CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Bonn, Bucarest, Dublín, Lisboa, Madrid, Milán, París, La Haya, Viena, Varsovia

Preguntas más frecuentes sobre la Data Act para DPOS

Grupo de trabajo sobre Estrategia Digital Europea, Octubre de 2025

Información de contacto:
https://cedpo.eu

Este documento ha sido creado por CEDPO originalmente en inglés. La traducción al castellano se ha realizado mediante herramientas de traducción automatizada con revisión pormenorizada por parte de APEP 1A para facilitar su lectura. En caso de duda consultar original en https://cedpo.eu/publications/

Índice

Introducción

Han pasado siete años desde la entrada en vigor del RGPD, que sentó unas bases sólidas para la protección de datos en Europa. A medida que avanzamos, el panorama normativo ha seguido evolucionando para guiar a Europa hacia un futuro digital responsable. La EU Data Act marca otro hito en este camino. El borrador filtrado del Digital Omnibus muestra que la Data Act desempeñará un papel cada vez más importante en la regulación del espacio digital en el futuro.

Por ahora, junto con otras leyes recientes sobre datos, como la Data Governance Act (DGA), la Digital Services Act (DSA), la Digital Markets Act (DMA), la Data Act introduce nuevas obligaciones y oportunidades. Como resultado, los responsables de la protección de datos (DPO) se ven cada vez más obligados a ampliar sus conocimientos más allá del RGPD, asesorando sobre una gama más amplia de cuestiones relacionadas con la gobernanza y el cumplimiento de los datos.

Para ayudar a la comunidad de delegados de protección de datos a afrontar estos retos futuros, CEDPO, a través de su grupo de trabajo sobre la Estrategia Digital Europea, ha colaborado con sus miembros más experimentados de toda Europa para elaborar respuestas prácticas y detalladas a las preguntas más frecuentes (FAQ) relacionadas con la Data Act. Estas preguntas frecuentes se centran específicamente en abordar temas relevantes para la protección de datos.

Extendemos nuestro más sincero agradecimiento a todos los miembros del grupo de trabajo y al personal de CEDPO por sus valiosas contribuciones.

Miembros del GT que han contribuido: **Thomas Ajoodha, Filippo Bianchini, Lionel Capel, Julie Crawford, Paul Jordan, Paul Lambert, Dra. Maria Maloney, Samira Marquaille, Massimo Pappalardo, Jeremiah Russel, Henry Simwinga.**

Dra. Sachiko Scheuing (GDD) y Filippo Bianchini (ASSO DPO)

Copresidentes del Grupo de Trabajo sobre Estrategia Digital Europea de CEDPO

Pregunta 1: ¿Qué es la Data Act y cuál es su objetivo?

La Data Act es una parte integral de la agenda legislativa de la UE con el objetivo de impulsar la estrategia europea en materia de datos, destinada a otorgar a la UE un papel de liderazgo en una sociedad basada en los datos. La Data Act apoya la libre circulación de datos en un mercado único en varios sectores empresariales, de investigación y de la administración pública. La norma tiene por objeto hacer que los datos sean más accesibles y utilizables para todos mediante mecanismos de intercambio de datos. Obliga a los titulares de datos a ponerlos a disposición en circunstancias pertinentes. Al mismo tiempo, permite a los usuarios beneficiarse de los datos que generan, por ejemplo, desde sus dispositivos IoT. Concretamente, la Data Act exige que los productos conectados se diseñen de manera que los usuarios puedan acceder directamente a los datos que generan (artículo 3). A primera vista, esto parece similar a la portabilidad de los datos y los derechos de acceso de los interesados en virtud del RGPD. Puede considerarse como una especificación adicional de estos derechos. En los casos en que no sea posible el acceso directo, los datos deben facilitarse rápidamente a los usuarios cuando lo soliciten (artículo 4). La Data Act se centra en garantizar un acceso equitativo a los datos y proteger los derechos de los usuarios, al tiempo que equilibra estos objetivos con la protección de los datos personales.

La norma es coherente con las normas vigentes sobre el tratamiento de datos personales, incluido el RGPD. En ocasiones, puede resultar útil cotejar las definiciones con otras normativas pertinentes de la UE. Por ejemplo, el Reglamento sobre la libre circulación de datos no personales establece un pilar fundamental de la economía europea de datos, al garantizar que los datos no personales puedan almacenarse, tratarse y transferirse en cualquier lugar de la UE.

Pregunta 2: ¿A quién aplica la Data Act?

