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

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

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

Vista la propuesta de la Comisión Europea,

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

Visto el dictamen del Comité Económico y Social Europeo ([1]),

Previa consulta al Comité de las Regiones,

De conformidad con el procedimiento legislativo ordinario ([2]),

Considerando lo siguiente:

(1) La digitalización de la economía se está acelerando. Las tecnologías de la información y la comunicación ya no son un sector específico sino el fundamento de todos los sistemas económicos y sociedades innovadores modernos. Los datos electrónicos se encuentran en el centro de esos sistemas y pueden generar un gran valor cuando se analizan o combinan con servicios y productos. Al mismo tiempo, el rápido desarrollo de la economía de los datos y las tecnologías emergentes, como la inteligencia artificial, productos y servicios del «internet de las cosas», sistemas autónomos y la tecnología 5G, están planteando problemas jurídicos nuevos en torno a las cuestiones del acceso a los datos y su reutilización, la responsabilidad, la ética y la solidaridad. Se debería considerar trabajar el ámbito de la responsabilidad, en particular mediante la aplicación de códigos de autorregulación y otras buenas prácticas, teniendo en cuenta recomendaciones, decisiones y acciones adoptadas sin interacción humana a lo largo de toda la cadena de valor del tratamiento de datos. Ese trabajo también puede incluir mecanismos adecuados para la determinación de responsabilidad, la transmisión de responsabilidad entre servicios complementarios, los seguros y la auditoría.

(2) Las cadenas de valor de datos se basan en diferentes actividades relativas a los datos: creación y recopilación de datos; agregación y organización de datos; tratamiento de datos; análisis, comercialización y distribución de datos; utilización y reutilización de datos. El funcionamiento eficaz y eficiente del tratamiento de datos es un componente fundamental en toda la cadena de valor de datos. No obstante, el funcionamiento eficaz y eficiente del tratamiento de datos y el desarrollo de la economía de los datos en la Unión se ven dificultados, en particular, por dos tipos de obstáculos a la movilidad de los datos y al mercado interior: los requisitos de localización de datos establecidos por las autoridades de los Estados miembros y las prácticas de dependencia de un solo proveedor en el sector privado.

(3) La libertad de establecimiento y la libre prestación de servicios en virtud del Tratado de Funcionamiento de la Unión Europea (TFUE) se aplican a los servicios de tratamiento de datos. No obstante, la prestación de tales servicios se ve dificultada o en algunas ocasiones impedida por determinados requisitos nacionales, regionales o locales que exigen que los datos se localicen en un territorio específico.

(4) Tales obstáculos a la libre circulación de servicios de tratamiento de datos y a la libertad de establecimiento de los proveedores de servicios tienen su origen en los requisitos establecidos en la legislación de los Estados miembros para que los datos se localicen en una zona o territorio geográfico específico a efectos del tratamiento de datos. Otras normas o prácticas administrativas tienen un efecto equivalente mediante la imposición de requisitos específicos que hacen más difícil tratar los datos fuera de una zona o territorio geográfico específico dentro de la Unión, como los requisitos para utilizar instalaciones tecnológicas certificadas o aprobadas en un determinado Estado miembro. La inseguridad jurídica en cuanto al alcance de los requisitos legítimos e ilegítimos en materia de localización de datos limita aún más las opciones a disposición de los agentes del mercado y del sector público relativas a la localización del tratamiento de datos. El presente Reglamento no limita de forma alguna la libertad de las empresas para celebrar contratos en los que se especifique dónde deben localizarse los datos. Su finalidad es simplemente preservar esa libertad garantizando que la localización acordada pueda situarse en cualquier lugar de la Unión.

([1]) DO C 227 de 28.6.2018, p. 78.
([2]) Posición del Parlamento Europeo de 4 de octubre de 2018 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 6 de noviembre de 2018.

(5) Al mismo tiempo, la movilidad de los datos en la Unión también está inhibida por restricciones privadas: cuestiones jurídicas, contractuales y técnicas que obstaculizan o impiden a los usuarios de los servicios de tratamiento de datos trasladar sus datos de un proveedor de servicios a otro o a sus propios sistemas informáticos, especialmente en el momento en que finalice su contrato con un proveedor de servicios.

(6) La combinación de esos obstáculos ha generado una falta de competencia entre los proveedores de servicios en nube en la Unión, diversos problemas de dependencia de un solo proveedor y una grave falta de movilidad de los datos. Asimismo, las políticas de localización de datos han menoscabado la capacidad de las empresas de investigación y desarrollo para facilitar la colaboración entre empresas, universidades y otras organizaciones dedicadas a la investigación con el fin de impulsar la innovación.

(7) La existencia de un conjunto único de normas para todos los participantes en el mercado constituye un elemento clave del funcionamiento del mercado interior por motivos de seguridad jurídica y por la necesidad de que exista una igualdad de condiciones en la Unión. Con objeto de eliminar obstáculos al comercio y distorsiones de la competencia como consecuencia de las divergencias existentes entre las normativas nacionales, e impedir el surgimiento de otros probables obstáculos al comercio e importantes distorsiones de la competencia, es necesario adoptar normas uniformes aplicables en todos los Estados miembros.

