoriales podrán proporcionar a los usuarios y a los titulares de datos asesoramiento técnico en ese contexto. Cuando el titular de datos se niegue a compartir datos en virtud del presente artículo, lo notificará a la autoridad competente designada en cumplimiento del artículo 37.

3. Sin perjuicio del derecho del usuario a recurrir, en cualquier fase, ante un órgano jurisdiccional de un Estado miembro, el usuario, en relación con cualquier litigio con el titular de datos relativo a las limitaciones o prohibiciones contractuales a que se refiere el apartado 2, podrá:

a) presentar, de conformidad con el artículo 37, apartado 5, letra b), una reclamación ante la autoridad competente, o

b) convenir con el titular de datos en remitir el asunto a un órgano de resolución de litigios de conformidad con el artículo 10, apartado 1.

4. Los titulares de datos no dificultarán indebidamente el ejercicio de las opciones o los derechos de los usuarios a que se refiere este artículo, también ofreciendo opciones a los usuarios de manera no neutra o neutralizando o mermando la autonomía, la toma de decisiones o las opciones del usuario a través de la estructura, el diseño, la función o el modo de funcionamiento de la interfaz digital de usuario o de una parte de ella.

5. Para verificar si una persona física o jurídica puede tener la consideración de usuario a efectos del apartado 1, un titular de datos no exigirá a dicha persona que proporcione ninguna información más allá de lo necesario. Los titulares de datos no conservarán ninguna información, en particular datos de registro, 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.

6. Los secretos comerciales se preservarán y se revelarán solo cuando el titular de datos y el usuario adopten antes de la revelación todas las medidas necesarias para preservar su confidencialidad, en particular, con respecto a terceros. El titular de datos o, cuando no sean la misma persona, el poseedor de secretos comerciales, identificará los datos protegidos como secretos comerciales, incluso en los metadatos pertinentes, y acordará con el usuario las medidas técnicas y organizativas proporcionadas necesarias para preservar la confidencialidad de los datos compartidos, en particular en relación con terceros, tales como cláusulas contractuales tipo, acuerdos de confidencialidad, protocolos de acceso estrictos, normas técnicas y la aplicación de códigos de conducta.

7. En los casos en que no exista un acuerdo sobre las medidas necesarias a que se refiere el apartado 6, o si el usuario no aplica las medidas acordadas en virtud del apartado 6 o vulnera la confidencialidad de los secretos comerciales, el titular de datos podrá retener o, en su caso, suspender el intercambio de datos identificados como secretos comerciales. La decisión del titular de datos se justificará debidamente y se comunicará por escrito al usuario sin demora indebida. En tales casos, el titular de datos notificará a la autoridad competente designada en cumplimiento del artículo 37 que ha retenido o suspendido el intercambio de datos e indicará qué medidas no se han acordado o aplicado y, en su caso, qué secretos comerciales han visto su confidencialidad comprometida.

8. En circunstancias excepcionales, cuando el titular de datos que sea poseedor de un secreto comercial pueda demostrar que es muy probable que sufra un perjuicio económico grave como consecuencia de la revelación de secretos comerciales, a pesar de las medidas técnicas y organizativas adoptadas por el usuario en cumplimiento del apartado 6 del presente artículo, dicho titular de datos podrá rechazar, según el caso, una solicitud de acceso a los datos específicos en cuestión. Dicha demostración estará debidamente justificada sobre la base de elementos objetivos, en particular la aplicabilidad de la protección de los secretos comerciales en terceros países, la naturaleza y el nivel de confidencialidad de los datos solicitados, así como la singularidad y la novedad del producto conectado, y se presentará por escrito al usuario sin demora indebida. Cuando el titular de datos se niegue a compartir datos con arreglo al presente apartado, lo notificará a la autoridad competente designada en cumplimiento del artículo 37.

9. Sin perjuicio del derecho del usuario a recurrir, en cualquier fase, ante un órgano jurisdiccional de un Estado miembro, un usuario que desee impugnar la decisión del titular de datos de rechazar o de retener o suspender el intercambio de datos de conformidad con los apartados 7 y 8, podrá:

a) presentar, de conformidad con el artículo 37, apartado 5, letra b), una reclamación ante la autoridad competente, que decidirá, sin demora indebida, si se iniciará o reanudará el intercambio de datos y en qué condiciones, o

b) convenir con el titular de datos en remitir el asunto a un órgano de resolución de litigios de conformidad con el artículo 10, apartado 1.

10. El usuario no utilizará los datos obtenidos con arreglo a una solicitud contemplada en el apartado 1 para desarrollar un producto conectado que compita con el producto conectado del que proceden los datos, ni compartirá los datos con un tercero con esa intención, ni utilizará dichos datos para obtener información sobre la situación económica, los activos y los métodos de producción del fabricante o, en su caso, del titular de datos.

11. El usuario no usará medios coercitivos ni abusará de las lagunas de la infraestructura técnica de un titular de datos destinada a proteger los datos, con el fin de obtener acceso a estos.

12. Cuando el usuario no sea el interesado cuyos datos personales se solicitan, el titular de datos pondrá a disposición del usuario los datos personales generados por el uso de un producto conectado o servicio relacionado solo cuando exista una base jurídica válida para el tratamiento con arreglo al artículo 6 del Reglamento (UE) 2016/679 y, en su caso, se cumplan las condiciones del artículo 9 de dicho Reglamento y del artículo 5, apartado 3, de la Directiva 2002/58/CE.

13. Un titular de datos solo utilizará cualquier dato fácilmente disponible que no sea personal sobre la base de un contrato con el usuario. Un titular de datos no utilizará dichos datos para obtener información sobre la situación económica, los activos y los métodos de producción del usuario, ni sobre el uso por parte de este de cualquier otra manera que pueda socavar la posición comercial de dicho usuario en los mercados en los que este opere.

14. Los titulares de datos no pondrán a disposición de terceros los datos no personales del producto, con fines comerciales o no comerciales distintos del cumplimiento de su contrato con el usuario. Cuando proceda, los titulares de datos obligarán contractualmente a los terceros a no compartir los datos recibidos de ellos.

Artículo 5

Derecho del usuario 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 fácilmente disponibles, y los metadatos correspondientes necesarios para interpretar y utilizar dichos datos sin demora indebida, con la misma calidad que esté a disposición del titular de datos, con facilidad, con seguridad, gratuitamente para el usuario, en un formato completo, estructurado, de utilización habitual y de lectura mecánica, y, cuando proceda y sea técnicamente viable, de forma continua y en tiempo real. Los datos se pondrán a disposición por parte del titular de datos al tercero de conformidad con los artículos 8 y 9.

2. El apartado 1 no se aplicará a los datos fácilmente disponibles en el contexto de la experimentación de productos conectados, sustancias o procesos nuevos que aún no se hayan introducido en el mercado, a menos que se permita su uso por un tercero contractualmente.

3. Ninguna empresa designada como guardián de acceso, de conformidad con el artículo 3 del Reglamento (UE) 2022/1925, podrá ser un tercero admisible 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.

4. Para verificar si una persona física o jurídica puede tener la consideración de usuario o de tercero a efectos del apartado 1, no se le exigirá al usuario ni al tercero que proporcione ninguna información más allá de lo necesario. Los titulares de datos no conservarán 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.

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

6. El titular de datos no utilizará ningún dato fácilmente disponible 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 de cualquier otra manera que pueda socavar la posición comercial del tercero en los mercados en los que opera, a menos que el tercero haya dado permiso para tal uso y tenga la posibilidad técnica de retirar con facilidad dicho permiso en cualquier momento.

7. Cuando el usuario no sea el interesado cuyos datos personales se soliciten, los datos personales generados por el uso de un producto conectado o servicio relacionado se pondrán a disposición del tercero por parte del titular de datos solo cuando exista una base jurídica válida para el tratamiento con arreglo al artículo 6 del Reglamento (UE) 2016/679 y, en su caso, se cumplan las condiciones del artículo 9 de dicho Reglamento y del artículo 5, apartado 3, de la Directiva 2002/58/CE.

8. 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.

9. Los secretos comerciales se preservarán y se revelarán a terceros solo en la medida en que dicha revelación sea estrictamente necesaria para cumplir el objetivo convenido entre el usuario y el tercero. El titular de datos o, cuando no sean la misma persona, el poseedor de secretos comerciales, identificará los datos protegidos como secretos comerciales, incluso en los metadatos pertinentes, y acordará con el tercero todas las medidas técnicas y organizativas proporcionadas necesarias para preservar la confidencialidad de los datos compartidos, tales como cláusulas contractuales tipo, acuerdos de confidencialidad, protocolos de acceso estrictos, normas técnicas y la aplicación de códigos de conducta.

10. En los casos en que no exista un acuerdo sobre las medidas necesarias a que se refiere el apartado 9 del presente artículo o si el tercero no aplica las medidas acordadas en virtud del apartado 9 del presente artículo o vulnera la confidencialidad de los secretos comerciales, el titular de datos podrá retener o, en su caso, suspender el intercambio de datos identificados como secretos comerciales. La decisión del titular de datos se justificará debidamente y se comunicará por escrito al tercero sin demora indebida. En tales casos, el titular de datos notificará a la autoridad competente designada en cumplimiento del artículo 37 que ha retenido o suspendido el intercambio de datos e indicará qué medidas no se han convenido o aplicado y, en su caso, qué secretos comerciales han visto su confidencialidad comprometida.

11. En circunstancias excepcionales, cuando el titular de datos que sea poseedor de un secreto comercial pueda demostrar que es muy probable que sufra un perjuicio económico grave como consecuencia de la revelación de secretos comerciales, a pesar de las medidas técnicas y organizativas adoptadas por el tercero en cumplimiento del apartado 9 del presente artículo, dicho titular de datos podrá rechazar, según el caso, una solicitud de acceso a los datos específicos en cuestión. Dicha demostración estará debidamente justificada sobre la base de elementos objetivos, en particular la aplicabilidad de la protección de los secretos comerciales en terceros países, la naturaleza y el nivel de confidencialidad de los datos solicitados y la singularidad y la novedad del producto conectado, y se presentará por escrito al tercero sin demora indebida. Cuando el titular de datos se niegue a compartir datos con arreglo al presente apartado, lo notificará a la autoridad competente designada en cumplimiento del artículo 37.

12. Sin perjuicio del derecho del tercero a recurrir, en cualquier fase, ante un órgano jurisdiccional de un Estado miembro, un tercero que desee impugnar una decisión del titular de datos de rechazar o de retener o suspender el intercambio de datos en virtud de los apartados 10 y 11, podrá:

a) formular, de conformidad con el artículo 37, apartado 5, letra b), una reclamación ante la autoridad competente, que decidirá, sin demora indebida, si se debe iniciar o reanudar el intercambio de datos y en qué condiciones, o

b) convenir con el titular de datos en remitir el asunto a un órgano de resolución de litigios de conformidad con el artículo 10, apartado 1.

13. El derecho a que se refiere el apartado 1 no afectará negativamente a los derechos de los interesados conforme al Derecho aplicable de la Unión y nacional en materia de protección de datos personales.

Artículo 6

Obligaciones de terceros que reciben datos a petición del usuario

1. Un tercero tratará los datos que se pongan a su disposición con arreglo al artículo 5 únicamente para la finalidad y en las condiciones acordados con el usuario y respetando el Derecho de la Unión y nacional en materia de protección de datos personales, incluidos los derechos del interesado en lo que respecta a los datos personales. El tercero suprimirá los datos cuando ya no sean necesarios para la finalidad acordada, a menos que acuerde otra cosa con el usuario en relación con los datos no personales.

