PREGUNTAS FRECUENTES

1. REGLAMENTO (UE) 2018/1807. DATOS NO PERSONALES.

¿Cuál es el objetivo del Reglamento de libre circulación de datos no personales?

El Reglamento (UE) 2018/1807, del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea (conocido como "*Free Flow of non-personal Data*", o "*FFoD"*) tiene por objeto garantizar:

1. 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
2. La disponibilidad de los datos para las autoridades competentes
3. La portabilidad de datos para los usuarios profesionales.

¿Por qué es necesario un Reglamento de libre circulación de datos no personales?

Es imprescindible permitir la libre circulación de datos no personales, de forma que se constituya en uno de los pilares fundamentales para la consecución del Mercado Único Digital, y contribuya al desarrollo del potencial de la "economía de los datos".

¿Qué son los datos no personales?

Los datos electrónicos de carácter no personal se refieren a información que no puede ser asociada a una persona física identificada o identificable.

En consecuencia, el «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.

Típicamente, estos enormes conjuntos de datos no personales se almacenan y procesan a través de proveedores de servicios de nube o *cloud*.

¿Cuál es el ámbito de aplicación del Reglamento?

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

¿Existe ya la libre circulación de datos electrónicos en la UE?

En virtud del Reglamento (UE) 2016/679, General de Protección de Datos, 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.

Por su parte, el Reglamento (UE) 2018/1807 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.

En consecuencia, 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, de forma que se consigue implantar la quinta libertad de movimiento en la UE, tras personas, capitales, mercancías y servicios.

¿Cómo se han de tratar conjuntos mixtos de datos personales y no personales?

El Reglamento (UE) 2018/1807 no impone la obligación de almacenar los distintos tipos de datos de forma separada.

En el caso de un conjunto de datos compuesto por datos personales y no personales, el Reglamento (UE) 2018/1807 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.

Para proporcionar más claridad a las empresas sobre el tratamiento de datos transfronterizo, la Comisión Europea ha publicado unas Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos.

2. LIBRE CIRCULACIÓN DE DATOS NO PERSONALES

¿Cómo se garantiza la libre circulación de datos no personales?

El Reglamento prohíbe explícitamente que los Estados miembros de la Unión Europea establezcan requisitos de localización de datos en su normativa, salvo que estén justificados por razones de seguridad pública.

¿Qué es un requisito de localización de datos?

Es 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.

¿Hay alguna excepción a la prohibición de imponer requisitos de localización de datos?

Sí, únicamente se pueden imponer requisitos de localización que estén justificados por motivos de seguridad pública.

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.

¿Existe algún tipo de tratamiento de datos excluido del ámbito del Reglamento?

El Reglamento no afecta a tratamientos de datos que se efectúen como parte de una actividad que no entre en el ámbito de aplicación del Derecho de la Unión. En particular, de conformidad con el artículo 4 del Tratado de la Unión Europea, la seguridad nacional es responsabilidad exclusiva de cada Estado miembro

¿Afecta a la contratación pública?

Sí, también se aplica en el ámbito de la contratación pública, incluido a los encargos a medios propios personificados definidos en la Ley 9/2017, de Contratos del Sector Público. Los pliegos correspondientes a una licitación pública no pueden contener requisitos de localización de datos.

¿Es posible incluir requisitos o criterios técnicos objetivos de baja latencia o similares, en los pliegos de una licitación, cuando así lo requiera el objeto del contrato?

En consonancia con el Reglamento, los requisitos de baja latencia no pueden utilizarse como obstáculo para crear una restricción indirecta de localización de datos y cerrar el mercado a posibles licitadores de otros Estados miembros de la Unión Europea. Sin embargo, los requisitos técnicos y objetivos en pliegos, incluyendo los de baja latencia, cuando así estén justificados para la correcta prestación del servicio, no son contrarios al Reglamento.

¿Obliga a los organismos públicos a externalizar sus servicios informáticos?

No, los organismos públicos no están obligados a contratar o externalizar la prestación de servicios que deseen prestar ellos mismos u organizar por medios distintos de contratos públicos.

¿Cuál es el punto único de contacto nacional designado por España para la aplicación del Reglamento?

La Secretaría de Estado de Digitalización e Inteligencia Artificial. Las funciones que tendrá que cumplir son las definidas en los siguientes artículos del Reglamento:

> *Art. 4.3: "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"*
>
> *Art. 4.3: "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."

Art. 4.4 "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"

Art. 7.1 "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."

Art. 7.6 "Los puntos de contacto únicos proporcionarán a los usuarios información general sobre el presente Reglamento, incluida información sobre los códigos de conducta."

¿A qué organismo deben las Administraciones públicas notificar **nuevas** disposiciones legales o administrativas que contengan restricciones de localización de datos basadas en la excepción de seguridad pública?

Al Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, a través del procedimiento previsto en la Directiva (UE) 2015/1535, tal y como establece el Reglamento en su artículo 4.2:

"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."

Las nuevas disposiciones se notificarán al correo d83-189@maec.es de la Dirección General de Coordinación del Mercado Interior y otras Políticas Comunitarias.

¿A partir de qué momento comienza la obligación de notificación de las nuevas disposiciones que establezcan requisitos de localización?

A partir del 29 de mayo de 2019.

¿A qué organismo se deben notificar las disposiciones **vigentes** que contienen requisitos de localización que se pretende mantener sobre la excepción de seguridad pública?