(8) El marco jurídico relativo a la protección de las personas físicas en lo que atañe al tratamiento de datos personales y el relativo al respeto de la vida privada y a la protección de los datos personales en las comunicaciones electrónicas, y en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([1]), y las Directivas (UE) 2016/680 ([2]) y 2002/58/CE ([3]) del Parlamento Europeo y del Consejo, no se ven afectados por el presente Reglamento.

(9) La expansión del «internet de las cosas», la inteligencia artificial y el aprendizaje automático representan las principales fuentes de datos no personales, por ejemplo como resultado de su despliegue en procesos de producción industrial automatizada. Entre los ejemplos específicos de datos no personales se encuentran los conjuntos de datos agregados y anonimizados utilizados para análisis de datos a gran escala, los datos sobre agricultura de precisión que pueden ayudar a controlar y optimizar la utilización de plaguicidas y de agua, o los datos sobre las necesidades de mantenimiento de máquinas industriales. Si los avances tecnológicos hicieran posible transformar datos anónimos en datos personales, dichos datos se deben tratar como datos personales y, en consecuencia, se debe aplicar el Reglamento (UE) 2016/679.

(10) En virtud del Reglamento (UE) 2016/679, los Estados miembros no pueden restringir ni prohibir la libre circulación de datos personales en la Unión por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. El presente Reglamento establece el mismo principio de libre circulación en la Unión de datos no personales salvo cuando una restricción o prohibición se justifique por razones de seguridad pública. El Reglamento (UE) 2016/679 y el presente Reglamento ofrecen una serie de normas coherentes que prevén la libre circulación de diferentes tipos de datos. Por otro lado, el presente Reglamento no impone la obligación de almacenar los distintos tipos de datos de forma separada.

(11) A fin de crear un marco para la libre circulación de datos no personales en la Unión y las bases para desarrollar la economía de los datos y mejorar la competitividad de la industria de la Unión, es necesario instaurar un marco jurídico claro, exhaustivo y previsible para el tratamiento de datos que no tengan carácter personal en el mercado interior. Un enfoque basado en principios que facilite la cooperación entre los Estados miembros, así como la autorregulación, debe garantizar que el marco sea lo suficientemente flexible para tener en cuenta las necesidades cambiantes de los usuarios, proveedores de servicios y autoridades nacionales en la Unión. Para evitar el riesgo de solapamientos con los mecanismos existentes, de modo que se eviten cargas más onerosas tanto para los Estados miembros como para las empresas, no deben establecerse normas técnicas detalladas.

(12) El presente Reglamento no debe afectar al tratamiento de los datos en la medida en que se efectúe como parte de una actividad que no entre en el ámbito de aplicación del Derecho de la Unión. En particular, procede recordar que, de conformidad con el artículo 4 del Tratado de la Unión Europea (en lo sucesivo, «TUE»), la seguridad nacional es responsabilidad exclusiva de cada Estado miembro.

([1]) 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).

([2]) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89).

([3]) 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).

(13) La libre circulación de datos en la Unión va a desempeñar un papel importante para alcanzar un crecimiento y una innovación basados en datos. Como sucede con las empresas y los consumidores, las autoridades y organismos de Derecho público de los Estados miembros pueden beneficiarse de una mayor libertad de elección en lo relativo a los proveedores de servicios basados en datos, precios más competitivos y una prestación de servicios a los ciudadanos más eficiente. Habida cuenta de las grandes cantidades de datos que gestionan las autoridades y organismos de Derecho público, resulta de vital importancia que prediquen con el ejemplo en la implantación de servicios de tratamiento de datos, y que se abstengan de imponer restricciones en materia de localización de datos cuando hagan uso de servicios de tratamiento de datos. Por consiguiente, el presente Reglamento se aplica a las autoridades y organismos de Derecho público. A este respecto, el principio de libre circulación de datos no personales contemplado en el presente Reglamento también se debe aplicar a prácticas administrativas generales y coherentes y a otros requisitos de localización de datos en el ámbito de la contratación pública, sin perjuicio de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo ([1]).

(14) Como en el caso de la Directiva 2014/24/UE, el presente Reglamento se entiende sin perjuicio de disposiciones legales, reglamentarias y administrativas relativas a la organización interna de los Estados miembros por las que se atribuyan a autoridades u organismos de Derecho público competencias o responsabilidades para el tratamiento de datos sin remuneración contractual de personas o entidades privadas, así como disposiciones legales, reglamentarias y administrativas de los Estados miembros que establecen la aplicación de esas competencias o responsabilidades. Si bien se anima a las autoridades y organismos públicos a considerar las ventajas económicas o de otra índole de contratar proveedores de servicios externos, pueden tener razones legítimas para decidir la autoprestación de dichos servicios o su encomienda a otro organismo del sector público. En consecuencia, nada en el presente Reglamento obliga a los Estados miembros a contratar o externalizar la prestación de servicios que deseen prestar ellos mismos u organizar por medios distintos de contratos públicos.