2. El tercero no podrá:

a) dificultar indebidamente el ejercicio de las opciones o los derechos de los usuarios con arreglo al artículo 5 y al presente artículo, tampoco ofreciendo opciones a los usuarios de manera no neutra o coaccionándolos, engañándolos o manipulándolos, o neutralizando o mermando la autonomía, la toma de decisiones o las opciones de los usuarios, tampoco a través de una interfaz digital de usuario o de una parte de ella;

b) no obstante lo dispuesto en el artículo 22, apartado 2, letras a) y c), del Reglamento (UE) 2016/679, utilizar los datos que reciba para la elaboración de perfiles, a menos que sea necesario para prestar el servicio solicitado por el usuario;

c) poner los datos que reciba a disposición de otro tercero, a menos que los datos se pongan a disposición sobre la base de un contrato con el usuario, y siempre que el otro tercero tome todas las medidas necesarias acordadas entre el titular de datos y el tercero para preservar la confidencialidad de los secretos comerciales;

d) poner los datos que reciba a disposición de una empresa designada como guardián de acceso de conformidad con el artículo 3 del Reglamento (UE) 2022/1925;

e) utilizar los datos que reciba para desarrollar un producto que compita con el producto conectado del que proceden los datos a los que ha accedido ni compartir los datos con otro tercero con tal finalidad; los terceros tampoco utilizarán datos no personales de los productos o datos no personales de los servicios relacionados que se pongan a su disposición para obtener información sobre la situación económica, los activos y los métodos de producción del titular de datos, ni sobre el uso por este;

f) utilizar los datos que reciba de una manera que afecte negativamente a la seguridad del producto conectado o del servicio relacionado;

g) ignorar las medidas específicas acordadas con un titular de datos o con el poseedor de los secretos comerciales de conformidad con el artículo 5, apartado 9, ni comprometer la confidencialidad de los secretos comerciales;

h) impedir a aquellos usuarios que sean consumidores, entre otros, sobre la base de un contrato, 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 mediante el uso de productos conectados fabricados o diseñados o servicios relacionados prestados por una microempresa o pequeña empresa, siempre que dicha empresa no tenga una empresa asociada o una empresa vinculada en el sentido del artículo 3 del anexo de la Recomendación 2003/361/CE, que no pueda considerarse microempresa o pequeña empresa, y cuando no se haya subcontratado a la microempresa o pequeña empresa para fabricar o diseñar un producto conectado o para prestar un servicio relacionado.

Lo mismo se aplicará a los datos generados mediante el uso de productos conectados fabricados o de servicios relacionados prestados por empresas que hayan adquirido la consideración de medianas empresas con arreglo al artículo 2 del anexo de la Recomendación 2003/361/CE hace menos de un año, y cuando se trate de productos conectados, durante un año después de que una mediana empresa los haya introducido en el mercado.

2. Ninguna cláusula contractual que, en detrimento del usuario, excluya la aplicación de los derechos del usuario en virtud del presente capítulo, establezca excepciones o modifique los efectos de esos derechos, será vinculante para el usuario.

CAPÍTULO III

OBLIGACIONES DE LOS TITULARES DE DATOS OBLIGADOS A PONER LOS DATOS A DISPOSICIÓN EN VIRTUD DEL DERECHO DE LA UNIÓN

Artículo 8

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

1. Cuando, en relaciones entre empresas, un titular de datos esté obligado a poner datos a disposición de un destinatario de datos en virtud del artículo 5 o de otras disposiciones aplicables de Derecho de la Unión o de la normativa nacional adoptada de conformidad con el Derecho de la Unión, acordará con el destinatario de datos las modalidades de puesta a disposición de los datos y lo hará en condiciones justas, razonables y no discriminatorias y de manera transparente de conformidad con el presente capítulo y el capítulo IV.

2. 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 unilateral de obligaciones relativas a datos será vinculante si constituye una cláusula contractual abusiva en el sentido del artículo 13 o si, en detrimento del usuario, excluye la aplicación, establece excepciones o modifica los derechos del usuario en virtud del capítulo II.

3. Los titulares de datos no discriminarán en lo que respecta a las modalidades de puesta a disposición de datos, entre categorías comparables de destinatarios de datos, incluidas las empresas asociadas o empresas vinculadas al titular de datos al poner 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, el titular de los datos proporcionará sin demora indebida al destinatario de datos, previa solicitud motivada, información que demuestre que no ha habido discriminación.

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

5. Los titulares de datos y los destinatarios de datos no estarán obligados a proporcionar ninguna información que vaya más allá de lo necesario para verificar el cumplimiento de las condiciones contractuales pactadas para la puesta a disposición de datos o de sus obligaciones en virtud del presente Reglamento o de otras disposiciones aplicables de Derecho de la Unión o de la normativa nacional adoptada de conformidad con el Derecho de la Unión.

6. Salvo que se disponga otra cosa en el Derecho de la Unión, incluidos el artículo 4, apartado 6, y el artículo 5, apartado 9, del presente Reglamento, o en la normativa nacional adoptada de conformidad con el Derecho de la Unión, la obligación de poner los datos a disposición de un destinatario de datos no obligará a la revelación de secretos comerciales.

Artículo 9

Compensación por la puesta a disposición de datos

1. Toda compensación acordada entre un titular de datos y un destinatario de datos por la puesta a disposición de datos en relaciones entre empresas deberá ser no discriminatoria y razonable, y podrá incluir un margen.

2. A la hora de convenir la compensación, el titular de datos y el destinatario de datos tendrán en cuenta, en particular:

a) los costes en que se haya incurrido para poner los datos a disposición, incluidos, en particular, los costes necesarios para el formateo de los datos, su difusión por medios electrónicos y su almacenamiento;

b) las inversiones en la recogida y producción de datos, cuando proceda, teniendo en cuenta si otras partes han contribuido a la obtención, generación o recogida de los datos en cuestión.

3. La compensación a que se refiere el apartado 1 también puede depender del volumen, el formato y la naturaleza de los datos.

4. Cuando el destinatario de datos sea una pyme o una organización de investigación sin ánimo de lucro, y cuando dicho destinatario de datos no tenga empresas asociadas o empresas vinculadas, que no se consideren pymes, ninguna compensación acordada podrá superar los costes a que se refiere el apartado 2, letra a).

5. La Comisión adoptará directrices sobre el cálculo de la compensación razonable, teniendo en cuenta el asesoramiento del Comité Europeo de Innovación en materia de Datos (CEID) a que se refiere el artículo 42.

6. El presente artículo no será óbice para que otras disposiciones de Derecho de la Unión de normativa nacional adoptada con arreglo al Derecho de la Unión excluyan la compensación por la puesta a disposición de datos o prevean una compensación inferior.

7. El titular de datos proporcionará 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 evaluar si se cumplen los requisitos de los apartados 1 a 4.

Artículo 10

Resolución de litigios

1. Los usuarios, los titulares de datos y los destinatarios de datos tendrán acceso a algún órgano de resolución de litigios, certificado de conformidad con el apartado 5 del presente artículo, para resolver todo litigio con arreglo al artículo 4, apartados 3 y 9, y al artículo 5, apartado 12, así como los litigios relacionados con las condiciones justas, razonables y no discriminatorias para poner los datos a disposición y la forma transparente de hacerlo, de conformidad con el presente capítulo y el capítulo IV.

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

3. En el caso de los litigios remitidos a un órgano de resolución de litigios en virtud del artículo 4, apartados 3 y 9, y del artículo 5, apartado 12, cuando el órgano de resolución de litigios resuelva un litigio en favor del usuario o del destinatario de datos, el titular de datos soportará todas las tasas cobradas por el órgano de resolución de litigios y reembolsará a dicho usuario o dicho destinatario de datos cualquier otro gasto razonable en que haya incurrido en relación con la resolución de litigios. Si el órgano de resolución de litigios resuelve un litigio en favor del titular de datos, el usuario o el destinatario de datos no estará obligado a reembolsar las tasas u otros gastos que el titular de datos haya pagado o deba pagar en relación con la resolución de litigios, a menos que el órgano de resolución de litigios considere que el usuario o el destinatario de los datos actuó manifiestamente de mala fe.

4. Los clientes y los proveedores de servicios de tratamiento de datos tendrán acceso a algún órgano de resolución de litigios, certificado de conformidad con el apartado 5 del presente artículo, para resolver litigios en relación con vulneraciones de los derechos de los clientes e incumplimientos de las obligaciones del proveedor de un servicio de tratamiento de datos de conformidad con los artículos 23 a 31.

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

a) es imparcial e independiente, y debe dictar sus resoluciones con arreglo a unas normas de procedimiento claras, no discriminatorias y justas;

b) dispone de los conocimientos técnicos necesarios, en particular, en relación con las condiciones justas, razonables y no discriminatorias, incluida la compensación, relativos a la puesta a disposición de datos de manera transparente, que permitan 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 al menos en una de las lenguas oficiales de la Unión.

6. Los Estados miembros notificarán a la Comisión los órganos de resolución de litigios certificados de conformidad con el apartado 5. La Comisión publicará la lista de dichos órganos en un sitio web específico y la mantendrá actualizada.

7. 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.

8. Los órganos de resolución de litigios brindarán a las partes la posibilidad de expresar, en un plazo razonable, sus puntos de vista sobre los asuntos que esas partes hayan sometido a dichos órganos. En ese contexto, se proporcionará a cada una de las partes litigantes las observaciones de la otra parte y cualquier declaración realizada por peritos. Se brindará a las partes la posibilidad de formular comentarios sobre dichas observaciones y declaraciones.

9. Los órganos de resolución de litigios adoptarán su decisión sobre los asuntos que les sean planteados en un plazo de noventa días a partir de la recepción de la solicitud con arreglo a los apartados 1 y 4. Dicha decisión se formulará por escrito o en un soporte duradero e irá justificada por una exposición de motivos.

10. Los órganos de resolución de litigios elaborarán y harán públicos los informes anuales de actividad. Dichos informes anuales incluirán, en particular, la siguiente información general:

a) una agregación de los resultados de los litigios;

b) la duración media de la resolución de los litigios;

c) los motivos más comunes de los litigios.

11. Con el fin de facilitar el intercambio de información y las mejores prácticas, los órganos de resolución de litigios podrán decidir la inclusión de recomendaciones en el informe mencionado en el apartado 10 sobre cómo evitar o resolver problemas.

12. La decisión de los órganos de resolución de litigios será vinculante para las partes solo si estas han dado su consentimiento expreso a su carácter vinculante antes del inicio del procedimiento de resolución de litigios.

13. El presente artículo no afectará al derecho de las partes a interponer un recurso efectivo ante los órganos jurisdiccionales de los Estados miembros.

Artículo 11

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

1. El titular de datos podrá aplicar medidas técnicas de protección adecuadas, incluidos contratos inteligentes y cifrado, para impedir el acceso no autorizado a los datos, incluidos los metadatos, y garantizar el cumplimiento de los artículos 4, 5, 6, 8 y 9, así como de las condiciones contractuales acordadas para la puesta a disposición de los datos. Dichas medidas técnicas de protección no discriminarán entre destinatarios de datos ni obstaculizarán el derecho de un usuario a obtener una copia, extraer, utilizar o acceder a los datos o a proporcionar datos a terceros de conformidad con el artículo 5 ni ningún derecho de un tercero en virtud del Derecho de la Unión o de normativa nacional adoptada de conformidad con el Derecho de la Unión. Los usuarios, los terceros y los destinatarios de datos no modificarán ni suprimirán dichas medidas técnicas de protección a menos que el titular de datos acepte.

2. En las circunstancias a que se refiere el apartado 3, el tercero o el destinatario de datos atenderá, sin demora indebida, las solicitudes del titular de datos y, en su caso, del poseedor de un secreto comercial cuando no sea la misma persona, o del usuario para:

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

b) poner fin a la producción, oferta o comercialización o utilización de bienes, datos derivados o servicios producidos sobre la base de conocimientos obtenidos a través de dichos datos, o la importación, exportación o almacenamiento de mercancías infractoras con esos fines, y destruir cualquier mercancía infractora, cuando exista un riesgo grave de que la utilización ilícita de dichos datos cause un perjuicio significativo al titular de datos, al poseedor de un secreto comercial o al usuario, o cuando dicha medida no fuese desproporcionada a la luz de los intereses del titular de datos, del poseedor de un secreto comercial o del usuario;

c) informar al usuario de la utilización o divulgación no autorizadas de los datos y de las medidas adoptadas para poner fin a la utilización o divulgación no autorizadas de los datos;

d) compensar a la parte que sufra la utilización indebida o la divulgación de dichos datos a los que se haya accedido o utilizado de forma ilícita.

3. El apartado 2 se aplicará cuando un tercero o un destinatario de datos:

a) con el fin de obtener datos haya proporcionado a un titular de datos información falsa, haya utilizado medios engañosos o coercitivos o haya abusado de las lagunas en la infraestructura técnica del titular de datos destinada a proteger los datos;

b) haya utilizado los datos puestos a disposición con fines no autorizados, incluido el desarrollo de un producto conectado competidor en el sentido del artículo 6, apartado 2, letra e);

c) haya divulgado ilícitamente datos a otro tercero;

d) no haya mantenido las medidas técnicas y organizativas acordadas en virtud del artículo 5, apartado 9, o

e) haya modificado o eliminado medidas técnicas de protección aplicadas por el titular de datos en virtud del apartado 1 del presente artículo sin el consentimiento del titular de datos.