En el caso de un Ministerio u organismo público dependiente o vinculado al mismo, la notificación se realizará a la Secretaría de Estado de Digitalización e Inteligencia Artificial, junto con la justificación correspondiente, a través del correo ffod@economia.gob.es

En el caso de una Comunidad Autónoma o una Entidad Local, la notificación se realizará a la Secretaría General de Coordinación Territorial del Ministerio de Política Territorial y Función Pública, a través del buzón asuntos.europeos@correo.gob.es, quien a su vez transmitirá a la Secretaría de Estado de Digitalización e Inteligencia Artificial para su remisión a la Comisión Europea.

¿Qué plazo se ha establecido para comunicar a la Comisión Europea las disposiciones vigentes que establecen requisitos de localización basados en la excepción de seguridad pública?

A más tardar, la Secretaría de Estado de Digitalización e Inteligencia Artificial comunicará a la Comisión Europea la lista de disposiciones que contienen requisitos de localización que se vayan a mantener en vigor, por estar amparadas en la excepción de seguridad pública, junto con las justificaciones correspondientes, el 30 de mayo de 2021.

¿Qué ha de ocurrir con aquellas disposiciones que contienen requisitos de localización que no se pueden mantener sobre la excepción de seguridad pública?

Las citadas disposiciones deben ser derogadas en todos aquellos aspectos que contravengan el Reglamento (UE) 2018/1807.

¿Qué ocurrirá con las disposiciones comunicadas por la Secretaría de Estado de Digitalización e Inteligencia Artificial a la Comisión Europea?

En el plazo de seis meses a partir de la fecha de recepción de la comunicación por parte de la Secretaría de Estado de Digitalización e Inteligencia Artificial, la Comisión examinará que dicha disposición se puede amparar en la excepción de seguridad pública y, en su caso, formulará observaciones al Estado miembro en cuestión, incluida, cuando sea necesario, la recomendación de modificar o derogar la disposición.

3. ACCESO A DATOS NO PERSONALES POR AUTORIDADES COMPETENTES

¿A qué se refiere el principio de disponibilidad de datos?

El principio de disponibilidad de datos para las autoridades competentes implica que los datos permanecen accesibles en el ejercicio de sus funciones de regulación y supervisión encomendadas a tales autoridades, de conformidad con el Derecho de la Unión o nacional, incluso cuando los datos se almacenen o procesen en otro Estado miembro de la UE.

En consecuencia, no podrá denegarse a las autoridades competentes el acceso a los datos alegando que son objeto de tratamiento en otro Estado miembro.

¿Cuál es el mecanismo de acceso transfronterizo a datos?

Por regla general, una autoridad competente deberá utilizar el mecanismo de cooperación entre autoridades competentes existente (p. ej. fiscal, financiero, penal, civil, mercantil o policial) y, si no existiera, el mecanismo de asistencia establecido en el artículo el Reglamento (UE) 2018/1807.

Este mecanismo prevé que cada Estado miembro designe un punto de contacto único (en España, la Secretaría de Estado de Digitalización e Inteligencia Artificial) que actuará de enlace con los puntos de contacto únicos de los demás Estados miembros y la Comisión.

Cuando una autoridad competente de un Estado miembro solicite la asistencia de otro Estado miembro para obtener acceso a datos, formulará una solicitud debidamente motivada al punto de contacto único designado, el cual identificará a la autoridad competente de su Estado miembro y le remitirá la solicitud recibida, de forma que ésta proporcione 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 Reglamento.

4. PORTABILIDAD DE DATOS NO PERSONALES

¿Cómo se prevé garantizar la portabilidad de datos no personales entre proveedores de servicios *cloud*?

La libre circulación de datos personales («Derecho a la portabilidad de los datos») ya fue establecida por el artículo 20 del Reglamento General de Protección de Datos (RGPD).

En el caso de datos no personales, este Reglamento prevé que la Comisión fomente la elaboración de códigos de conducta autorreguladores a escala de la Unión, 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.

Se debe completar el desarrollo de los códigos de conducta a más tardar el 29 de noviembre de 2019 y aplicarlos efectivamente, por parte de las entidades que a ellos se adhieran, a más tardar el 29 de mayo de 2020.

¿Se está desarrollando alguna iniciativa al respecto por parte de la industria?

Dentro del grupo de trabajo denominado Working Group on Cloud Switching/Porting Data (SWIPO), se han desarrollado 2 códigos de conducta, para infraestructura como servicio (IaaS) y software como servicio (SaaS), que buscan garantizar la portabilidad de datos en condiciones de transparencia, reduciéndose así el riesgo de "*vendor lock-in*".

5. SEGURIDAD DE DATOS NO PERSONALES

¿Siguen aplicando los requisitos de seguridad nacionales al externalizar el tratamiento de datos en un proveedor de servicios en la nube de otro país de la UE?

Sí, los 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.

¿Existe un marco de certificación de la seguridad de proveedores de servicios en la nube?

El Grupo de trabajo europeo de certificación de proveedores de servicios en nube (CSPCERT) presentó una recomendación a la Comisión Europea para establecer un mecanismo de certificación de nube europeo.

La Comisión Europea, por su parte, ha solicitado a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) que, teniendo en cuenta esa recomendación y otras similares, prepare una propuesta en línea con las disposiciones del Reglamento (UE) 2019/881, sobre la Ciberseguridad. En cualquier caso, este esquema de certificación será de uso voluntario.

¿Los códigos de conducta sobre portabilidad de datos incluyen requisitos de seguridad?

Los códigos de conducta incluirán, entre otros aspectos, información sobre regímenes de certificación de gestión de la seguridad de la información 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.

6. MÁS INFORMACIÓN

En la web de la Comisión Europea sobre la libre circulación de datos no personales puede encontrar más información.