(15) El presente Reglamento debe aplicarse a las personas físicas o jurídicas que presten servicios de tratamiento de datos a usuarios que residan o tengan un establecimiento en la Unión, incluidas aquellas que presten servicios de tratamiento de datos en la Unión sin tener un establecimiento en esta. El presente Reglamento no se aplicará, por tanto, al servicio de tratamiento de datos que tenga lugar fuera de la Unión ni a los requisitos de localización relativos a esos datos.

(16) El presente Reglamento no establece normas relativas a la determinación de la ley aplicable en materia mercantil y, por tanto, se entiende sin perjuicio del Reglamento (CE) n.º 593/2008 del Parlamento Europeo y del Consejo ([2]). En particular, en la medida en que la ley aplicable a un contrato no se haya elegido de conformidad con dicho Reglamento, un contrato de prestación de servicios se rige, en principio, por la ley del país de residencia habitual del prestador del servicio.

(17) El presente Reglamento debe aplicarse al tratamiento de datos en sentido amplio, abarcando el uso de todo tipo de sistemas informáticos, tanto si están situados en las instalaciones del usuario como si están externalizados a un proveedor de servicios. Debe incluir el tratamiento de datos de distintos grados de intensidad, desde el almacenamiento de datos [infraestructura como servicio (IaaS)] hasta el tratamiento de datos en plataforma [plataforma como servicio (PaaS)] o en aplicaciones [software como servicio (SaaS)].

(18) Los requisitos de localización de datos constituyen un claro obstáculo a la libre prestación de servicios de tratamiento de datos en la Unión y al mercado interior. Como tales, deben ser prohibidos a menos que estén justificados por motivos de seguridad pública, tal como los define el Derecho de la Unión, en particular en el sentido del artículo 52 del TFUE, y que respeten el principio de proporcionalidad establecido en el artículo 5 del TUE. Para dar efecto al principio de libre circulación de datos no personales a través de las fronteras, garantizar la rápida supresión de los actuales requisitos de localización de datos y permitir, por razones operativas, el tratamiento de datos en múltiples lugares en la Unión, y dado que el presente Reglamento establece medidas para garantizar la disponibilidad de los datos para fines de control normativo, los Estados miembros solo han de poder invocar la seguridad pública como justificación de los requisitos de localización de datos.

(19) El concepto de «seguridad pública», en el sentido del artículo 52 del TFUE y según la interpretación del Tribunal de Justicia, abarca la seguridad interna y externa de un Estado miembro, así como cuestiones de orden público, para, en particular, permitir la investigación, detección y enjuiciamiento de infracciones penales. Presupone la existencia de una amenaza real y suficientemente grave que afecte a uno de los intereses fundamentales de la sociedad, tales como una amenaza al funcionamiento de las instituciones y los servicios públicos esenciales y la supervivencia de la población, así como el riesgo de una perturbación grave de las relaciones exteriores o la coexistencia pacífica de las naciones, o un riesgo para los intereses militares. De conformidad con el principio de proporcionalidad, los requisitos de localización de datos justificados por motivos de seguridad pública deben ser adecuados al objetivo perseguido, y no deben ir más allá de lo que sea necesario para alcanzar dicho objetivo.

([1]) Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

([2]) Reglamento (CE) n.º 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I) (DO L 177 de 4.7.2008, p. 6).

(20) A fin de garantizar la aplicación efectiva del principio de libre circulación de datos no personales a través de las fronteras e impedir la aparición de nuevos obstáculos al buen funcionamiento del mercado interior, los Estados miembros deben comunicar inmediatamente a la Comisión cualquier proyecto de acto que introduzca un nuevo requisito de localización de datos o modifique un requisito existente. Estos proyectos de acto deben presentarse y valorarse de conformidad con la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo ([1]).

(21) Además, a fin de eliminar obstáculos que puedan existir, durante un período transitorio de veinticuatro meses a partir de la fecha de aplicación del presente Reglamento, los Estados miembros deben llevar a cabo una revisión de las disposiciones legales, reglamentarias o administrativas nacionales de carácter general vigentes por las que se establecen requisitos de localización de datos y comunicar a la Comisión los requisitos de localización de datos que consideren que cumplen lo dispuesto en el presente Reglamento, junto con una justificación. Esto debe permitir a la Comisión examinar el cumplimiento de los restantes requisitos de localización de datos. La Comisión debe poder formular observaciones al Estado miembro en cuestión. Dichas observaciones podrían incluir una recomendación para modificar o derogar el requisito de localización de datos.

(22) Las obligaciones establecidas en el presente Reglamento de comunicar a la Comisión los requisitos de localización de datos vigentes y los proyectos de acto se deben aplicar a los requisitos normativos de localización de datos y a los proyectos de acto de carácter general, pero no a las decisiones dirigidas a una persona física o jurídica específica.