4. El apartado 2 también será aplicable cuando el usuario altere o elimine las medidas técnicas de protección aplicadas por el titular de datos o no mantenga las medidas técnicas y organizativas adoptadas por el usuario de acuerdo con el titular de datos o, cuando no sean la misma persona, el poseedor de un secreto comercial, con el fin de preservar secretos comerciales, así como respecto de cualquier otra persona que reciba los datos por parte del usuario en infracción del presente Reglamento.

5. Cuando el destinatario de los datos infrinja el artículo 6, apartado 2, letras a) o b), los usuarios tendrán los mismos derechos que los titulares de datos en virtud del apartado 2 del presente artículo.

Artículo 12

Ámbito de aplicación de las obligaciones de los titulares de datos obligados por el Derecho de la Unión a poner los datos a disposición

1. El presente capítulo se aplicará cuando, en las relaciones entre empresas, el titular de datos esté obligado, en virtud del artículo 5 o en virtud del Derecho de la Unión aplicable o de normativa nacional adoptada de conformidad con el 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 a este o modifique sus efectos, será vinculante para esa parte.

CAPÍTULO IV

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

Artículo 13

Cláusulas contractuales abusivas impuestas unilateralmente a otra empresa

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 unilateral de obligaciones relativas a datos que hayan sido impuestas unilateralmente por una empresa a otra empresa no serán vinculantes en caso de ser abusivas.

2. No se considerará abusiva una cláusula contractual que refleje disposiciones imperativas del Derecho de la Unión o disposiciones del Derecho de la Unión que se aplicarían si las cláusulas contractuales no regularan la materia.

3. 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, contrariamente a la buena fe y a la lealtad de las relaciones comerciales.

4. En particular, a los efectos del apartado 3, una cláusula contractual tendrá la consideración de 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 proporcionados son acordes con el contrato o de interpretar cualquier cláusula contractual.

5. A los efectos del apartado 3, 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 responsabilidad en caso de incumplimiento de dichas obligaciones, o ampliar la responsabilidad de la empresa a la que se haya impuesto unilateralmente la cláusula;

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, en particular cuando esos datos contengan datos sensibles desde el punto de vista comercial o estén protegidos por secretos comerciales o derechos de propiedad intelectual;

c) impedir a la parte a la que se haya impuesto unilateralmente la cláusula utilizar los datos que haya proporcionado 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 adecuada;

d) impedir que la parte a la que se haya impuesto unilateralmente la cláusula resuelva unilateralmente el contrato en un plazo razonable;

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

f) permitir a la parte que haya impuesto unilateralmente la cláusula resolver unilateralmente el contrato con un plazo de preaviso excesivamente corto, habida cuenta de cualquier posibilidad razonable 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;

g) permitir que la parte que haya impuesto unilateralmente la cláusula modifique sustancialmente el precio especificado en el contrato o cualquier otra condición sustantiva relativa a la naturaleza, el formato, la calidad o la cantidad de los datos que deban compartirse, cuando el contrato no especifique ninguna razón válida ni derecho de la otra parte para resolver unilateralmente el contrato en caso de efectuarse tal modificación.

La letra g) del presente apartado no afectará a las cláusulas en virtud de las cuales la parte que haya impuesto unilateralmente la cláusula se reserva el derecho de modificar unilateralmente las cláusulas de un contrato de duración indeterminada, siempre que el contrato especificase alguna razón válida para efectuar dicha modificación unilateral, que la parte que haya impuesto unilateralmente la cláusula esté obligada a proporcionar a la otra parte contratante un preaviso razonable para efectuar la modificación planeada y que la otra parte contratante tenga libertad para resolver unilateralmente el contrato sin coste alguno en caso de que se produzca tal modificación.

6. 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 la cláusula contractual demostrar que no ha sido impuesta unilateralmente. La parte contratante que haya aportado la cláusula contractual controvertida no podrá alegar que se trata de una cláusula contractual abusiva.

7. En caso de que la cláusula contractual abusiva sea disociable de las demás cláusulas del contrato, estas serán vinculantes.

8. El presente artículo no se aplicará a las cláusulas comerciales del objeto principal del contrato ni a la adecuación del precio, con respecto a los datos suministrados a cambio.

9. Las partes de un contrato que entre en el ámbito de aplicación del apartado 1 no excluirán la aplicación del presente artículo, ni establecerán excepciones a este ni modificarán sus efectos.

CAPÍTULO V

PONER DATOS A DISPOSICIÓN DE LOS ORGANISMOS DEL SECTOR PÚBLICO, LA COMISIÓN, EL BANCO CENTRAL EUROPEO Y LOS ORGANISMOS DE LA UNIÓN EN RAZÓN DE NECESIDADES EXCEPCIONALES

Artículo 14

Obligación de poner a disposición datos en razón de una necesidad excepcional

Cuando un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión demuestre una necesidad excepcional, tal como figura en el artículo 15, de utilizar determinados datos, incluidos los metadatos pertinentes necesarios para interpretar y utilizar dichos datos, para desarrollar sus funciones estatutarias en interés público, los titulares de datos que sean personas jurídicas, distintos de organismos del sector público, que posean dichos datos los pondrán a disposición previa solicitud debidamente motivada.

Artículo 15

Necesidad excepcional de utilizar los datos

1. Una necesidad excepcional de utilizar determinados datos en el sentido del presente capítulo estará limitada en el tiempo y en su ámbito de aplicación y se considerará que existe únicamente en cualquiera de las circunstancias siguientes:

a) cuando los datos solicitados sean necesarios para responder a una emergencia pública y el organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión no pueda obtener dichos datos por medios alternativos de manera oportuna y efectiva en condiciones equivalentes;

b) en circunstancias no contempladas en la letra a) y únicamente en lo que respecta a los datos no personales, cuando:

   i) un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión actúe sobre la base del Derecho de la Unión o nacional y haya identificado datos específicos cuya ausencia le impida desempeñar una tarea específica realizada en interés público, que haya sido expresamente prevista por la ley, como la elaboración de estadísticas oficiales o la mitigación de una emergencia pública o recuperación tras dicha emergencia, y

   ii) el organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión haya agotado todos los demás medios a su disposición para obtener dichos datos, incluida la compra de datos no personales en el mercado ofreciendo precios de mercado, o basándose en obligaciones existentes de poner datos a disposición o la adopción de nuevas medidas legislativas que puedan garantizar la disponibilidad de los datos en tiempo oportuno.

2. El apartado 1, letra b), no se aplicará a las microempresas ni a las pequeñas empresas.

3. La obligación de demostrar que el organismo del sector público no ha podido obtener datos no personales comprándolos en el mercado no se aplicará cuando la tarea específica desempeñada en interés público sea la elaboración de estadísticas oficiales y cuando el Derecho nacional no permita la compra de dichos datos.

Artículo 16

Relación con otras obligaciones de poner datos a disposición de los organismos del sector público, la Comisión, el Banco Central Europeo y los 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, de dar cumplimiento a las solicitudes de acceso a información o de la demostración o verificación del cumplimiento de obligaciones legales.

2. El presente capítulo no se aplicará a los organismos del sector público, a la Comisión, al Banco Central Europeo ni a los organismos de la Unión que efectúen actividades con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o administrativas o de ejecución de sanciones penales, ni a la administración aduanera o tributaria. El presente capítulo no afecta al Derecho aplicable de la Unión y nacional 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, la Comisión, el Banco Central Europeo o un organismo de la Unión solicite datos con arreglo al artículo 14, deberá:

a) especificar qué datos son necesarios, incluidos los metadatos pertinentes necesarios para interpretarlos y utilizarlos;

b) demostrar que se cumplen las condiciones necesarias para la existencia de una necesidad excepcional a que se refiere el artículo 15 para la que se solicitan los datos;

c) explicar la finalidad de la solicitud, la utilización prevista de los datos solicitados, incluso, cuando proceda, por un tercero de conformidad con el apartado 4 del presente artículo, la duración de dicha utilización y, en su caso, la forma en que el tratamiento de los datos personales responde a la necesidad excepcional;

d) especificar, siempre que sea posible, cuándo se prevé que los datos sean suprimidos por todas las partes que tengan acceso a ellos;

e) justificar la elección del titular de datos al que se dirige la solicitud;

f) especificar todos los demás organismos del sector público o la Comisión, el Banco Central Europeo o los organismos de la Unión y los terceros con los que se prevea compartir los datos solicitados;

g) cuando se soliciten datos personales, especificar cualquier medida técnica y organizativa necesaria y proporcionada para aplicar los principios de protección de datos y las garantías necesarias, como la seudonimización, y si el titular de los datos puede aplicar la anonimización antes de poner los datos a disposición;

h) indicar la disposición legal por la que se asigna al organismo del sector público solicitante, a la Comisión, al Banco Central Europeo o a los organismos de la Unión la tarea específica desempeñada en interés público pertinente para solicitar los datos;

i) especificar el plazo en que deben ponerse los datos a disposición y el plazo a que se refiere el artículo 18, apartado 2, en que el titular de datos puede denegar o pedir la modificación de la solicitud;

j) hacer todo lo posible por evitar que el cumplimiento de la solicitud de datos dé lugar a la responsabilidad de los titulares de datos por infracción del Derecho de la Unión o nacional.

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

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

b) ser específica por lo que respecta al tipo de datos solicitados y corresponder a datos que el titular de datos controle en el momento de la solicitud;

c) guardar proporción con la necesidad excepcional y estar debidamente motivada, por lo que respecta a la granularidad y el volumen de los datos solicitados y la frecuencia de acceso a los datos solicitados;

d) respetar los objetivos legítimos del titular de datos, con el compromiso de garantizar la protección de los secretos comerciales de conformidad con el artículo 19, apartado 3, y habida cuenta del coste y el esfuerzo necesarios para poner los datos a disposición;

e) referirse a datos no personales y, sólo si se demuestra que ello es insuficiente para responder a la necesidad excepcional de utilizar datos, de conformidad con el artículo 15, apartado 1, letra a), solicitar datos personales en forma seudonimizada y establecer las medidas técnicas y organizativas que se vayan a adoptar para proteger los datos;

f) informar al titular de datos de las sanciones que impondrá de conformidad con el artículo 40 la autoridad competente designada en cumplimiento del artículo 37 en caso de que no se atienda la solicitud;

g) cuando la solicitud proceda de un organismo del sector público, transmitirse al coordinador de datos a que se refiere el artículo 37 del Estado miembro en el que esté establecido el organismo del sector público solicitante, que la hará pública en línea sin demora indebida, a menos que el coordinador de datos considere que dicha publicación podría crear un riesgo para la seguridad pública;

h) cuando la solicitud proceda de la Comisión, el Banco Central Europeo o los organismos de la Unión, ponerse a disposición en línea sin demora indebida;

i) cuando se soliciten datos personales, notificarse sin demora indebida a la autoridad de control responsable de supervisar la aplicación del Reglamento (UE) 2016/679 en el Estado miembro en el que esté establecido el organismo del sector público.

El Banco Central Europeo y los organismos de la Unión informarán a la Comisión de sus solicitudes.

3. Un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión no pondrá los datos obtenidos de conformidad con el presente capítulo a disposición para su reutilización tal como se define en el artículo 2, punto 2, del Reglamento (UE) 2022/868 o en el artículo 2, punto 11, de la Directiva (UE) 2019/1024. El Reglamento (UE) 2022/868 y la Directiva (UE) 2019/1024 no se aplicarán a aquellos datos en poder de organismos del sector público que se obtengan de conformidad con el presente capítulo.

4. Lo dispuesto en el apartado 3 del presente artículo no impedirá a un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión intercambiar los datos obtenidos con arreglo al presente capítulo con otro organismo del sector público o la Comisión, el Banco Central Europeo o un organismo de la Unión con el fin de completar las tareas a que se refiere el artículo 15, tal como se especifica en la solicitud con arreglo al apartado 1, letra f), del presente artículo, ni poner los datos a disposición de un tercero en los casos en que se haya delegado en ese tercero, mediante un acuerdo disponible al público, la realización de inspecciones técnicas u otras funciones. Las obligaciones de los organismos del sector público con arreglo al artículo 19, en particular, las garantías para preservar la confidencialidad de los secretos comerciales, se aplicarán también a dichos terceros. Cuando un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión transmita o ponga a disposición datos en aplicación del presente apartado, lo notificará al titular de datos del que haya recibido los datos sin demora indebida.