La Data Act aplica a las organizaciones y personas responsables de producir, tratar o utilizar, gestionar y compartir datos derivados de la tecnología inteligente en la UE. En particular, la norma regula a los titulares de datos, normalmente diseñadores, fabricantes o proveedores de servicios que generan o pueden recuperar datos brutos de estas tecnologías inteligentes. La Data Act se centra principalmente en las relaciones entre empresas y entre empresas y consumidores, pero también regula el intercambio de datos entre empresas y administraciones públicas.

Las pequeñas y microempresas, junto con las organizaciones medianas que llevan menos de un año en funcionamiento, están exentas de la obligación de compartir información establecida en el artículo 5 de la Data Act

.

Pregunta 3: ¿A qué tipo de datos aplica la Data Act?

La Data Act aplica a todos los datos brutos y pre-procesados generados por el uso de un producto conectado o un servicio relacionado que esté fácilmente disponible para el titular de los datos, como datos de producto (generados mediante el uso de productos conectados), datos de servicios relacionados (datos generados por las acciones de los usuarios) o metadatos (datos necesarios para interpretar los datos de productos y los datos de servicios relacionados). Los datos en bruto (sin procesar) y pre-procesados pueden ser tanto datos personales como no personales. Los datos que han sido sometidos a un procesamiento intensivo, como los datos inferidos y derivados (por ejemplo, datos altamente enriquecidos, material audiovisual) generados mediante algoritmos complejos, no están sujetos a la Data Act.

La Ley de Datos también distingue entre datos sin procesar (en bruto) y datos inferidos o derivados. En caso de que los datos sin procesar sean datos personales, se aplica el RGPD además de la Data Act.

El Registro de Actividades de Tratamiento (RAT) será un buen punto de partida para determinar si la Ley de Datos es aplicable a tu organización.

Pregunta 4: ¿Cuáles son los diferentes tipos de actores que figuran en la Data Act?

La Ley de Datos define los siguientes tres tipos de actores principales: el titular de los datos, el destinatario de los datos y el usuario.

Un **titular** de **datos** es una persona física o jurídica que tiene acceso legal a datos sin procesar, procedentes de productos conectados o servicios relacionados, y que tiene la autoridad para conceder acceso a los mismos. Básicamente, un titular de datos es una persona física o jurídica con el derecho u obligación de utilizar o compartir datos generados o recopilados durante la prestación de un servicio relacionado. En la práctica, los titulares de datos suelen ser empresas, como fabricantes de productos conectados o proveedores de servicios relacionados, que gestionan dispositivos inteligentes y conservan los datos de los clientes recopilados a través de dichos dispositivos. Podría decirse que esta función es la más importante en virtud de la Ley de datos. Cualquier organización, ya sea pública o privada, que controle los datos generados por productos y servicios conectados se considera un titular de datos.

Las responsabilidades de un titular de datos incluyen facilitar el acceso a los datos y garantizar la posibilidad de transferirlos a otros proveedores de servicios en un formato fácil de usar, tal y como se especifica en la ley. También se les prohíbe imponer condiciones contractuales injustas a los usuarios en lo que respecta al acceso a sus datos y a sus derechos de portabilidad de los mismos.

Un **destinatario** de **datos** es una persona física u organización que recibe datos sin procesar de un titular de datos a petición del usuario. Básicamente, un destinatario de datos es una persona física o jurídica, distinta del usuario, a la que el titular de datos proporciona datos, incluidos terceros que actúan a petición del usuario o en cumplimiento de una obligación legal.

En la práctica, los destinatarios de datos suelen ser entidades jurídicas, como empresas, autoridades públicas, organizaciones de investigación u organizaciones sin ánimo de lucro.

Existen límites específicos para restringir a los grandes proveedores, o «guardianes», en virtud de la DMA, para que no actúen como terceros en determinados acuerdos de intercambio de datos.

En esencia, un destinatario de datos es una entidad que recibe datos de un titular de datos con la intención de utilizarlos con fines comerciales o profesionales. Esto podría implicar que las empresas analicen los datos de comportamiento de los usuarios, proporcionen almacenamiento en la nube para los datos generados por los dispositivos conectados u ofrezcan servicios basados en datos. La diferencia clave es que un destinatario de datos utiliza los datos con fines comerciales u organizativos, en lugar de para uso personal, como podría hacerlo un usuario de datos.

Un usuario es una persona física o jurídica que posee o tiene derecho a utilizar un producto conectado o a recibir servicios relacionados. Básicamente, un usuario es la persona física o jurídica que posee, alquila o arrienda un dispositivo inteligente.

En la práctica, el usuario suele ser el cliente de un dispositivo inteligente. Es importante señalar que las personas que utilizan el dispositivo pero que no son parte del acuerdo, como los familiares, probablemente no se consideren usuarios.