(23) A fin de garantizar la transparencia de los requisitos de localización de datos en los Estados miembros establecida en una disposición legal, reglamentaria o administrativa de carácter general para las personas físicas y jurídicas, como los proveedores de servicios y los usuarios de los servicios de tratamiento de datos, los Estados miembros deben publicar información sobre dichos requisitos en un punto único nacional de información en línea sobre esas medidas y actualizar dicha información periódicamente. Como alternativa, los Estados miembros deben proporcionar información actualizada sobre tales requisitos a un punto central de información establecido en virtud de otro acto de la Unión. Con el fin de informar debidamente a las personas físicas y jurídicas de los requisitos de localización de datos en el conjunto de la Unión, los Estados miembros deben notificar a la Comisión las direcciones de dichos puntos únicos nacionales de información en línea. La Comisión debe publicar esta información en su propio sitio web, junto con una lista consolidada y actualizada periódicamente de todos los requisitos de localización de datos en vigor en los Estados miembros, incluida información resumida sobre dichos requisitos.

(24) Los requisitos de localización de datos a menudo se derivan de una falta de confianza en el tratamiento transfronterizo de datos, derivada de la supuesta indisponibilidad de datos para los fines de las autoridades competentes de los Estados miembros, como la inspección y la auditoría en el marco de un control normativo o de vigilancia. Esa falta de confianza no se puede superar únicamente a través de la nulidad de las condiciones contractuales que prohíban un acceso legítimo a los datos por parte de las autoridades competentes para el ejercicio de sus funciones oficiales. Por consiguiente, el presente Reglamento debe establecer claramente que no afecta a las competencias de las autoridades competentes de solicitar u obtener acceso a los datos de conformidad con el Derecho de la Unión o nacional, y que no se puede denegar el acceso a los datos a las autoridades competentes alegando que los datos se tratan en otro Estado miembro. Las autoridades competentes podrían imponer requisitos funcionales para apoyar el acceso a los datos, como exigir que las descripciones del sistema se guarden en el Estado miembro en cuestión.

(25) Las personas físicas o jurídicas sujetas a la obligación de facilitar datos a las autoridades competentes pueden cumplir tales obligaciones proporcionando y garantizando el acceso electrónico efectivo y en tiempo oportuno a los datos a dichas autoridades, con independencia del Estado miembro en cuyo territorio los datos sean tratados. Este acceso puede garantizarse a través de cláusulas y condiciones concretas incluidas en los contratos entre la persona física o jurídica sujeta a la obligación de proporcionar el acceso y el proveedor de servicios.

(26) Cuando una persona física o jurídica esté sujeta a una obligación de facilitar datos e incumpla dicha obligación, la autoridad competente debe poder solicitar la asistencia de las autoridades competentes en otros Estados miembros. En tales casos, las autoridades competentes deben utilizar instrumentos de cooperación específicos de Derecho de la Unión o en virtud de convenios internacionales, en función del asunto en un caso concreto, como

([1]) Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

por ejemplo, en el ámbito de la cooperación policial, la justicia penal o civil o en asuntos administrativos, respectivamente, la Decisión Marco 2006/960/JAI del Consejo ([1]), la Directiva 2014/41/UE del Parlamento Europeo y del Consejo ([2]), el Convenio sobre la Ciberdelincuencia del Consejo de Europa ([3]), el Reglamento (CE) n.º 1206/2001 del Consejo ([4]), la Directiva 2006/112/CE del Consejo ([5]) y el Reglamento (UE) n.º 904/2010 del Consejo ([6]). En ausencia de tales mecanismos de cooperación específicos, las autoridades competentes deben cooperar entre ellas con el fin de proporcionar acceso a los datos solicitados, a través de puntos de contacto únicos designados.

(27) Cuando una solicitud de asistencia implique obtener el acceso a todos los locales de una persona física o jurídica, incluidos cualesquiera equipos y medios de tratamiento de datos, por la autoridad requerida, dicho acceso debe ajustarse al Derecho de la Unión o al Derecho procesal nacional, incluido cualquier requisito para obtener autorización judicial previa.

(28) El presente Reglamento no debe permitir a los usuarios intentar eludir la aplicación del Derecho nacional. Por tanto, procede disponer que los Estados miembros impongan sanciones efectivas, proporcionadas y disuasorias a los usuarios que impidan a las autoridades competentes obtener el acceso a sus datos necesarios para el ejercicio de las funciones oficiales de dichas autoridades en virtud del Derecho de la Unión y nacional. En casos de urgencia, cuando un usuario abuse de su derecho, los Estados miembros han de poder imponer medidas provisionales estrictamente proporcionadas. Toda medida provisional que exija la relocalización de los datos por un período superior a 180 días a partir de la relocalización se apartaría del principio de libre circulación de datos por un período importante y, en consecuencia, se debe comunicar a la Comisión para examinar su compatibilidad con el Derecho de la Unión.