5. Cuando el titular de datos considere que sus derechos en virtud del presente capítulo han sido vulnerados por la transmisión o puesta a disposición de datos, podrá presentar una reclamación ante la autoridad competente designada en cumplimiento del artículo 37 del Estado miembro en el que esté establecido el titular de datos.

6. La Comisión elaborará un modelo para las solicitudes con arreglo al presente artículo.

Artículo 18

Cumplimiento de las solicitudes de datos

1. Cuando un titular de datos reciba una solicitud de puesta a disposición de datos con arreglo al presente capítulo, pondrá los datos a disposición del organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión solicitante sin demora indebida, teniendo en cuenta las medidas técnicas, organizativas y jurídicas necesarias.

2. Sin perjuicio de las necesidades específicas relativas a la disponibilidad de datos definidas en el Derecho de la Unión o nacional, el titular de datos podrá denegar o solicitar la modificación de una solicitud de poner a disposición los datos con arreglo al presente capítulo sin demora indebida y, en cualquier caso, a más tardar cinco días hábiles después de la recepción de una solicitud de los datos necesarios para responder a una emergencia pública y sin demora indebida y, en cualquier caso, a más tardar treinta días hábiles después de la recepción de dicha solicitud en otros casos de necesidad excepcional, por cualquiera de los motivos siguientes:

a) que el titular de datos no tenga control sobre los datos solicitados;

b) que otro organismo del sector público o la Comisión, el Banco Central Europeo o un organismo de la Unión haya presentado previamente una solicitud similar para el mismo fin y no se haya notificado la supresión de los datos al titular de los datos de conformidad con el artículo 19, apartado 1, letra c);

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

3. En caso de que el titular de datos decida denegar la solicitud o pedir su modificación de conformidad con el apartado 2, letra b), indicará la identidad del organismo del sector público o la Comisión, el Banco Central Europeo o el organismo de la Unión que haya presentado previamente una solicitud con la misma finalidad.

4. Cuando los datos solicitados incluyan datos personales, el titular de datos anonimizará adecuadamente los datos, a menos que el cumplimiento de la solicitud de poner datos a disposición de un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión exija la divulgación de datos personales. En tales casos, el titular de datos seudonimizará los datos.

5. Cuando el organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión desee impugnar la negativa de un titular de datos a proporcionar los datos solicitados, o cuando el titular de datos desee impugnar la solicitud y el asunto no pueda resolverse mediante una modificación adecuada de la solicitud, el asunto se someterá a la autoridad competente designada en cumplimiento del artículo 37 del Estado miembro en el que esté establecido el titular de datos.

Artículo 19

Obligaciones de los organismos del sector público, la Comisión, el Banco Central Europeo y los organismos de la Unión

1. Un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión que reciba datos de conformidad con 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) habrá aplicado medidas técnicas y organizativas que preserven la confidencialidad y la integridad de los datos solicitados y la seguridad de las transferencias de datos, en particular los datos personales, y garanticen los derechos y libertades de los interesados;

c) suprimirá los datos en cuanto dejen de ser necesarios para la finalidad declarada e informará sin demora indebida al titular de datos y a las personas u organizaciones que hayan recibido los datos de conformidad con el artículo 21, apartado 1, de que los datos han sido suprimidos, a menos que el archivo de los datos sea necesario de conformidad con el Derecho de la Unión o nacional sobre acceso público a los documentos en el contexto de las obligaciones de transparencia.

2. El organismo del sector público, la Comisión, el Banco Central Europeo, el organismo de la Unión o el tercero que reciba datos con arreglo al presente capítulo no podrá:

a) utilizar los datos o las ideas sobre la situación económica, los activos y los métodos de producción o funcionamiento del titular de datos para desarrollar o mejorar un producto conectado o servicio relacionado que compita con el producto conectado o servicio relacionado del titular de datos;

b) compartir los datos con otro tercero para cualquiera de los fines a que se refiere la letra a).

3. La revelación de secretos comerciales a un organismo del sector público, a la Comisión, al Banco Central Europeo o a un organismo de la Unión se exigirá solo en la medida en que sea estrictamente necesario para cumplir la finalidad de una solicitud en virtud del artículo 15. En tal caso, el titular de datos o, si no se trata de la misma persona, el poseedor del secreto comercial, identificará los datos protegidos como secretos comerciales, también en los metadatos pertinentes. El organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión adoptarán, antes de la revelación de los secretos comerciales, todas las medidas técnicas y organizativas necesarias y adecuadas para preservar la confidencialidad de los secretos comerciales, incluido, en su caso, el uso de cláusulas contractuales tipo, normas técnicas y la aplicación de códigos de conducta.

4. Un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión será responsable de la seguridad de los datos que reciba.

Artículo 20

Compensación en caso de necesidad excepcional

1. Los titulares de datos distintos de las microempresas y pequeñas empresas pondrán a disposición de forma gratuita los datos necesarios para responder a una emergencia pública con arreglo al artículo 15, apartado 1, letra a). El organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión que haya recibido los datos dará reconocimiento público al titular de datos si este así lo solicita.

2. El titular de datos tendrá derecho a una compensación justa por poner a disposición datos en cumplimiento de una solicitud presentada con arreglo al artículo 15, apartado 1, letra b). Tal compensación cubrirá los costes técnicos y organizativos soportados para dar cumplimiento a la solicitud, incluidos, en su caso, los costes de anonimización, seudonimización, agregación y de adaptación técnica, más un margen razonable. A petición del organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión, el titular de datos proporcionará información sobre la base de cálculo de los costes y del margen razonable.

3. El apartado 2 también será de aplicación cuando una microempresa y pequeña empresa exija una compensación por poner a disposición los datos.

4. Los titulares de datos no tendrán derecho a una compensación por la puesta de datos a disposición en cumplimiento de una solicitud realizada con arreglo al artículo 15, apartado 1, letra b), cuando la tarea específica desempeñada en interés público sea la elaboración de estadísticas oficiales y el Derecho nacional no permita la compra de datos. Los Estados miembros notificarán a la Comisión los casos en que el Derecho nacional no permita la compra de datos para la elaboración de estadísticas oficiales.

5. Cuando el organismo del sector público, la Comisión, el Banco Central Europeo o el organismo de la Unión no acepte el nivel de compensación solicitado por el titular de datos, podrá presentar una reclamación ante la autoridad competente designada en cumplimiento del artículo 37 del Estado miembro en el que esté establecido el titular de datos.

Artículo 21

Intercambio de datos con organizaciones de investigación u organismos estadísticos, obtenidos en el contexto de alguna necesidad excepcional

1. Un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión tendrá derecho a compartir datos recibidos en virtud del presente capítulo:

a) con personas u organizaciones con miras a la realización de investigaciones científicas o análisis compatibles con el fin para el que se solicitaron los datos, o

b) con los institutos nacionales de estadística y Eurostat para la elaboración 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 nacional. Quedarán excluidas las organizaciones sujetas a una influencia importante de empresas comerciales que es probable que resulte en un acceso preferente a los resultados de la investigación.

3. Las personas físicas u organizaciones que reciban los datos con arreglo al apartado 1 del presente artículo cumplirán las mismas obligaciones que se aplican a los organismos del sector público, a la Comisión, al Banco Central Europeo o a los organismos de la Unión con arreglo al artículo 17, apartado 3, y al artículo 19.

4. No obstante lo dispuesto en el artículo 19, apartado 1, letra c), las personas físicas u organizaciones que reciban los datos con arreglo al apartado 1 del presente artículo podrán conservar los datos recibidos para el fin para el que se solicitaron los datos hasta seis meses desde la supresión de los datos por los organismos del sector público, la Comisión, el Banco Central Europeo y los organismos de la Unión.

5. Cuando un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión se proponga transmitir o poner datos a disposición con arreglo al apartado 1 del presente artículo, lo notificará sin demora indebida al titular de datos del que se hayan recibido los datos, indicando la identidad y los datos de contacto de la organización o persona física que reciba los datos, la finalidad de la transmisión o puesta a disposición de los datos, el plazo durante el cual se utilizarán los datos y las medidas técnicas y organizativas de protección adoptadas, también cuando se trate de datos personales o secretos comerciales. Cuando el titular de datos no acepte la transmisión o puesta a disposición de datos, podrá presentar una reclamación ante la autoridad competente designada en cumplimiento del artículo 37 del Estado miembro en el que esté establecido el titular de datos.

Artículo 22

Asistencia mutua y cooperación transfronteriza

1. Los organismos del sector público, la Comisión, el Banco Central Europeo y los 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 designada en cumplimiento del artículo 37 en dicho Estado miembro. Este requisito se aplicará también a las solicitudes de la Comisión, el Banco Central Europeo y los organismos de la Unión. La solicitud será examinada por la autoridad competente del Estado miembro en el que esté establecido el titular de los datos.

4. Tras haber examinado la solicitud a la luz de los requisitos establecidos en el artículo 17, la autoridad competente pertinente adoptará, sin demora indebida, una de las siguientes medidas:

a) transmitirá la solicitud al titular de datos y, en su caso, asesorará al organismo del sector público solicitante, a la Comisión, al Banco Central Europeo o al organismo de la Unión sobre la necesidad, en su caso, de cooperar con los organismos del sector público del Estado miembro en el que esté establecido el titular de datos con el fin de reducir la carga administrativa que pesa sobre el titular de datos en el cumplimiento de la solicitud;

b) rechazará la solicitud por razones debidamente motivadas, de conformidad con el presente capítulo.

El organismo del sector público solicitante, la Comisión, el Banco Central Europeo y el organismo de la Unión tendrán en cuenta el asesoramiento y los motivos de la autoridad competente pertinente de conformidad con el párrafo primero antes de iniciar cualquier acción adicional, como volver a enviar la solicitud, en su caso.

CAPÍTULO VI

CAMBIO ENTRE SERVICIOS DE TRATAMIENTO DE DATOS

Artículo 23

Eliminación de los obstáculos a un cambio efectivo

Los proveedores de servicios de tratamiento de datos adoptarán las medidas previstas en los artículos 25, 26, 27, 29 y 30 para permitir a los clientes cambiar a un servicio de tratamiento de datos que cubra el mismo tipo de servicio, que sea prestado por un proveedor diferente de servicios de tratamiento de datos o a una infraestructura de TIC local o, cuando proceda, usar varios proveedores de servicios de tratamiento de datos simultáneamente. En particular, los proveedores de servicios de tratamiento de datos eliminarán y no pondrán obstáculos precomerciales, comerciales, técnicos, contractuales y organizativos que disuada a los clientes:

a) resolver, tras el plazo máximo de preaviso y la tramitación con éxito del proceso de cambio, de conformidad con el artículo 25, el contrato de servicio de tratamiento de datos;

b) celebrar nuevos contratos con otro proveedor de servicios de tratamiento de datos que cubran el mismo tipo de servicio;

c) transferir los datos exportables del cliente y sus activos digitales a un proveedor diferente de servicios de tratamiento de datos o a una infraestructura de TIC local, incluso después de haberse beneficiado de una oferta gratuita;

d) de conformidad con el artículo 24, alcanzar la equivalencia funcional en el uso del nuevo servicio de tratamiento de datos en el entorno de las TIC de un proveedor o proveedores diferentes de servicios de tratamiento de datos que incluyan el mismo tipo de servicio;

e) la desagregación, cuando sea técnicamente viable, de los servicios de tratamiento de datos a que se refiere el artículo 30, apartado 1, de otros servicios de tratamiento de datos prestados por el proveedor de servicios de tratamiento de datos.

Artículo 24

Alcance de las obligaciones técnicas

Las responsabilidades de los proveedores de servicios de tratamiento de datos establecidas en los artículos 23, 25, 29, 30 y 34, se aplicarán solo a los servicios, contratos o prácticas comerciales prestados por el proveedor de servicios de tratamiento de datos de origen.