Pregunta 5: ¿Qué son los datos no personales?

La Data Act define los datos no personales como cualquier dato que no entre en la categoría de datos personales, tal y como se especifica en el artículo 2, apartado 4, de la norma. Si bien el RGPD se refiere a los datos anónimos como información que no puede vincularse a una persona física identificada o identificable en el considerando 26, no define explícitamente los datos no personales.

El Regulation on a Framework for the Free Flow of Non-personal Data within the European Union introduce los datos no personales en el artículo 1 como «datos distintos de los datos personales». En comparación con la definición de datos personales del artículo 1, los datos no personales pueden entenderse como cualquier información que no se refiera a una persona física identificada o identificable (el «interesado»). La Guía de 2019 de la Comisión Europea sobre el Reglamento relativo al marco para la libre circulación de datos no personales respalda esta interpretación.

Además, la Comisión clasifica los datos no personales en dos categorías:

(1) los datos que originalmente no pertenecían a una persona física identificada o identificable, y
(2) Datos que inicialmente eran personales, pero que posteriormente se anonimizaron.

Las lecturas de temperatura de un edificio son un ejemplo del caso (1), y la edad media de los alumnos de una clase es un ejemplo del caso (2).

Es importante señalar que la anonimización de los datos personales es diferente de la seudonimización. Mientras que la anonimización implica el tratamiento de los datos de manera que no puedan atribuirse a una persona, la seudonimización se refiere a datos que aún pueden atribuirse a una persona mediante información adicional. También es importante señalar que los datos seudonimizados se convierten en datos anónimos cuando están en manos de organizaciones que no tienen medios para volver a identificar al interesado[1].

Entre los ejemplos de datos no personales se incluyen los conjuntos de datos agregados o

anonimizados utilizados en el análisis de macrodatos, los datos de agricultura de precisión que ayudan a optimizar el uso de pesticidas y agua, y los datos sobre las necesidades de mantenimiento de la maquinaria industrial. Sin embargo, si los avances tecnológicos permiten la reidentificación de datos anonimizados, dichos datos se considerarían datos personales y se aplicaría el RGPD.

Pregunta 6: ¿Cómo debo tratar un archivo que contiene tanto datos personales como datos no personales?

La mayor parte de los datos contemplados en la Data Act se clasifican como «no personales», ya que se refieren a productos y servicios industriales y no a personas físicas. Sin embargo, no es raro que estos datos se mezclen con datos personales. Cuando un archivo contiene tanto datos personales como no personales, se denomina conjunto de datos mixtos.

En lo que respecta a los conjuntos de datos mixtos (mixed datasets), el considerando 7 de la Data Act señala que el RGPD[2] y la ePrivacy Directive (cuando sea aplicable) sientan las bases para un tratamiento de datos sostenible y responsable.

Se encuentra un matiz ligeramente diferente en otra normativa Europea que menciona los conjuntos de datos mixtos (mixed datasets): el Regulation on a Framework for the Free Flow of Non-personal Data in the European Union. De acuerdo con esta ley y con las directrices de la Comisión sobre el Reglamento relativo a la libre circulación de datos no personales, se aplica lo siguiente:

1. el «Regulation on a Framework for the Free Flow of Non-personal Data in the European Union» se aplica a la parte del conjunto que contiene datos no personales;
2. El RGPD se aplica a la parte del conjunto que contiene datos personales;
3. Si los datos no personales y los datos personales están «íntimamente vinculados», el RGPD se aplicará a todo el conjunto de datos, incluso si los datos personales representan una pequeña parte del conjunto.

La guía de la Comisión explica además que los datos no personales y los datos personales están «íntimamente relacionados» cuando es imposible o tecnológicamente o económicamente inviable separar ambos tipos de datos.

La recomendación para el tratamiento de conjuntos de mixed datasets es garantizar una protección adecuada y cumplir con las obligaciones establecidas en el RGPD. Sin embargo, cuando no es posible identificar al interesado, el responsable del tratamiento queda exento de las obligaciones establecidas en los artículos 15 a 20 del RGPD. Estas obligaciones incluyen los derechos de rectificación, supresión, limitación del tratamiento, la obligación de notificar la rectificación, supresión o limitación del tratamiento, y la portabilidad de los datos, tal y como se establece en el artículo 11 del RGPD.

---

[1] Sentencia de 4 de septiembre de 2025, EDPS contra SRB, C-413/23 P, ECLI:EU:C:2025:645

[2] *Reglamento* de 2018 *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, organismos, oficinas y agencias de la Unión y a la libre circulación de dichos datos*

Pregunta 7: ¿Cuándo debe mi organización utilizar medidas técnicas y organizativas para proteger los datos?