(29) La capacidad para trasladar datos sin trabas es un factor clave que favorece las posibilidades de elección de los usuarios y la competencia efectiva en los mercados de servicios de tratamiento de datos. Las dificultades reales o percibidas para la portabilidad de datos a través de las fronteras también socavan la confianza de los usuarios profesionales en las ofertas transfronterizas y, por tanto, su confianza en el mercado interior. Mientras que los consumidores particulares se benefician del Derecho vigente de la Unión, la capacidad de cambiar de un proveedor de servicios a otro no se facilita a aquellos usuarios que actúan en el marco de sus actividades empresariales o profesionales. Unos requisitos técnicos coherentes en toda la Unión, ya sea en lo referente a una armonización técnica, al reconocimiento mutuo o a una armonización voluntaria, también contribuyen al desarrollo de un mercado interior competitivo de servicios de tratamiento de datos.

(30) Para gozar plenamente de las ventajas del entorno competitivo, los usuarios profesionales deben poder tomar decisiones con conocimiento de causa y comparar fácilmente los componentes individuales de diferentes servicios de tratamiento de datos ofrecidos en el mercado interior, en particular en lo que atañe a las cláusulas y condiciones contractuales de la portabilidad de datos al finalizar un contrato. Con el fin de adaptarse al potencial innovador del mercado y tener en cuenta la experiencia y la competencia de los proveedores de servicios y usuarios profesionales de servicios de tratamiento de datos, la información detallada y los requisitos operativos para la portabilidad de datos deben ser definidos por los agentes del mercado a través de la autorregulación, fomentada, facilitada y supervisada por la Comisión, en forma de códigos de conducta de la Unión que pueden incluir y cláusulas y condiciones contractuales tipo.

(31) Para que sea eficaz y hacer más fácil el cambio de proveedor de servicios y la portabilidad de datos, dichos códigos de conducta deben ser detallados y tratar al menos los aspectos clave que son importantes durante el proceso de traslado de los datos, como son los procedimientos utilizados para efectuar copias de seguridad de los datos o la ubicación de dichas copias, los formatos y soportes de datos disponibles, la configuración informática necesaria y el ancho de banda mínimo, el tiempo necesario antes de iniciar el proceso de traslado y el tiempo durante el cual los datos van a seguir estando disponibles para su traslado y las garantías de acceso a los datos en caso de quiebra del proveedor del servicio. Los códigos de conducta también deben aclarar que la dependencia de un solo proveedor no es una práctica comercial aceptable, deben prever tecnologías que aumenten la confianza y deben actualizarse periódicamente para seguir la evolución tecnológica. La Comisión debe asegurarse que durante el proceso se consulte a todos los interesados, incluidas las asociaciones de pequeñas y medianas empresas (en lo sucesivo, «pymes»), las empresas emergentes, los usuarios y proveedores de servicios en nube. La Comisión debe evaluar el desarrollo y la eficacia de la aplicación de tales códigos de conducta.

([1]) Decisión marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea (DO L 386 de 29.12.2006, p. 89).

([2]) Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal (DO L 130 de 1.5.2014, p. 1).

([3]) Convenio sobre la Ciberdelincuencia del Consejo de Europa, STCE n.º 185.

([4]) Reglamento (CE) n.º 1206/2001 del Consejo, de 28 de mayo de 2001, relativo a la cooperación entre los órganos jurisdiccionales de los Estados miembros en el ámbito de la obtención de pruebas en materia civil o mercantil (DO L 174 de 27.6.2001, p. 1).

([5]) Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido (DO L 347 de 11.12.2006, p. 1).

([6]) Reglamento (UE) n.º 904/2010 del Consejo, de 7 de octubre de 2010, relativo a la cooperación administrativa y la lucha contra el fraude en el ámbito del impuesto sobre el valor añadido (DO L 268 de 12.10.2010, p. 1).

(32) Cuando una autoridad competente de un Estado miembro solicite la asistencia de otro Estado miembro para obtener acceso a los datos conforme al presente Reglamento, debe presentar, a través del punto de contacto único designado, una solicitud debidamente motivada al punto de contacto único designado de este último, incluida una explicación por escrito de los motivos y los fundamentos jurídicos para solicitar el acceso a los datos. El punto de contacto único designado por el Estado miembro cuya asistencia se solicita debe facilitar la transmisión de la solicitud a la autoridad competente en el Estado miembro requerido. Para garantizar una cooperación eficaz, la autoridad a la que se transmite una solicitud debe prestar asistencia sin demora indebida en respuesta a una solicitud determinada o facilitar información sobre las dificultades experimentadas al cumplimentar dicha solicitud o sobre sus motivos para denegarla.

(33) Aumentar la confianza en la seguridad del tratamiento de datos transfronterizo debe reducir la propensión de los agentes del mercado y del sector público a utilizar la localización de datos como un indicador para la seguridad de estos. También debe mejorar la seguridad jurídica para las empresas en lo referente al cumplimiento de los requisitos de seguridad aplicables cuando externalizan sus actividades de tratamiento de datos a proveedores de servicios, incluidos los de otros Estados miembros.