Artículo 25

Cláusulas contractuales relativas al cambio

1. Los derechos del cliente y las obligaciones del proveedor de servicios de tratamiento de datos en relación con el cambio de proveedor de esos servicios o, en su caso, el cambio a una infraestructura de TIC local se establecerán con claridad en un contrato escrito. El proveedor de servicios de tratamiento de datos pondrá dicho contrato a disposición del cliente antes de su firma, de un modo que permita al cliente conservar y reproducir el contrato.

2. Sin perjuicio de lo dispuesto en la Directiva (UE) 2019/770, el contrato a que se refiere el apartado 1 del presente artículo incluirá al menos los siguientes elementos:

a) cláusulas que permitan al cliente, previa solicitud, cambiar a un servicio de tratamiento de datos ofrecido por un proveedor diferente de servicios de tratamiento de datos o trasladar todos los datos exportables y activos digitales a una infraestructura de TIC local, sin demora indebida y, en cualquier caso, en un plazo no superior al período transitorio obligatorio máximo de treinta días naturales, que comenzará al final del plazo máximo de preaviso a que se refiere la letra d), durante el cual el contrato de servicio se seguirá aplicando y durante el cual el proveedor de servicios de tratamiento de datos:

   i) prestará una asistencia razonable al cliente y a terceros autorizados por el cliente en el proceso de cambio,

ii) actuará con la diligencia debida para mantener la continuidad de las actividades y continuará la prestación de las funciones o servicios en virtud del contrato,

iii) proporcionará información clara sobre los riesgos conocidos para la continuidad de la prestación de las funciones o servicios por parte del proveedor de servicios de tratamiento de datos de origen,

iv) garantizará que se mantenga un alto nivel de seguridad a lo largo de todo el proceso de cambio, en particular, la seguridad de los datos durante su transferencia y la seguridad continua de los datos durante el período de extracción especificado en la letra g), de conformidad con el Derecho aplicable de la Unión o nacional;

b) la obligación del proveedor de servicios de tratamiento de datos de apoyar la estrategia de salida del cliente pertinente para los servicios contratados, también proporcionando toda la información pertinente;

c) la cláusula en la que se especifique que el contrato se considerará resuelto y se notificará al cliente la resolución, en uno de los siguientes casos:

i) cuando proceda, una vez concluido con éxito el proceso de cambio,

ii) al final del plazo máximo de preaviso a que se refiere la letra d), cuando el cliente no desee cambiar de proveedor, sino suprimir todos sus datos exportables y activos digitales una vez resuelto el servicio;

d) un plazo máximo de preaviso para el inicio del proceso de cambio, que no excederá de dos meses;

e) una especificación exhaustiva de todas las categorías de datos y activos digitales que pueden ser exportadas durante el proceso de cambio, que deberá comprender, como mínimo, todos los datos exportables;

f) una especificación exhaustiva de las categorías de datos específicas del funcionamiento interno del servicio de tratamiento de datos del proveedor que deben quedar excluidas de los datos exportables con arreglo a la letra e) del presente apartado cuando exista un riesgo de violación de secretos comerciales del proveedor, siempre que dichas exenciones no impidan ni retrasen el proceso de cambio previsto en el artículo 23;

g) un período mínimo para la extracción de datos de al menos treinta días naturales después de la expiración del período transitorio pactado entre el cliente y el proveedor de servicios de tratamiento de datos, de conformidad con la letra a) del presente apartado y el apartado 4;

h) una cláusula que garantice la supresión total de todos los datos exportables y activos digitales generados directamente por el cliente, o directamente relacionados con el cliente, tras la expiración del período de extracción a que se refiere la letra g) o tras la expiración de un período alternativo pactado fijado en una fecha posterior a la fecha de expiración del período de extracción a que se refiere la letra g), siempre que el proceso de cambio haya finalizado con éxito;

i) los costes por cambio que puedan imponer los proveedores de servicios de tratamiento de datos de conformidad con el artículo 29.

3. El contrato al que se refiere el apartado 1, incluirá cláusulas que estipulen que el cliente puede notificar al proveedor de servicios de tratamiento de datos su decisión de realizar una o varias de las siguientes acciones una vez expire el plazo máximo de preaviso a que se refiere el apartado 2, letra d):

a) cambiar a un proveedor diferente de servicios de tratamiento de datos, en cuyo caso el cliente proporcionará los datos de contacto necesarios de dicho proveedor;

b) cambiar a una infraestructura de TIC local;

c) suprimir sus datos exportables y sus activos digitales.

4. Cuando el período transitorio obligatorio máximo establecido en el apartado 2, letra a), sea técnicamente inviable, el proveedor de servicios de tratamiento de datos notificará la inviabilidad técnica al cliente dentro de un plazo de catorce días hábiles desde que se haya presentado la solicitud de cambio, y justificará debidamente dicha inviabilidad e indicará un período transitorio alternativo, que no excederá de siete meses. De conformidad con el apartado 1, se garantizará la continuidad del servicio durante todo el período transitorio alternativo.

5. Sin perjuicio de lo dispuesto en el apartado 4, el contrato al que se refiere el apartado 1 incluirá disposiciones que otorguen al cliente el derecho a prorrogar el período transitorio una vez por un período que el cliente considere más adecuado para sus propios fines.

Artículo 26

Obligación de información de los proveedores de servicios de tratamiento de datos

El proveedor de servicios de tratamiento de datos proporcionará al cliente:

a) información sobre los procedimientos disponibles para el cambio y la transferencia al servicio de tratamiento de datos, incluida la información sobre los métodos y formatos de cambio y de transferencia disponibles, así como las restricciones y limitaciones técnicas conocidas por el proveedor de servicios de tratamiento de datos;

b) una referencia a un registro en línea actualizado alojado por el proveedor de servicios de tratamiento de datos, con detalles de todas las estructuras y formatos de datos, así como de las normas pertinentes y las especificaciones de interoperabilidad abiertas, en el que estén disponibles los datos exportables a que se refiere el artículo 25, apartado 2, letra e).

Artículo 27

Obligación de buena fe

Todas las partes implicadas, incluidos los proveedores de servicios de tratamiento de datos de destino, cooperarán de buena fe para que el proceso de cambio sea eficaz, posibilitar la transferencia de los datos en tiempo oportuno y mantener la continuidad del servicio de tratamiento de datos.

Artículo 28

Obligaciones de transparencia contractual en materia de acceso y transferencia internacionales

1. Los proveedores de servicios de tratamiento de datos pondrán a disposición en sus sitios web la siguiente información y la mantendrán actualizada:

a) la jurisdicción a la que está sujeta la infraestructura de TIC desplegada para el tratamiento de datos de sus servicios individuales;

b) una descripción general de las medidas técnicas, organizativas y contractuales adoptadas por el proveedor de servicios de tratamiento de datos para impedir el acceso o transferencia internacionales por parte de las administraciones públicas de datos no personales que se encuentren en la Unión, cuando dicho acceso o transferencia pueda entrar en conflicto con el Derecho de la Unión o con el Derecho nacional del Estado miembro de que se trate.

2. Los sitios web a que se refiere el apartado 1 se enumerarán en los contratos de todos los servicios de tratamiento de datos ofrecidos por los proveedores de servicios de tratamiento de datos.

Artículo 29

Supresión gradual de los costes por cambio

1. A partir del 12 de enero de 2027, los proveedores de servicios de tratamiento de datos no impondrán al cliente ningún coste por cambio por el proceso de cambio.

2. Del 11 de enero de 2024 hasta el 12 de enero de 2027, los proveedores de servicios de tratamiento de datos podrán imponer al cliente costes por cambio reducidos por el proceso de cambio.

3. Los costes por cambio reducidos contemplados en el apartado 2 no excederán 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. Antes de celebrar un contrato con un cliente, los proveedores de servicios de tratamiento de datos proporcionarán al posible cliente información clara sobre los costes estándar del servicio y las sanciones por resolución anticipada que podrían imponerse, así como sobre la reducción de los costes por cambio que podrían imponerse durante el plazo a que se refiere el apartado 2.

5. Cuando proceda, los proveedores de servicios de tratamiento de datos proporcionarán información al cliente sobre los servicios de tratamiento de datos que impliquen un cambio muy complejo o costoso o para los que sea imposible cambiar de proveedor sin interferencias significativas en los datos, los activos digitales o la arquitectura del servicio.

6. Cuando proceda, los proveedores de servicios de tratamiento de datos pondrán la información a que se refieren los apartados 4 y 5 a disposición pública para los clientes a través de una sección específica de su sitio web o de cualquier otra forma fácilmente accesible.

7. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 45, con el fin de completar el presente Reglamento mediante el establecimiento de un mecanismo de seguimiento que permita a la Comisión supervisar los costes por cambio aplicados por los proveedores de servicios de tratamiento de datos en el mercado para garantizar que la supresión y la reducción de los costes por cambio con arreglo a los apartados 1 y 2 del presente artículo, se alcancen de conformidad con los plazos previstos en dichos apartados.

Artículo 30

Aspectos técnicos del cambio

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 virtuales 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, adoptarán, de conformidad con el artículo 27, todas las medidas razonables a su alcance para facilitar que el cliente, tras cambiar a un servicio que cubra el mismo tipo de servicio, logre la equivalencia funcional en el uso del servicio de tratamiento de datos de destino. El proveedor de servicios de tratamiento de datos de origen facilitará el proceso de cambio proporcionando capacidades, información adecuada, documentación, apoyo técnico y, cuando proceda, las herramientas necesarias.

2. Los proveedores de servicios de tratamiento de datos, distintos de a los que se refiere el apartado 1, pondrán gratuitamente interfaces abiertas a disposición de todos sus clientes y de los proveedores de servicios de tratamiento de datos de destino afectados, de igual manera, para facilitar el proceso de cambio. Estas interfaces incluirán información suficiente sobre el servicio de que se trate para permitir el desarrollo de programas informáticos para comunicarse con los servicios, a efectos de la portabilidad de los datos y la interoperabilidad.

3. En el caso de servicios de tratamiento de datos distintos de los contemplados en el apartado 1 del presente artículo, los proveedores de servicios de tratamiento de datos garantizarán la compatibilidad con las especificaciones comunes basadas en especificaciones de interoperabilidad abiertas o normas armonizadas de interoperabilidad al menos doce meses después de la publicación de las referencias a dichas especificaciones comunes de interoperabilidad o normas armonizadas de interoperabilidad de los servicios de tratamiento de datos en el repositorio central de la Unión de normas para la interoperabilidad de los servicios de tratamiento de datos tras la publicación de los actos de ejecución correspondientes en el *Diario Oficial de la Unión Europea* de conformidad con el artículo 35, apartado 7.

4. Los proveedores de servicios de tratamiento de datos distintos de los contemplados en el apartado 1 del presente artículo actualizarán el registro en línea a que se refiere el artículo 26, letra b), de conformidad con sus obligaciones en virtud del apartado 3 del presente artículo.

5. En caso de cambio entre servicios del mismo tipo de servicio, para los que no se hayan publicado las especificaciones comunes o las normas armonizadas de interoperabilidad a que se refiere el apartado 3 del presente artículo en el repositorio central de la Unión de normas para la interoperabilidad de los servicios de tratamiento de datos de conformidad con el artículo 35, apartado 8, el proveedor de servicios de tratamiento de datos exportará, a petición del cliente, todos los datos exportables en un formato estructurado, de utilización habitual y de lectura mecánica.

6. Los proveedores de servicios de tratamiento de datos no estarán obligados a desarrollar nuevas tecnologías o servicios, ni a revelar o transferir activos digitales protegidos por derechos de propiedad intelectual o que constituyan un secreto comercial, a un cliente o a un proveedor diferente de servicios de tratamiento de datos, ni a comprometer la seguridad y la integridad del servicio del cliente o del proveedor.

Artículo 31

Régimen específico para determinados servicios de tratamiento de datos

1. Las obligaciones establecidas en el artículo 23, letra d), en el artículo 29 y en el artículo 30, apartados 1 y 3, no se aplicarán a los servicios de tratamiento de datos una mayor parte de cuyas características principales se hayan desarrollado a medida para satisfacer las necesidades específicas de un cliente concreto o en los que todos los componentes se hayan desarrollado para los fines de un cliente concreto, y cuando esos servicios de tratamiento de datos no se ofrezcan a gran escala comercial a través del catálogo de servicios del proveedor de servicios de tratamiento de datos.

2. Las obligaciones establecidas en el presente capítulo no se aplicarán a los servicios de tratamiento de datos prestados como versión no destinada a la producción con fines de ensayo y evaluación y durante un período de tiempo limitado.