Al tratar datos personales, deben aplicarse medidas técnicas y organizativas adecuadas para proteger los datos. Una medida de protección que se destaca tanto en el RGPD como en la Data Act es la seudonimización. Se recomienda aplicar el mismo estándar de seudonimización en virtud de la Ley de Datos que el exigido por el RGPD.

La Data Act también aborda las medidas de protección en situaciones en las que los datos personales deben compartirse con un organismo del sector público, la Comisión, el Banco Central Europeo o una institución Europea que muestre una «necesidad excepcional». En tales casos, la organización solicitante debe especificar las medidas técnicas y organizativas necesarias para proteger los datos. Además, la organización solicitante debe evaluar si los datos personales pueden ser anonimizados.

Por otra parte, el titular de los datos debe anonimizar los datos personales, salvo que la solicitud de puesta a disposición de los datos a un organismo del sector público, la Comisión, el Banco Central Europeo o una institución de la UE requiera la divulgación de datos personales. En tales casos, el titular de los datos está obligado a seudonimizar los datos.

Es posible que, con el tiempo, se aprueben leyes nacionales que regulen la divulgación de otros tipos de datos en situaciones específicas, como los datos médicos o estadísticos. Cuando estos datos no puedan agregarse y deban compartirse como datos personales, deberán aplicarse medidas técnicas y organizativas adecuadas para protegerlos.

Pregunta 8: ¿Qué hay que tener en cuenta para minimizar los riesgos asociados a la Ley de Datos?

La EU Data Act establece un marco único y coherente para compartir datos personales y no personales dentro del mercado único europeo. Sus objetivos son garantizar la equidad en las cadenas de valor basadas en datos, mejorar el acceso de los usuarios a los datos generados por los productos conectados y los servicios relacionados, y estimular la innovación en todos los sectores.

Al mismo tiempo, el hecho de que haya más datos disponibles aumenta inevitablemente la exposición al uso indebido, las violaciones de la privacidad, la pérdida de secretos comerciales, los incidentes de ciberseguridad y el acceso discriminatorio o desigual. Por lo tanto, la norma combina los nuevos derechos de acceso con un conjunto de salvaguardias por niveles que varían en función de la relación en la que se comparten los datos: empresa a consumidor (B2C), empresa a empresa (B2B) y empresa a gobierno (B2G).

Mitigación de riesgos en las relaciones B2C y B2B

En los contextos B2C (artículos 3 y 4), los productos conectados y los servicios relacionados deben diseñarse de manera que los datos sean, por defecto, directamente accesibles para los usuarios en un formato estructurado, seguro y legible por máquina. Los consumidores deben tener acceso gratuito y estar protegidos contra condiciones contractuales injustas u opacas.

Deben conservar un control significativo sobre sus datos, incluidas las opciones de conceder o revocar el acceso y gestionar las condiciones de reutilización.

En las relaciones B2B, en las que pueden existir desequilibrios, la Data Act permite a las partes definir restricciones contractuales sobre el uso o el intercambio posterior de datos cuando dicho uso pueda poner en peligro la seguridad, la salud o los secretos comerciales (artículos 4(2) y 4(6)). Los acuerdos deben incluir cláusulas de confidencialidad y las empresas pueden suspender el intercambio de datos si no se aplican las medidas acordadas o si se comprometen secretos comerciales (artículo 4, apartado 7). La norma exige que dichas condiciones sean justas y eviten explotar asimetrías en el poder de negociación, especialmente en el caso de las pymes (artículo 5, apartado 3).

Protecciones técnicas y organizativas

La Data Act permite a los titulares de datos aplicar medidas de protección técnicas, como el cifrado, los controles de acceso y los contratos inteligentes, para impedir el acceso o el uso no autorizados (artículo 11, apartado 1). Estas medidas no deben impedir el acceso legítimo de los usuarios, pero son fundamentales para garantizar el cumplimiento y proteger la información sensible. Los titulares de datos también pueden recurrir a la seudonimización y a protocolos seguros de transferencia de datos, especialmente cuando los datos contienen información sensible o implican el acceso de terceros.

El intercambio de datos también está sujeto a la limitación del propósito. Los terceros solo deben procesar los datos para los fines acordados con el usuario y deben eliminarlos cuando ya no sean necesarios (artículo 6, apartado 1). En el caso de los datos personales, es obligatorio el pleno cumplimiento del RGPD. Si se incumplen estas obligaciones, los titulares de los datos pueden exigir la supresión de los datos y el cese de los servicios o productos derivados (artículo 11, apartados 2 a 4). En contextos B2B, las medidas técnicas también pueden incluir pistas de auditoría para supervisar el cumplimiento.