(34) Cualesquiera requisitos de seguridad relacionados con el tratamiento de datos que se apliquen de forma justificada y proporcionada sobre la base del Derecho de la Unión o nacional de conformidad con el Derecho de la Unión en el Estado miembro de residencia o establecimiento de las personas físicas o jurídicas cuyos datos se vean afectados deben seguir aplicándose al tratamiento de dichos datos en otro Estado miembro. Estas personas físicas o jurídicas deben poder cumplir tales requisitos por sí mismos o a través de cláusulas contractuales en los contratos con los proveedores de servicios.

(35) Los requisitos de seguridad establecidos a nivel nacional deben ser necesarios y proporcionados respecto de los riesgos que se planteen para la seguridad del tratamiento de datos en el ámbito de aplicación del Derecho nacional en el que se establezcan tales requisitos.

(36) La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo [1] prevé medidas jurídicas para incrementar el nivel general de ciberseguridad en la Unión. Los servicios de tratamiento de datos constituyen uno de los servicios digitales a los que se aplica dicha Directiva. Según dicha Directiva, los Estados miembros deben velar por que los proveedores de servicios digitales determinen y adopten medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos existentes para la seguridad de las redes y los sistemas de información que utilizan. Tales medidas deben garantizar un nivel de seguridad adecuado en relación con el riesgo planteado, y deben tener en cuenta la seguridad de los sistemas e instalaciones, la gestión de incidentes, la gestión de la continuidad de las actividades, la supervisión, auditorías y pruebas, y el cumplimiento de las normas internacionales. Estos elementos se deben especificar en mayor medida por la Comisión en actos de ejecución en virtud de dicha Directiva.

(37) La Comisión debe presentar un informe sobre la aplicación del presente Reglamento, en particular con vistas a determinar si es preciso modificarlo a la luz de los avances tecnológicos o de la evolución del mercado. Ese informe debe, en particular, evaluar el presente Reglamento, especialmente su aplicación a los conjuntos de datos compuestos tanto por datos personales como no personales, así como la aplicación de la excepción de seguridad pública. Antes de que el presente Reglamento se empiece a aplicar, la Comisión debe asimismo publicar orientaciones informativas sobre el modo de tratar los conjuntos de datos compuestos tanto por datos personales como no personales, para que las empresas, incluidas las pymes, comprendan mejor la interacción entre el presente Reglamento y el Reglamento (UE) 2016/679, y garantizar que se cumplan ambos Reglamentos.

(38) El presente Reglamento respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea, y debe interpretarse y aplicarse de conformidad con dichos derechos y principios, en particular el derecho a la protección de datos de carácter personal, la libertad de expresión y de información y la libertad de empresa.

(39) Dado que el objetivo del presente Reglamento, a saber, garantizar la libre circulación de datos que no tengan carácter personal en la Unión, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a sus dimensiones y efectos, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

---

[1] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Objeto

El presente Reglamento tiene por objeto garantizar la libre circulación en la Unión de datos que no tengan carácter personal mediante el establecimiento de normas relativas a los requisitos de localización de datos, la disponibilidad de los datos para las autoridades competentes y la portabilidad de datos para los usuarios profesionales.

Artículo 2

Ámbito de aplicación

1. El presente Reglamento se aplica al tratamiento en la Unión de datos electrónicos que no tengan carácter personal, que:

a) se preste como un servicio a usuarios que residan o tengan un establecimiento en la Unión, independientemente de si el proveedor de servicios está establecido o no en la Unión, o

b) efectuado por una persona física o jurídica que resida o tenga un establecimiento en la Unión para sus propias necesidades.

2. En el caso de un conjunto de datos compuesto por datos personales y no personales, el presente Reglamento se aplicará a los datos no personales del conjunto de datos. Cuando los datos personales y los no personales de un conjunto de datos estén inextricablemente ligados, el presente Reglamento se aplicará sin perjuicio del Reglamento (UE) 2016/679.

3. El presente Reglamento no se aplica a las actividades que no entren en el ámbito de aplicación del Derecho de la Unión.

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

Artículo 3

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «datos»: los datos que no sean datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679;

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

3) «proyecto de acto»: un texto redactado con el objetivo de que se convierta en una disposición legal, reglamentaria o administrativa de carácter general, que se encuentre en una fase de elaboración que permita aún efectuar modificaciones de fondo;

4) «proveedor de servicios»: toda persona física o jurídica que preste servicios de tratamiento de datos;

5) «requisito de localización de datos»: cualquier obligación, prohibición, condición, restricción u otro requisito previsto en las disposiciones legales, reglamentarias o administrativas de los Estados miembros o que se derive de prácticas administrativas generales y coherentes en un Estado miembro y en organismos de Derecho público, también en el ámbito de la contratación pública sin perjuicio de la Directiva 2014/24/UE, que imponga el tratamiento de datos en el territorio de un determinado Estado miembro o dificulte el tratamiento de datos en cualquier otro Estado miembro;

6) «autoridad competente»: una autoridad de un Estado miembro, o cualquier otra entidad autorizada por el Derecho nacional para desempeñar una función pública o ejercer el poder público, que tiene la facultad de obtener acceso a datos tratados por una persona física o jurídica para el ejercicio de sus funciones oficiales, conforme a lo previsto en el Derecho de la Unión o nacional;

7) «usuario»: una persona física o jurídica, incluidas las autoridades y organismos de Derecho público, que utiliza o solicita un servicio de tratamiento de datos;

8) «usuario profesional»: una persona física o jurídica, incluidas las autoridades y organismos de Derecho público, que utiliza o solicita un servicio de tratamiento de datos para fines relacionados con su actividad comercial, negocio, oficio, profesión o función.