3. Antes de la celebración de un contrato sobre la prestación de los servicios de tratamiento de datos a que se refiere el presente artículo, el proveedor de servicios de tratamiento de datos informará al posible cliente de las obligaciones del presente capítulo que no sean aplicables.

CAPÍTULO VII

ACCESO Y TRANSFERENCIA INTERNACIONALES ILÍCITOS DE DATOS NO PERSONALES POR PARTE DE ADMINISTRACIONES PÚBLICAS

Artículo 32

Acceso y transferencia internacionales por parte de administraciones públicas

1. Los proveedores de servicios de tratamiento de datos personales adoptarán todas las medidas técnicas, organizativas y jurídicas adecuadas, lo que incluye la celebración de contratos, para impedir el acceso y la transferencia internacionales y por parte de las administraciones públicas de terceros países de datos no personales que se encuentren en la Unión, cuando dicha transferencia o 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 órganos jurisdiccionales de un tercer país y las decisiones de autoridades administrativas de un tercer país en las que se exija a un proveedor de servicios de tratamiento de datos transferir o dar acceso a datos no personales incluidos en el ámbito de aplicación del presente Reglamento que se encuentren en la Unión solo se reconocerá o ejecutará 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 un acuerdo internacional de los contemplados en el apartado 2, cuando un proveedor de servicios de tratamiento de datos sea el destinatario de una resolución o sentencia de un órgano jurisdiccional de un tercer país o de una decisión de una autoridad administrativa de un tercer país de transferir o dar acceso a datos no personales incluidos en el ámbito de aplicación del presente Reglamento que se encuentren en la Unión y el cumplimiento de dicha decisión entrañe el riesgo de que el destinatario entre en conflicto con el Derecho de la Unión o con el Derecho nacional del Estado miembro de que se trate, la transferencia a dichos datos o el acceso a los mismos por parte de dicha autoridad de un tercer país solo tendrá lugar cuando:

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

b) la oposición motivada del destinatario se someta a la apreciación de un órgano jurisdiccional competente del tercer país, y

c) el órgano jurisdiccional competente del tercer país que dicte la resolución o sentencia o revise la resolución de una autoridad administrativa esté facultado, con arreglo al Derecho del tercer país, 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 o sentencia podrá solicitar el dictamen del organismo nacional pertinente o de la autoridad competente en materia de cooperación internacional en asuntos jurídicos, con el fin de determinar si se cumplen las condiciones establecidas en el párrafo primero, en particular, cuando considere que la decisión puede referirse a secretos comerciales y otros datos sensibles desde el punto de vista comercial, así como a contenidos protegidos por derechos de propiedad intelectual, o que la transferencia puede dar lugar a una reidentificación. El organismo o autoridad nacional competente podrá consultar a la Comisión. Si el destinatario considera que la decisión o sentencia puede afectar a los intereses de la seguridad nacional o de la defensa de la Unión o de sus Estados miembros, solicitará el dictamen del organismo o autoridad nacional competente, a fin de determinar si los datos solicitados se refieren a intereses de seguridad nacional o de defensa de la Unión o de sus Estados miembros. Si el destinatario no ha recibido una respuesta en el plazo de un mes, o si el dictamen de tal organismo o autoridad llega a la conclusión de que no se cumplen las condiciones establecidas en el párrafo primero, el destinatario podrá denegar por esos motivos la solicitud de transferencia o acceso a datos no personales.

El CEID a que se refiere el artículo 42 asesorará y asistirá a la Comisión en la elaboración de directrices para la evaluación del cumplimiento de las condiciones establecidas en el párrafo primero del presente apartado.

4. Si se cumplen las condiciones establecidas en los apartados 2 o 3, el proveedor de servicios de tratamiento de datos proporcionará la cantidad mínima de datos permitida en respuesta a una solicitud, sobre la base de la interpretación razonable de dicha solicitud por parte del proveedor o del organismo o autoridad nacional competente a que se refiere el apartado 3, párrafo segundo.

5. Antes de dar cumplimiento a dicha solicitud, el proveedor de servicios de tratamiento de datos informará al cliente de que una autoridad 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 33

Requisitos esenciales en materia de interoperabilidad de los datos, de los mecanismos y servicios de intercambio de datos, y de los espacios comunes europeos de datos

1. Los participantes en espacios de datos que ofrezcan datos o servicios de datos a otros participantes cumplirán los siguientes requisitos esenciales para facilitar la interoperabilidad de los datos, de los mecanismos y servicios de intercambio de datos, y de los espacios comunes europeos de datos que sean marcos interoperables específicos, sectoriales o intersectoriales de normas y prácticas comunes para compartir o tratar conjuntamente datos con el fin, entre otros, de desarrollar nuevos productos y servicios, investigación científica o iniciativas de la sociedad civil:

a) el contenido del conjunto de datos, las restricciones de utilización, las licencias, la metodología de recopilación de datos y la calidad e incertidumbre de los datos se describirán en una medida suficiente, cuando proceda, en un formato de lectura mecánica 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, cuanto estén disponibles, 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, incluido de forma continua, en descarga masiva o en tiempo real, en un formato de lectura mecánica cuando sea técnicamente viable y no impida el buen funcionamiento del producto conectado;

d) cuando proceda, se proporcionarán los medios que posibiliten la interoperabilidad de las herramientas para automatizar la ejecución de los acuerdos de intercambio de datos, como los contratos inteligentes.

Los 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 disposiciones del Derecho de la Unión o nacional.

2. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 45 del presente Reglamento por los que se complete el presente Reglamento especificando en mayor medida los requisitos esenciales establecidos en el apartado 1 del presente artículo, en relación con aquellos requisitos que, por su naturaleza, no puedan producir el efecto deseado a menos que se especifiquen con más detalle en actos jurídicos vinculantes de la Unión y con el fin de reflejar adecuadamente la evolución tecnológica y del mercado.

Cuando adopte actos delegados, la Comisión tendrá en cuenta el asesoramiento del CEID de conformidad con el artículo 42, letra c), inciso iii).

3. Se presumirá que los participantes en espacios de datos que ofrezcan datos o servicios de datos a otros participantes en espacios de datos que cumplan las normas armonizadas o partes de estas normas, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea,* cumplen los requisitos esenciales establecidos en el apartado 1 en la medida en que dichas normas armonizadas o partes de ellas cubran dichos requisitos.

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

5. La Comisión podrá adoptar, mediante actos de ejecución, especificaciones comunes que cubran alguno o todos los requisitos esenciales establecidos en el apartado 1 cuando se cumplan las siguientes condiciones:

a) que la Comisión haya solicitado, en virtud del artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, a una o varias organizaciones europeas de normalización la redacción de una norma armonizada que cumpla los requisitos esenciales establecidos en el apartado 1 del presente artículo y:

   i) la solicitud no haya sido aceptada,

   ii) las normas armonizadas en respuesta a dicha solicitud no se entreguen dentro del plazo establecido de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, o

   iii) las normas armonizadas no se ajusten a la solicitud, y

b) no se haya publicado en el *Diario Oficial de la Unión Europea* ninguna referencia a normas armonizadas que regulen los requisitos esenciales pertinentes establecidos en el apartado 1 del presente artículo, de conformidad con el Reglamento (UE) n.º 1025/2012 y no se prevea la publicación de ningún proyecto de norma en un plazo razonable.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 46, apartado 2.

6. Antes de preparar un proyecto de acto de ejecución a que se refiere el apartado 5 del presente artículo, la Comisión informará al comité a que se refiere el artículo 22 del Reglamento (UE) n.º 1025/2012 de que considera que se cumplen las condiciones establecidas en el apartado 5 del presente artículo.

7. Al preparar el proyecto de acto de ejecución a que se refiere el apartado 5, la Comisión tendrá en cuenta el asesoramiento del CEID y las opiniones de otros organismos o grupos de expertos pertinentes y consultará debidamente a todas las partes interesadas pertinentes.

8. Se presumirá que los participantes en espacios de datos que ofrezcan datos o servicios de datos a otros participantes en espacios de datos que cumplan las especificaciones comunes establecidas por los actos de ejecución a que se refiere el apartado 5, o partes de estos, cumplen los requisitos esenciales establecidos en el apartado 1, en la medida en que dichos requisitos estén contemplados por tales especificaciones comunes o partes de ellas.

9. Cuando una norma armonizada sea adoptada por una organización europea de normalización y propuesta a la Comisión con el fin de publicar su referencia en el *Diario Oficial de la Unión Europea,* la Comisión evaluará la norma armonizada de conformidad con el Reglamento (UE) n.º 1025/2012. Cuando la referencia de una norma armonizada se haya publicado en el *Diario Oficial de la Unión Europea,* la Comisión derogará los actos de ejecución a que se refiere el apartado 5 del presente artículo, o partes de estos que prevean los mismos requisitos esenciales que los contemplados por las normas armonizadas.

10. Cuando un Estado miembro considere que una especificación común no cumple plenamente los requisitos esenciales establecidos en el apartado 1, informará de ello a la Comisión presentando una explicación detallada. La Comisión evaluará dicha explicación detallada y podrá modificar, si procede, el acto de ejecución por el que se establezca la especificación común en cuestión.

11. La Comisión podrá adoptar directrices teniendo en cuenta la propuesta del CEID de conformidad con el artículo 30, letra h), del Reglamento (UE) 2022/868, que establezcan marcos de interoperabilidad de las normas y prácticas comunes para el funcionamiento de los espacios comunes europeos de datos.

Artículo 34

Interoperabilidad a efectos del uso en paralelo de los servicios de tratamiento de datos

1. Los requisitos establecidos en el artículo 23, el artículo 24, el artículo 25, apartado 2, letra a), incisos ii) y iv), letras e) y f), y el artículo 30, apartados 2 a 5, se aplicarán también *mutatis mutandis* a los proveedores de servicios de tratamiento de datos para facilitar la interoperabilidad a efectos del uso en paralelo de los servicios de tratamiento de datos.

2. Cuando un servicio de tratamiento de datos se utilice en paralelo con otro servicio de tratamiento de datos, los proveedores de servicios de tratamiento de datos podrán imponer costes de salida de datos, pero solo con el fin de repercutir los costes de salida soportados, sin superar dichos costes.

Artículo 35

Interoperabilidad de los servicios de tratamiento de datos

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

a) lograr, cuando sea técnicamente viable, 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) facilitar, cuando sea técnicamente viable, la equivalencia funcional entre los servicios de tratamiento de datos a que se refiere el artículo 30, apartado 1, que cubran el mismo tipo de servicios;

d) no afectar negativamente a la seguridad e integridad de los servicios de tratamiento de datos y de los datos;

e) formularse de tal forma que permitan avances técnicos y la incorporación de nuevas funciones e innovaciones en los servicios de tratamiento de datos.

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

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 del Reglamento (UE) n.º 1025/2012.

4. Tras tener en cuenta las normas internacionales y europeas pertinentes y las iniciativas de autorregulación, la Comisión podrá, de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, pedir a una o varias organizaciones europeas de normalización que elaboren normas armonizadas que satisfagan los requisitos esenciales establecidos en los apartados 1 y 2 del presente artículo.

5. La Comisión podrá adoptar, mediante actos de ejecución, especificaciones comunes sobre la base de especificaciones de interoperabilidad abiertas que cubran todos los requisitos esenciales establecidos en los apartados 1 y 2.

6. Cuando prepare el proyecto de acto de ejecución a que se refiere el apartado 5 del presente artículo, la Comisión tendrá en cuenta las opiniones de las autoridades competentes a que se refiere el artículo 37, apartado 5, letra h), y de otros organismos o grupos de expertos pertinentes, y consultará debidamente a todas las partes interesadas pertinentes.

7. Cuando un Estado miembro considere que una especificación común no cumple plenamente los requisitos establecidos en los apartados 1 y 2, informará de ello a la Comisión presentando una explicación detallada. La Comisión evaluará dicha explicación detallada y podrá modificar, si procede, el acto de ejecución por el que se establezca la especificación común en cuestión.

8. A efectos del artículo 30, apartado 3, la Comisión publicará, mediante actos de ejecución, las referencias de las normas armonizadas y las especificaciones comunes para la interoperabilidad de los servicios de tratamiento de datos en un repositorio central de la Unión de normas para la interoperabilidad de los servicios de tratamiento de datos.

9. Los actos de ejecución a que se refiere el presente artículo se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 46, apartado 2.