Gestión de secretos comerciales en escenarios de intercambio

Tanto si los datos se comparten con usuarios como con terceros, la norma ofrece una sólida protección de los secretos comerciales. Estos solo pueden revelarse si es estrictamente necesario y si se han establecido las garantías técnicas y contractuales adecuadas (artículos 4(6) y 5(9)). Si no se respetan dichas protecciones, los titulares de los datos pueden suspender el intercambio y deben informar a la autoridad competente (artículo 5(10)). Los contratos deben definir cómo se protegen los secretos comerciales y especificar las obligaciones de confidencialidad.

Acceso del sector público y la dimensión B2G

En casos excepcionales, las autoridades públicas pueden solicitar datos cuando exista un claro interés público (artículo 17). Estas solicitudes deben ser específicas, proporcionadas y justificadas. La autoridad debe utilizar los datos únicamente para los fines indicados, aplicar medidas de seguridad estrictas y suprimir los datos cuando ya no sean necesarios (artículos 18 y 19). Siempre que sea posible, se debe aplicar la anonimización o la seudonimización a los datos personales. Los organismos públicos también deben aplicar medidas técnicas y organizativas similares a las de los agentes privados y cumplir los requisitos de confidencialidad al tratar datos sensibles.

El contexto importa

Las obligaciones y protecciones establecidas en la Data Act dependen del contexto. El intercambio B2C se centra en el empoderamiento del usuario y la protección del consumidor. Las relaciones B2B hacen hincapié en la equidad contractual y la confidencialidad. El acceso B2G se limita a necesidades excepcionales y está estrictamente regulado. Este enfoque por capas permite mitigar eficazmente los riesgos sin imponer un modelo único para todos.

En conclusión, al definir normas adaptadas a los diferentes contextos de intercambio de datos y promover el uso de garantías contractuales, técnicas y organizativas, la norma proporciona una base jurídica sólida para minimizar los riesgos. Sin embargo, la puesta en práctica de estas garantías requiere algo más que el cumplimiento legal. Las soluciones técnicas, incluidas las API y los mecanismos de acceso estandarizados, desempeñan un papel clave para garantizar un intercambio de datos seguro, auditable y fiable entre todos los actores.

Pregunta 9: ¿Cuál es el método más utilizado para compartir datos según la Data Act y cuáles son las formas de reducir los riesgos relacionados con la protección de datos?

Existen varias formas de reducir los riesgos asociados a la Data Act; el primer paso es implementar políticas de gobernanza para el intercambio de datos. Al igual que con el cumplimiento del RGPD, se puede formalizar una gestión sólida del intercambio de datos mediante contratos y documentos que definan las funciones y responsabilidades de cada parte; esto resulta especialmente útil entre los titulares de los datos y terceros. Los contratos pueden incluir procedimientos para gestionar el acceso y, si es necesario, asignar derechos de control de acceso, establecer requisitos de seguridad y garantizar la rendición de cuentas y la trazabilidad.

El destinatario de los datos suele ser un encargado del tratamiento dentro del proceso de intercambio. Sin embargo, el contrato con el tercero podría prever una responsabilidad conjunta en el tratamiento si el tercero, en la ley o en la práctica, ejerce una influencia determinante sobre los objetivos y las condiciones del tratamiento. Esto podría aplicarse, por ejemplo, cuando el tercero proporciona una API de intercambio a la que se conecta el titular de los datos para compartirlos.

Medidas para prevenir el acceso no autorizado, recomendadas por diversos reguladores nacionales: Al igual que con el RGPD, se debe adoptar un enfoque basado en el riesgo, en el que el nivel de protección requerido sea proporcional a la gravedad de las posibles consecuencias para el interesado o el usuario. Por ejemplo, la recomendación de la autoridad francesa de protección de datos, la CNIL, incluye lo siguiente:

- Dividir los datos que se van a compartir mediante una segmentación física o lógica de los datos, o ambas. La disponibilidad de los datos puede ser importante en determinadas situaciones, en las que el usuario puede verse gravemente afectado sin ellos. En tales situaciones, mantener los datos en «compartimentos» separados puede reducir la posibilidad de que se produzca una violación de los datos.

- Uso de medidas técnicas adicionales, como una caja fuerte digital, para proteger las

contraseñas y los protocolos de autenticación.
- Mantener un registro completo de los accesos y las acciones realizadas en la base de datos para identificar cualquier uso indebido de los datos y errores, así como garantizar que el titular de los datos/destinatario de los datos (o su agente) haya proporcionado las actualizaciones de datos necesarias en el marco del intercambio continuo.
- Crear un entorno de pruebas «sandbox» para el intercambio de datos en el que los usuarios puedan experimentar con los datos de forma segura.