Artículo 4

Libre circulación de datos en la Unión

1. Los requisitos para la localización de datos estarán prohibidos, salvo que estén justificados por razones de seguridad pública de conformidad con el principio de proporcionalidad.

El párrafo primero del presente apartado no afecta a la aplicación del apartado 3 ni a los requisitos de localización de datos establecidos sobre la base del Derecho vigente de la Unión.

2. Los Estados miembros comunicarán inmediatamente a la Comisión cualquier proyecto de acto que introduzca un nuevo requisito de localización de datos o modifique uno existente, de conformidad con los procedimientos establecidos en los artículos 5, 6 y 7 de la Directiva (UE) 2015/1535.

3. A más tardar el 30 de mayo de 2021, los Estados miembros velarán por que se derogue cualquier requisito existente de localización de datos establecido en disposiciones legales, reglamentarias o administrativas que no se ajuste a lo dispuesto en el apartado 1 del presente artículo.

A más tardar el 30 de mayo de 2021, si un Estado miembro considera que una disposición vigente que contenga un requisito de localización de datos cumple lo dispuesto en el apartado 1 del presente artículo y, por lo tanto, puede seguir en vigor, comunicará dicha disposición a la Comisión, junto con una justificación para mantenerla en vigor. Sin perjuicio de lo dispuesto en el artículo 258 del TFUE y en el plazo de seis meses a partir de la fecha de recepción de dicha comunicación, la Comisión examinará que dicha disposición cumpla con el apartado 1 del presente artículo y, en su caso, formulará observaciones al Estado miembro en cuestión, incluida, cuando sea necesario, la recomendación de modificar o derogar la disposición.

4. Los Estados miembros pondrán a disposición del público, a través de un punto único nacional de información en línea, información sobre todo requisito de localización de datos establecido en disposiciones legales, reglamentarias o administrativas de carácter general y aplicable en su territorio, que mantendrán actualizada, o proporcionarán información actualizada sobre tales requisitos de localización a un punto de información central establecido en virtud de otro acto de la Unión.

5. Los Estados miembros informarán a la Comisión sobre la dirección de sus puntos únicos de información a que se refiere el apartado 4. La Comisión publicará los enlaces a dichos puntos en su sitio web, junto con una lista consolidada y actualizada periódicamente de todos los requisitos de localización de datos a que se refiere el apartado 4, incluida información resumida sobre dichos requisitos.

Artículo 5

Disponibilidad de datos para las autoridades competentes

1. El presente Reglamento no afectará a las competencias de las autoridades competentes de solicitar u obtener acceso a los datos para el desempeño de sus funciones oficiales de conformidad con el Derecho de la Unión o nacional. No podrá denegarse a las autoridades competentes el acceso a los datos alegando que son objeto de tratamiento en otro Estado miembro.

2. Cuando, tras una petición de acceso a los datos de un usuario, una autoridad competente no obtenga el acceso y no exista un mecanismo específico de cooperación en virtud del Derecho de la Unión o de convenios internacionales para el intercambio de datos entre autoridades competentes de diferentes Estados miembros, dicha autoridad competente podrá solicitar asistencia de una autoridad competente de otro Estado miembro, de conformidad con el procedimiento establecido en el artículo 7.

3. Cuando una solicitud de asistencia implique obtener acceso a todos los locales de una persona física o jurídica, incluidos cualesquiera equipos y medios de tratamiento de datos, por la autoridad requerida, dicho acceso debe ser conforme al Derecho de la Unión o al Derecho procesal del Estado miembro.

4. Los Estados miembros podrán imponer sanciones efectivas, proporcionadas y disuasorias por incumplimiento de una obligación de proporcionar datos, de conformidad con el Derecho de la Unión y nacional.

En caso de abuso de derechos por parte de un usuario, un Estado miembro podrá, cuando esté justificado por la urgencia de acceder a los datos y de tener en cuenta los intereses de los afectados, imponer medidas provisionales estrictamente proporcionadas a dicho usuario. Si una medida provisional impone la relocalización de los datos por una duración superior a 180 días a partir de la relocalización, se comunicará a la Comisión dentro del plazo de esos 180 días. La Comisión, en el plazo más breve posible, examinará la medida y su compatibilidad con el Derecho de la Unión y, en su caso, adoptará las medidas necesarias. La Comisión intercambiará información con los puntos de contacto únicos de los Estados miembros a que se refiere el artículo 7 sobre la experiencia adquirida a este respecto.