Artículo 36

Requisitos esenciales relativos a los contratos inteligentes para la ejecución de acuerdos de 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 el despliegue de contratos inteligentes para terceros en el contexto de la ejecución de la totalidad o parte de un acuerdo, para poner datos a disposición garantizará que los contratos inteligentes cumplen los siguientes requisitos esenciales:

a) solidez y control de acceso, para garantizar que el contrato inteligente se haya diseñado de manera que ofrezca unos mecanismos de control de acceso y un grado de solidez muy elevado con el fin de evitar errores funcionales y contrarrestar los intentos de manipulación por terceros;

b) resolución unilateral e interrupción seguras, para garantizar que exista un mecanismo que permita poner fin a la ejecución de transacciones y que el contrato inteligente incluye funciones internas que permitan reinicializar el contrato o darle instrucciones para poner fin a la operación o interrumpirla, en particular, para evitar futuras ejecuciones accidentales;

c) archivo y continuidad de los datos, para garantizar, en circunstancias en las que el contrato inteligente deba finalizar o desactivarse, 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);

d) control de acceso, para garantizar que el contrato inteligente esté protegido con mecanismos rigurosos de control de acceso en el nivel de la gobernanza y en el del contrato inteligente, y

e) coherencia, para garantizar la coherencia con las condiciones del acuerdo de intercambio de datos que ejecuta el contrato inteligente.

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

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 el despliegue de contratos inteligentes para terceros en el contexto de la ejecución de la totalidad o de parte de un acuerdo de puesta a disposición de datos será responsable del cumplimiento de los requisitos esenciales establecidos 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, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea,* es conforme con los requisitos esenciales establecidos en el apartado 1, en la medida en que dichos requisitos estén contemplados por tales normas armonizadas o partes de ellas.

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

6. La Comisión podrá adoptar, mediante actos de ejecución, especificaciones comunes que cubran alguno o todos los requisitos esenciales establecidos en el apartado 1 cuando se cumplan las siguientes condiciones:

a) que la Comisión haya solicitado, en virtud del artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, a una o varias organizaciones europeas de normalización la redacción de una norma armonizada que cumpla los requisitos esenciales establecidos en el apartado 1 del presente artículo y:

   i) la solicitud no haya sido aceptada,

   ii) las normas armonizadas en respuesta a dicha solicitud no se entreguen dentro del plazo establecido de conformidad con el artículo 10, apartado 1, del Reglamento (UE) n.º 1025/2012, o

   iii) las normas armonizadas no se ajusten a la solicitud, y

b) no se haya publicado en el *Diario Oficial de la Unión Europea* ninguna referencia a normas armonizadas que regulen los requisitos esenciales pertinentes establecidos en el apartado 1 del presente artículo, de conformidad con el Reglamento (UE) n.º 1025/2012 y no se prevea la publicación de ningún proyecto de norma en un plazo razonable.

Dichos actos de ejecución se adoptarán de conformidad con el procedimiento de examen a que se refiere el artículo 46, apartado 2.

7. Antes de preparar un proyecto de acto de ejecución a que se refiere el apartado 6 del presente artículo, la Comisión informará al Comité a que se refiere el artículo 22 del Reglamento (UE) n.º 1025/2012 de que considera que se cumplen las condiciones establecidas en el apartado 6 del presente artículo.

8. Cuando prepare el proyecto de acto de ejecución a que se refiere el apartado 6, la Comisión tendrá en cuenta el asesoramiento del CEID y las opiniones de otros organismos o grupos de expertos pertinentes y consultará debidamente a todas las partes interesadas pertinentes.

9. Se presumirá que el proveedor de un contrato inteligente o, en su defecto, la persona cuya actividad comercial, empresarial o profesional implique el despliegue de contratos inteligentes para terceros en el contexto de la ejecución de la totalidad o de parte de un acuerdo de puesta a disposición de datos que cumplan las especificaciones comunes establecidas por los actos de ejecución a que se refiere el apartado 6, o partes de estos, cumple los requisitos esenciales establecidos en el apartado 1 en la medida en que dichos requisitos estén cubiertos por tales especificaciones comunes o partes de ellas.

10. Cuando una norma armonizada sea adoptada por una organización europea de normalización y propuesta a la Comisión con el fin de publicar su referencia en el *Diario Oficial de la Unión Europea,* la Comisión evaluará la norma armonizada de conformidad con el Reglamento (UE) n.º 1025/2012. Cuando la referencia de una norma armonizada se haya publicado en el *Diario Oficial de la Unión Europea,* la Comisión derogará los actos de ejecución a que se refiere el apartado 6 del presente artículo, o partes de este que prevean los mismos requisitos esenciales que los contemplados por la norma armonizada.

11. Cuando un Estado miembro considere que una especificación común no cumple plenamente los requisitos establecidos en el apartado 1, informará de ello a la Comisión presentando una explicación detallada. La Comisión evaluará dicha explicación detallada y podrá modificar, si procede, el acto de ejecución por el que se establezca la especificación común en cuestión.

CAPÍTULO IX

APLICACIÓN Y EJECUCIÓN

Artículo 37

Autoridades competentes y coordinadores de datos

1. Cada Estado miembro designará una o varias autoridades nacionales competentes para garantizar la aplicación y ejecución del presente Reglamento (en lo sucesivo, «autoridades competentes»). Los Estados miembros podrán establecer una o varias autoridades nuevas o recurrir a las autoridades existentes.

2. Cuando un Estado miembro designe más de una autoridad competente, designará a un coordinador de datos de entre ellas para facilitar la cooperación entre las autoridades competentes y ayudar a las entidades dentro del ámbito de aplicación del presente Reglamento en todas las cuestiones relacionadas con la aplicación y el control del cumplimiento de este. Las autoridades competentes cooperarán mutuamente en el ejercicio de las funciones y competencias que les hayan sido asignadas con arreglo al apartado 5.

3. Las autoridades de control 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.

El Supervisor Europeo de Protección de Datos tendrá la responsabilidad de supervisar la aplicación del presente Reglamento en lo que respecta a la Comisión, el Banco Central Europeo o los organismos de la Unión. Cuando proceda, se aplicará *mutatis mutandis* el artículo 62 del Reglamento (UE) 2018/1725.

Las funciones y competencias de las autoridades de control a que se refiere el presente apartado se ejercerán respecto al tratamiento de datos personales.

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

a) para cuestiones sectoriales específicas de la utilización y acceso de datos relacionados con la aplicación del presente Reglamento, se respetará la competencia de las autoridades sectoriales;

b) la autoridad competente responsable de la aplicación y ejecución de los artículos 23 a 31 y de los artículos 34 y 35 tendrá experiencia en el ámbito de los datos y los servicios de comunicaciones electrónicas.

5. Los Estados miembros velarán por que las funciones y competencias de las autoridades competentes estén claramente definidas e incluyan:

a) fomentar la alfabetización en materia de datos y 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, también en relación con secretos comerciales, investigar el objeto de las denuncias en la medida adecuada e informar periódicamente a los denunciantes, cuando proceda de conformidad con el Derecho nacional, 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 sanciones económicas efectivas, proporcionadas y disuasorias, que pueden incluir multas coercitivas y multas con efecto retroactivo, o iniciar procedimientos judiciales para la imposición de multas;

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

f) cooperar con las autoridades competentes de otros Estados miembros y, cuando proceda, con la Comisión o el CEID, para garantizar la aplicación coherente y eficiente del presente Reglamento, lo que incluye el intercambio de toda la información pertinente por medios electrónicos, sin demora indebida, también con respecto al apartado 10 del presente artículo;

g) cooperar con las autoridades competentes pertinentes responsables de la aplicación de otros actos jurídicos de la Unión o nacionales, también con las autoridades competentes en el ámbito de los datos y los servicios de comunicaciones electrónicas, con la autoridad de control responsable del seguimiento de la aplicación del Reglamento (UE) 2016/679 o con las autoridades sectoriales para garantizar que el presente Reglamento se aplica de manera coherente con otras disposiciones del Derecho de la Unión y nacional;

h) cooperar con las autoridades competentes pertinentes para garantizar que los artículos 23 a 31 y los artículos 34 y 35 se cumplan de manera coherente con otras disposiciones del Derecho de la Unión y medidas de autorregulación aplicables a los proveedores de servicios de tratamiento de datos;

i) velar por la supresión de los costes por cambio de conformidad con el artículo 29;

j) examinar las solicitudes de datos formuladas con arreglo al capítulo V.

Si se ha designado, el coordinador de datos facilitará la cooperación a que se refieren las letras f), g) y h) del párrafo primero y asistirá a las autoridades competentes si estas lo solicitan.

6. En caso de que dicha autoridad competente haya sido designada, el coordinador de datos deberá:

a) actuar como punto de contacto único para todas las cuestiones relacionadas con la aplicación del presente Reglamento;

b) asegurar la disponibilidad pública en línea de las solicitudes de puesta a disposición de datos presentadas por organismos del sector público en los casos de necesidad excepcional con arreglo al capítulo V y promover acuerdos voluntarios de intercambio de datos entre organismos del sector público y titulares de datos;

c) informar anualmente a la Comisión de las denegaciones notificadas con arreglo al artículo 4, apartados 2 y 8, y al artículo 5, apartado 11.

7. Los Estados miembros notificarán a la Comisión los nombres de las autoridades competentes y sus funciones y competencias, así como, cuando proceda, el nombre del coordinador de datos. La Comisión mantendrá un registro público de dichas autoridades.

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

9. Los Estados miembros velarán por dotar a las autoridades competentes de los recursos técnicos y humanos suficientes y de los conocimientos especializados pertinentes para el ejercicio adecuado de sus funciones de conformidad con el presente Reglamento.

10. Las entidades incluidas en el ámbito de aplicación del presente Reglamento estarán sujetas a la competencia del Estado miembro en el que esté establecida la entidad. Cuando la entidad esté establecida en más de un Estado miembro, se considerará que es competencia del Estado miembro en el que tenga su establecimiento principal, es decir, donde la entidad tenga su domicilio social o administración central, desde el que se ejerza las principales funciones financieras y el control operativo.

11. Toda entidad incluida en el ámbito de aplicación del presente Reglamento que ponga a disposición productos conectados u ofrezca servicios en la Unión y que no esté establecida en la Unión designará un representante legal en uno de los Estados miembros.

12. A efectos de garantizar el cumplimiento del presente Reglamento, toda entidad incluida en el ámbito de aplicación del presente Reglamento que ponga a disposición productos conectados u ofrezca servicios en la Unión, otorgará un mandato a un representante legal para que las autoridades competentes se pongan en contacto con dicho representante, además o en lugar de la entidad, en relación con todas las cuestiones relacionadas con esta. Dicho representante legal cooperará y demostrará exhaustivamente a las autoridades competentes, previa solicitud, las medidas y las disposiciones adoptadas por la entidad incluida en el ámbito de aplicación del presente Reglamento que ponga a disposición productos conectados u ofrezca servicios en la Unión, a fin de garantizar el cumplimiento del presente Reglamento.

13. Se considerará que toda entidad incluida en el ámbito de aplicación del presente Reglamento que ponga a disposición productos conectados u ofrezca servicios en la Unión queda sometida a la competencia del Estado miembro en el que esté ubicado su representante legal. La designación de un representante legal por tal entidad se entenderá sin perjuicio de las responsabilidades que se puedan exigir a dicha entidad y de cualesquiera acciones legales que puedan ejercitarse contra ella. Hasta que designe a un representante legal de conformidad con el presente artículo, la entidad será competencia de todos los Estados miembros, cuando proceda, a efectos de garantizar la aplicación y ejecución del presente Reglamento. Cualquier autoridad competente podrá ejercer su competencia, incluso imponiendo sanciones efectivas, proporcionadas y disuasorias, siempre que la entidad no esté sujeta a procedimientos de ejecución en virtud del presente Reglamento por los mismos hechos por otra autoridad competente.

14. Las autoridades competentes estarán facultadas para solicitar a los usuarios, titulares de datos o destinatarios de datos, o a sus representantes legales, que sean competencia de su Estado miembro, toda la información necesaria para verificar el cumplimiento del presente Reglamento. Las solicitudes de información serán proporcionadas al cumplimiento de la tarea subyacente y estarán motivadas.