Debido al tipo específico de datos que cubre la Data Act, la transferencia de datos a través de interfaces de programación de aplicaciones (API) puede ser el método más utilizado. Las API permiten el intercambio seguro de datos personales y no personales entre los titulares de los datos y terceros autorizados. Las API suelen ofrecer un mayor nivel de seguridad que las plataformas de intercambio de datos o los servicios de correo electrónico, lo que permite reducir el riesgo de violaciones de datos durante el intercambio.

Las API son una herramienta preferida para compartir datos, especialmente cuando:
- Se actualizan con frecuencia grandes volúmenes de datos.
- Terceros necesitan acceder regularmente a los datos para satisfacer las solicitudes de acceso de los usuarios, especialmente cuando hay un gran número de solicitudes de este tipo, y
- El tercero transfiere directamente los datos al usuario sin almacenamiento permanente de los mismos.

Pregunta 10: ¿Cuáles son las obligaciones del titular de los datos?

La Data Act establece varias obligaciones clave para los titulares de datos.

Acceso a los datos por diseño y por defecto

Los titulares de datos deben diseñar y fabricar productos conectados o servicios relacionados (como dispositivos inteligentes) de manera que los datos generados por el dispositivo sean accesibles por defecto y de forma gratuita para el usuario. Esto incluye los metadatos pertinentes necesarios para interpretar y utilizar los datos. El acceso debe ser fácil, seguro, completo, estructurado y proporcionarse en un formato común y legible por máquina.

Solicitudes de acceso a datos

Si los usuarios no pueden acceder directamente a los datos a través del dispositivo inteligente, el titular de los datos deberá compartir los datos cuando se le solicite. Estas solicitudes deberán atenderse sin demoras indebidas, en un formato común y legible por máquina, de forma gratuita y, cuando sea pertinente y viable, de forma continua y en tiempo real. Además, los usuarios pueden solicitar al titular de los datos que comparta los datos generados por el dispositivo con un tercero. Al atender dicha solicitud, el titular de los datos deberá proporcionar los datos en las mismas condiciones descritas anteriormente. Sin embargo, a diferencia de lo que ocurre cuando se comparten datos con el usuario, en este caso el titular de los datos podrá cobrar una compensación razonable al tercero por compartir los datos. El titular de los datos deberá garantizar que las solicitudes de acceso se puedan tramitar de forma sencilla y sin que se vean entorpecidas por procedimientos innecesarios o solicitudes de información por parte del usuario.

Transparencia

Antes de celebrar un contrato de compra, alquiler o arrendamiento de un producto conectado, el titular de los datos debe proporcionar al usuario información clara y comprensible. Esto incluye detalles sobre el tipo y el volumen de los datos, los períodos de conservación de los datos, si el producto genera datos de forma continua y en tiempo real, y si los datos se almacenan de forma remota o en el dispositivo. También se debe informar al usuario sobre cómo ejercer sus derechos de acceso, recuperación o supresión de datos.

Del mismo modo, antes de celebrar un contrato de servicios relacionados con un producto conectado, el titular de los datos debe informar al usuario sobre el tipo y el volumen de los datos, los períodos de conservación de los datos, los terceros que pueden utilizarlos y los fines para los que se utilizan. El titular de los datos también debe explicar cómo el usuario puede solicitar el intercambio de datos con un tercero, poner fin al intercambio de datos y presentar una reclamación en caso de incumplimiento de la Data Act.

Portabilidad de los datos

La Data Act faculta a los usuarios a transferir sus datos a un tercero, lo que facilita el cambio entre proveedores de servicios o el uso de datos con diferentes aplicaciones. El titular de los datos debe hacer que este proceso sea fluido y garantizar que los datos se proporcionen en un formato de uso común y legible por máquina.

Pregunta 11: ¿Cómo formalizo el intercambio de datos en un contexto entre empresas?

Los términos y condiciones para el intercambio de datos deben formalizarse en un contrato entre las partes implicadas. El acuerdo debe ser justo, razonable, no discriminatorio y transparente, lo cual es especialmente importante cuando la parte contratante es una pequeña o mediana empresa, una organización sin ánimo de lucro o una institución de investigación.

Cuando un titular de datos comparte datos con otra empresa (el destinatario de los datos) en virtud de la Data Act, puede solicitar al destinatario de los datos una tarifa razonable por los datos proporcionados.

Pregunta 12: Mi organización es un titular de datos. ¿Puedo negarme a facilitar los datos?