Artículo 6

Portabilidad de datos

1. La Comisión fomentará y facilitará la elaboración de códigos de conducta autorreguladores a escala de la Unión (en lo sucesivo, «códigos de conducta»), con el fin de contribuir a una economía de datos competitiva, basada en los principios de transparencia e interoperabilidad, que tenga debidamente en cuenta estándares abiertos y que incluya, entre otros, los siguientes aspectos:

a) las mejores prácticas para facilitar el cambio de proveedores de servicios y la portabilidad en un formato estructurado, de uso común y de lectura automática, incluidos formatos basados en estándares abiertos cuando lo exija o solicite el proveedor de servicios que reciba los datos;

b) los requisitos de información mínimos para garantizar que los usuarios profesionales, antes de celebrar un contrato de tratamiento de datos, reciban información suficientemente detallada, clara y transparente relativa a los procedimientos, los requisitos técnicos, los plazos y los costes aplicables en caso de que un usuario profesional desee cambiar de proveedor de servicios o transferir sus datos a sus propios sistemas informáticos;

c) los enfoques de regímenes de certificación que faciliten la comparación de los productos y servicios de tratamiento de datos para usuarios profesionales, teniendo en cuenta las normas nacionales o internacionales establecidas, que facilitan la comparabilidad de estos productos y servicios. Dichos enfoques podrán incluir, entre otros, la gestión de la calidad, la gestión de la seguridad de la información, la gestión de la continuidad de negocio y la gestión medioambiental;

d) los planes de comunicación que adopten un enfoque multidisciplinar para concienciar a los interesados sobre el código de conducta.

2. La Comisión garantizará que los códigos de conducta se elaboren en estrecha cooperación con todos los interesados, incluidas las asociaciones de pymes y empresas emergentes, los usuarios y los proveedores de servicios en nube.

3. La Comisión alentará a los proveedores de servicios a completar el desarrollo de los códigos de conducta a más tardar el 29 de noviembre de 2019 y a aplicarlos efectivamente a más tardar el 29 de mayo de 2020.

Artículo 7

Procedimiento de cooperación entre autoridades

1. Cada Estado miembro designará un punto de contacto único que actuará de enlace con los puntos de contacto únicos de los demás Estados miembros y la Comisión en cuanto a la aplicación del presente Reglamento. Los Estados miembros notificarán a la Comisión los puntos de contacto únicos designados y cualquier modificación posterior de estos.

2. Cuando una autoridad competente de un Estado miembro solicite la asistencia de otro Estado miembro conforme al artículo 5, apartado 2, para obtener acceso a datos, formulará una solicitud debidamente motivada al punto de contacto único designado. La solicitud incluirá una explicación por escrito de los motivos y los fundamentos jurídicos para solicitar el acceso a los datos.

3. El punto de contacto único identificará a la autoridad competente de su Estado miembro y remitirá la solicitud recibida con arreglo al apartado 2 a dicha autoridad competente.

4. La autoridad competente requerida, sin demora injustificada y dentro de un plazo proporcionado en relación con la urgencia de la solicitud, proporcionará una respuesta en la que comunique los datos solicitados o informe a la autoridad competente solicitante de que no considera que se reúnan las condiciones para solicitar asistencia al amparo del presente Reglamento.

5. Toda la información intercambiada en el contexto de la asistencia solicitada y facilitada en virtud del artículo 5, apartado 2, se utilizará únicamente en relación con el asunto para el que se solicitó.

6. Los puntos de contacto únicos proporcionarán a los usuarios información general sobre el presente Reglamento, incluida información sobre los códigos de conducta.

Artículo 8

Evaluación y orientaciones

1. A más tardar el 29 de noviembre de 2022, la Comisión presentará un informe al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo en el que evalúe la aplicación del presente Reglamento, en particular respecto a:

a) la aplicación del presente Reglamento, en especial a los conjuntos de datos compuestos tanto por datos personales como no personales a la luz de la evolución del mercado y los avances tecnológicos que puedan ampliar las posibilidades para la desanonimización de datos;

b) la aplicación del artículo 4, apartado 1, por parte de los Estados miembros, en particular la excepción de seguridad pública; y

c) la elaboración y la aplicación efectiva de los códigos de conducta y el suministro efectivo de información por parte de los proveedores de servicios.

2. Los Estados miembros facilitarán a la Comisión toda la información necesaria para la preparación del informe a que se refiere el apartado 1.

3. A más tardar el 29 de mayo de 2019, la Comisión publicará orientaciones informativas sobre la interacción del presente Reglamento y el Reglamento (UE) 2016/679, en particular en lo que se refiere a los conjuntos de datos compuestos tanto por datos personales como no personales.

Artículo 9

Disposiciones finales

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

El presente Reglamento se aplicará seis meses después de su publicación.

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

Hecho en Estrasburgo, el 14 de noviembre de 2018.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*La Presidenta*
A. TAJANI	K. EDTSTADLER