15. Cuando una autoridad competente de un Estado miembro solicite asistencia o medidas de ejecución a una autoridad competente de otro Estado miembro, presentará una solicitud motivada. Una vez recibida dicha solicitud, la autoridad competente responderá, sin demora indebida, detallando las medidas adoptadas o previstas.

16. Las autoridades competentes respetarán los principios de confidencialidad y de secreto profesional y comercial, y protegerán los datos de carácter personal con arreglo al Derecho de la Unión o nacional. Toda la información intercambiada en el contexto de una solicitud de asistencia y proporcionada en virtud del presente artículo se utilizará únicamente en relación con el asunto para el que se solicitó.

Artículo 38

Derecho a presentar una reclamación

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. El coordinador de datos proporcionará, previa solicitud, toda la información necesaria a las personas físicas y jurídicas para la presentación de sus reclamaciones ante la correspondiente autoridad competente.

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

3. Las autoridades competentes cooperarán para tramitar y resolver las reclamaciones, de manera efectiva y en tiempo oportuno, lo que incluirá el intercambio de toda información pertinente por medios electrónicos, sin demora indebida. Dicha cooperación no afectará a los mecanismos de cooperación previstos en los capítulos VI y VII del Reglamento (UE) 2016/679 y en el Reglamento (UE) 2017/2394.

Artículo 39

Derecho a una tutela judicial efectiva

1. No obstante cualquier recurso administrativo o extrajudicial, toda persona física o jurídica afectada tendrá derecho a una tutela judicial efectiva en lo que respecta a las decisiones jurídicamente vinculantes adoptadas por las autoridades competentes.

2. En caso de que una autoridad competente no dé curso a una reclamación, cualquier persona física o jurídica afectada tendrá derecho, de conformidad con el Derecho nacional, a la tutela judicial efectiva o acceso a revisión por un órgano imparcial que disponga de los conocimientos especializados adecuados.

3. Los recursos presentados en virtud del presente artículo se dirimirán ante los órganos jurisdiccionales del Estado miembro de la autoridad competente contra la cual se interponga el recurso a título individual o colectivo, según corresponda, por los representantes de una o varias personas físicas o jurídicas.

Artículo 40

Sanciones

1. Los Estados miembros establecerán el régimen de sanciones aplicables a cualquier infracción del presente Reglamento y adoptarán todas las medidas necesarias para garantizar su ejecución. Tales sanciones serán efectivas, proporcionadas y disuasorias.

2. A más tardar el 12 de septiembre de 2025, los Estados miembros comunicarán a la Comisión el régimen establecido y las medidas adoptadas, y le notificarán sin demora toda modificación posterior. La Comisión actualizará periódicamente y mantendrá un registro público de fácil acceso de dichas medidas.

3. Por lo que respecta a la imposición de sanciones por infracciones del presente Reglamento, los Estados miembros tendrán en cuenta las recomendaciones del CEID y los siguientes criterios no exhaustivos:

a) la naturaleza, gravedad, magnitud y duración de la infracción;

b) cualquier medida adoptada por la parte infractora para mitigar o reparar el perjuicio causado por la infracción;

c) las infracciones anteriores cometidas por la parte infractora;

d) los beneficios financieros obtenidos o las pérdidas evitadas por la parte infractora debido a la infracción, en la medida en que dichos beneficios o pérdidas puedan establecerse de forma fiable;

e) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso;

f) el volumen de negocio anual del infractor durante el ejercicio financiero anterior en la Unión.

4. En caso de infracción de las obligaciones establecidas en los capítulos II, III y V del presente Reglamento, las autoridades de control responsables de supervisar la aplicación del Reglamento (UE) 2016/679 podrán, dentro de su ámbito de competencia, imponer multas administrativas de conformidad con el artículo 83 del Reglamento (UE) 2016/679 y hasta el importe mencionado en el artículo 83, apartado 5, de dicho Reglamento.

5. En caso de infracción de las obligaciones establecidas en el capítulo V del presente Reglamento, el Supervisor Europeo de Protección de Datos podrá imponer, dentro de su ámbito de competencia, 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 41

Cláusulas contractuales tipo y cláusulas contractuales estándar

La Comisión, antes del 12 de septiembre de 2025, elaborará y recomendará cláusulas contractuales tipo no vinculantes sobre el acceso a los datos y su utilización, incluidas cláusulas relativas a la compensación razonable y la protección de los secretos comerciales, así como cláusulas contractuales estándar no vinculantes para contratos de computación en la nube para ayudar a las partes en la elaboración y negociación de contratos con derechos y obligaciones contractuales justos, razonables y no discriminatorios.

Artículo 42

Función del CEID

El CEID establecido como grupo de expertos de la Comisión en virtud del artículo 29 del Reglamento (UE) 2022/868, en el que estarán representadas las autoridades competentes, apoyará la aplicación coherente del presente Reglamento mediante:

a) el asesoramiento y la asistencia a la Comisión en el desarrollo de una práctica coherente de las autoridades competentes en la aplicación de los capítulos II, III, V y VII;

b) la facilitación de la cooperación entre las autoridades competentes mediante el desarrollo de capacidades y el intercambio de información, en particular con el establecimiento de métodos para el intercambio eficiente de información relativa al cumplimiento de los derechos y obligaciones en virtud de los capítulos II, III y V en los casos transfronterizos, incluida la coordinación con respecto al establecimiento de sanciones;

c) el asesoramiento y la asistencia a la Comisión en relación a lo siguiente:

   i) la posibilidad de solicitar la elaboración de las normas armonizadas a que se refieren el artículo 33, apartado 4, el artículo 35, apartado 4, y el artículo 36, apartado 5,

   ii) la preparación de los actos de ejecución a que se refieren el artículo 33, apartado 5, el artículo 35, apartados 5 y 8, y el artículo 36, apartado 6,

   iii) la preparación de los actos delegados a que se refieren el artículo 29, apartado 7, y el artículo 33, apartado 2, y

   iv) la adopción de las directrices que establezcan los marcos de interoperabilidad de las normas y prácticas comunes para el funcionamiento de los espacios comunes europeos de datos a que se refiere el artículo 33, apartado 11.

CAPÍTULO X

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

Artículo 43

Bases de datos que contienen ciertos datos

El derecho *sui generis* establecido en el artículo 7 de la Directiva 96/9/CE no se aplicará si los datos son obtenidos o generados por un producto conectado o servicio relacionado que entre en el ámbito de aplicación del presente Reglamento, en particular en relación con los artículos 4 y 5.

CAPÍTULO XI

DISPOSICIONES FINALES

Artículo 44

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 11 de enero de 2024 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 del Derecho 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 proporcionados por usuarios o de utilizarlos;

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

3. El presente Reglamento, con excepción del capítulo V, se entiende sin perjuicio del Derecho de la Unión y nacional que establece el acceso a los datos y autoriza la utilización de los datos con fines de investigación científica.

Artículo 45

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 29, apartado 7, y en el artículo 33, apartado 2, se otorgan a la Comisión por un período de tiempo indefinido a partir del 11 de enero de 2024.

3. La delegación de poderes mencionada en el artículo 29, apartado 7, y en el artículo 33, apartado 2, 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 de 13 de abril de 2016 sobre la mejora de la legislación.

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 29, apartado 7, o del artículo 33, apartado 2, 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 46

Procedimiento de comité

1. La Comisión estará asistida por el Comité establecido por el Reglamento (UE) 2022/868. 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 47

Modificación del Reglamento (UE) 2017/2394

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

«29. Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (DO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).».

Artículo 48

Modificación de la Directiva (UE) 2020/1828

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

«68. Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (DO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).».

Artículo 49

Evaluación y revisión

1. A más tardar el 12 de septiembre de 2028, la Comisión llevará a cabo una evaluación del presente Reglamento y presentará un informe sobre sus principales conclusiones al Parlamento Europeo y al Consejo, y al Comité Económico y Social Europeo. En la evaluación se analizarán, en particular:

a) situaciones que hayan de considerarse situaciones de necesidad excepcional a efectos del artículo 15 del presente Reglamento y de la aplicación del capítulo V del presente Reglamento en la práctica, en particular, la experiencia adquirida con la aplicación del capítulo V del presente Reglamento por parte de organismos del sector público, la Comisión, el Banco Central Europeo y los organismos de la Unión; el número y el resultado de los recursos iniciados ante la autoridad competente con arreglo al artículo 18, apartado 5, sobre la aplicación del capítulo V del presente Reglamento, comunicados por las autoridades competentes; el impacto de otras obligaciones establecidas en el Derecho de la Unión o nacional a efectos del cumplimiento de las solicitudes de acceso a información; el impacto de los mecanismos voluntarios de intercambio de datos, como los establecidos por organizaciones de gestión de datos con fines altruistas reconocidas en virtud del Reglamento (UE) 2022/868, en el cumplimiento de los objetivos del capítulo V del presente Reglamento, y la función de los datos personales en el contexto del artículo 15 del presente Reglamento, incluida la evolución de tecnologías que protejan mejor la intimidad;

b) las repercusiones del presente Reglamento en la utilización de datos en la economía, incluyendo la innovación en materia de datos, las prácticas de monetización de los datos y los servicios de intermediación de datos, así como en el intercambio de datos dentro de los espacios comunes europeos de datos;

c) la accesibilidad a diferentes categorías y tipos de datos y su utilización;

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

e) la ausencia de cualquier impacto en los derechos de propiedad intelectual;

f) el impacto en los secretos comerciales, incluida la protección contra su obtención, utilización y revelación ilícitas, así como el impacto del mecanismo que permite al titular de datos denegar la solicitud del usuario con arreglo al artículo 4, apartado 8, y al artículo 5, apartado 11, teniendo en cuenta, en la medida de lo posible, cualquier revisión de la Directiva (UE) 2016/943;

g) si la lista de cláusulas contractuales abusivas a que se refiere el artículo 13 está actualizada a la luz de las nuevas prácticas comerciales y del rápido ritmo de innovación del mercado;

h) las variaciones en las prácticas contractuales de los proveedores de servicios de tratamiento de datos y si esas variaciones se traducen en un cumplimiento suficiente del artículo 25;

i) la reducción de los costes añadidos aplicados por los proveedores de servicios de tratamiento de datos por el proceso de cambio, en consonancia con la supresión gradual de esos costes de conformidad con el artículo 29;

j) la interacción del presente Reglamento con otros actos jurídicos de la Unión pertinentes para la economía de los datos;

k) la prevención del acceso ilícito a datos no personales por parte de administraciones públicas;

l) la eficacia del régimen de ejecución exigido en virtud del artículo 37;

m) las repercusiones del presente Reglamento en las pymes, por lo que respecta a su capacidad para innovar y a la disponibilidad de servicios de tratamiento de datos para los usuarios en la Unión y la carga del cumplimiento de las nuevas obligaciones.

2. A más tardar el 12 de septiembre de 2028, 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. Dicha evaluación valorará el impacto de los artículos 23 a 31 y de los artículos 34 y 35, en particular, en lo que respecta a la fijación de precios y la diversidad de los servicios de tratamiento de datos ofrecidos en la Unión, prestando especial atención a las pymes proveedoras.

3. Los Estados miembros proporcionarán a la Comisión la información necesaria para la preparación de los informes a que se refieren los apartados 1 y 2.

4. Sobre la base de los informes a que se refieren los apartados 1 y 2, la Comisión podrá presentar, en su caso, una propuesta legislativa al Parlamento Europeo y al Consejo para modificar el presente Reglamento.

Artículo 50

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 12 de septiembre de 2025.

La obligación derivada del artículo 3, apartado 1, será aplicable a los productos conectados y a los servicios relacionados con ellos introducidos en el mercado después del 12 de septiembre de 2026.

El capítulo III será aplicable en relación con las obligaciones de puesta a disposición de los datos en virtud de disposiciones del Derecho de la Unión o de normativa nacional adoptada de conformidad con el Derecho de la Unión que entren en vigor después del 12 de septiembre de 2025.

El capítulo IV será aplicable a los contratos celebrados después del 12 de septiembre de 2025.

El capítulo IV será aplicable a partir del 12 de septiembre de 2027 a los contratos celebrados el 12 de septiembre de 2025 o con anterioridad, siempre que:

a) sean de duración indefinida, o

b) expiren al menos diez años a partir del 11 de enero de 2024.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Estrasburgo, el 13 de diciembre de 2023.

Por el Parlamento Europeo	*Por el Consejo*
La Presidenta	*El Presidente*
R. METSOLA	P. NAVARRO RÍOS