El usuario y el titular de los datos pueden restringir el acceso a los datos si dicho acceso pudiera comprometer los requisitos de seguridad del producto exigidos por la ley. También pueden acordar limitar o prohibir el acceso, el uso o el intercambio posterior de los datos.

En los casos relacionados con secretos comerciales, el titular de los datos está autorizado a establecer acuerdos para mantener la confidencialidad de los datos y proteger los secretos comerciales. Esto incluye acordar medidas técnicas y organizativas para garantizar la confidencialidad.

Además, el titular de los datos no tiene la obligación de compartir los datos con terceros

ubicados fuera de la UE.

Pregunta 13: ¿Cuál es el impacto de la Data Act en la gestión de los derechos de los interesados en los casos en que los datos son datos personales?

La Data Act no modifica los derechos y obligaciones establecidos en el RGPD. Por el contrario, refuerza y facilita el derecho a la portabilidad de los datos. En concreto, la Data Act exige a los titulares de datos que permitan a los clientes transferir sus datos en un plazo de 30 días.

Cuando se trata de datos personales, el titular de los datos actuará en muchos casos como responsable del tratamiento y deberá gestionar las solicitudes de acceso a los datos de conformidad con el RGPD. En los casos en que el usuario sea una organización, este se convertirá en el responsable del tratamiento. El responsable del tratamiento deberá verificar si se trata de datos personales y asegurarse de que existe una base jurídica para facilitar dichos datos, especialmente si el usuario no es el interesado.

Pregunta 14: ¿Cuáles son las bases legales que pueden utilizarse para el tratamiento de datos personales, a los que se aplica la Data Act?

La Data Act se aplica sin perjuicio del RGPD, lo que significa que el RGPD tiene prioridad sobre la Data Act (art. 1(5), Rec. 7 Data Act). Por consiguiente, todo tratamiento de datos personales debe tener una base jurídica válida.

Los titulares de datos tienen fundamentos jurídicos en virtud del artículo 6 del RGPD. Si el interesado es también el único usuario, la situación es sencilla, ya que el titular de los datos puede basarse en el fundamento jurídico del cumplimiento de una obligación legal (véase el artículo 6, apartado 1, letra c), del RGPD, artículo 4 de la Data Act). Sin embargo, si el usuario es una organización con varias personas que utilizan el dispositivo conectado, la situación puede ser más compleja. Por ejemplo, si una empresa utiliza un vehículo compartido, debe seleccionar un fundamento jurídico que tenga en cuenta los datos de los empleados. En tales casos, el tratamiento de los datos personales generados por los empleados que utilizan un vehículo compartido puede tener que basarse en el consentimiento (artículo 6, apartado 1, letra a), y artículo 9, apartado 2, del RGPD) o en la ejecución de un contrato (artículo 6, apartado 1, letra b), del RGPD). Es importante señalar que la Data Act se basa en gran medida en acuerdos contractuales, complementando así el artículo 6, apartado 1, letra b), del RGPD para el tratamiento de datos personales en virtud de un contrato. Por ejemplo, en virtud de un contrato, un usuario puede compartir datos personales con un tercero para prestar un servicio, utilizando el artículo 6, apartado 1, letra b), como base jurídica.

Por último, en la mayoría de los casos, el destinatario de los datos tratará los datos en nombre del titular de los datos o del usuario.

Pregunta 15: Mi organización es usuario y desea tratar los datos facilitados por el titular de los datos sobre la base del interés legítimo. ¿Es posible?

De conformidad con el artículo 6, apartado 1, letra f), del primer párrafo del artículo 6, apartado 1, del RGPD, el tratamiento puede considerarse necesario para los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, solo a condición de que:

- el responsable del tratamiento ha informado a los usuarios del interés legítimo que persigue el tratamiento de datos;
- dicho tratamiento de datos se lleva a cabo únicamente en la medida en que sea estrictamente necesario para los fines de ese interés legítimo; y
- de un equilibrio entre los intereses en conflicto, teniendo en cuenta todas las circunstancias pertinentes, se desprende que los intereses o las libertades y derechos fundamentales de los usuarios no prevalecen sobre el interés legítimo del responsable del tratamiento o de un tercero.

La prueba de ponderación compara esencialmente los intereses contrapuestos del responsable del tratamiento con los intereses o los derechos y libertades fundamentales de los interesados.

¿Evaluación de las limitaciones y restricciones?

El uso de los datos personales generados por dispositivos conectados puede restringirse o limitarse de conformidad con la legislación nacional y europea aplicable. Por ejemplo, la legislación laboral nacional puede regular la supervisión de los empleados que utilizan dispositivos conectados en el lugar de trabajo.

Además, el interés legítimo no puede utilizarse como base jurídica cuando los datos recibidos del titular de los datos entran en las categorías especiales de datos personales definidas en el artículo 9 del RGPD. Esto incluye los datos biométricos y los datos relacionados con la salud generados por dispositivos médicos conectados.

Por otra parte, cuando los datos recibidos del titular de los datos se tratan para tomar decisiones automatizadas que producen efectos jurídicos en relación con el interesado o le afectan de manera similar (como la calificación crediticia automatizada), el interés legítimo no puede utilizarse como base jurídica válida.

En estos casos, se requerirá una base jurídica diferente.

Ejemplos de intereses o derechos y libertades fundamentales del interesado

Los derechos y libertades en juego dependen, en principio, de las circunstancias específicas de cada caso concreto[3].

[3] Véase la sentencia de 4 de mayo de 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, apartado 31.

A modo de ejemplo, el intercambio o el uso —no acordado con el usuario— de los datos personales generados por un coche conectado o por un asistente doméstico puede representar una amenaza:

- para la vida privada y familiar de los interesados, protegida por el artículo 7 de la Carta de los Derechos Fundamentales de la UE (la «Carta»); y
- para el derecho a la seguridad, protegido por el artículo 6 de dicha Carta.

Cómo puede ayudar el delegado de protección de datos en este proceso

La prueba de equilibrio debe realizarse caso por caso, teniendo en cuenta todos los riesgos posibles para los interesados. Según el Dictamen 06/2014 del GT29 sobre el concepto de intereses legítimos del responsable del tratamiento, este debe:

- Identificar los derechos e intereses fundamentales del interesado que podrían verse afectados.
- Tener en cuenta las expectativas razonables de los interesados.
- Evaluar las repercusiones en el interesado y compararlas con los beneficios que se esperan del tratamiento por parte del responsable del tratamiento.

Es importante señalar que los niños merecen una protección específica en lo que respecta a sus datos personales, ya que pueden ser menos conscientes de los riesgos potenciales.

Aunque el RGPD no regula específicamente el papel del delegado de protección de datos en la evaluación del interés legítimo, este es análogo al papel del delegado de protección de datos en una evaluación de impacto relativa a la protección de datos. Por lo tanto, el delegado de protección de datos debe asesorar, cuando lo solicite el responsable del tratamiento, sobre la prueba de equilibrio y supervisar su ejecución.

Pregunta 16: Mi organización es un organismo público. ¿En qué situaciones puede mi organización solicitar datos basándose en una «necesidad excepcional»?

El concepto de «necesidad excepcional» se introduce al principio de la Data Act, donde el artículo 1(1) establece que parte del objetivo de la norma es armonizar las normas sobre la disponibilidad de los datos en poder del Titular de los Datos para los organismos públicos cuando exista una «necesidad excepcional» de los datos para realizar una tarea específica de interés público. Esto establece un estándar elevado, ya que limita la provisión a organismos de tipo público y exige una «necesidad excepcional», específicamente para una tarea de interés público. Los datos que se ponen a disposición se limitan al cumplimiento de esta necesidad excepcional.

Si existen medios alternativos para llevar a cabo la tarea, algunos podrían argumentar que esta disposición no es aplicable. Es probable que el término «excepcional» excluya el uso normal y habitual, lo que implica que solo se aplicaría en circunstancias verdaderamente extraordinarias. Además, debe existir una tarea predeterminada e identificada que sea excepcional y que desencadene esta necesidad. Si un organismo público no puede identificar y documentar claramente por adelantado dicha «necesidad excepcional» y «tarea específica», es posible que no pueda invocar esta disposición.

Además, la disposición sobre el alcance debe leerse junto con los detalles específicos de lo que constituye una necesidad excepcional y cuándo se aplica, tal y como se explica con más detalle más adelante en la Data Act. El artículo 1, apartado 3, refuerza estas posibles limitaciones, al establecer que los datos solo pueden ponerse a disposición «cuando exista una necesidad excepcional». Esto plantea una advertencia de que la disposición sobre el alcance podría limitar inadvertidamente la aplicación de disposiciones posteriores, posiblemente de formas no previstas por la legislación.

Las principales definiciones de la Data Act no definen explícitamente el término «necesidad excepcional». Sin embargo, el artículo 2(29) agrupa las «emergencias públicas» y las «situaciones excepcionales», lo que podría llevar a algunos a interpretar que la necesidad excepcional se limita a las emergencias públicas. El término «circunstancias excepcionales» también se menciona en diversos contextos, como en los artículos 4(7) y 5(11), incluidos los relacionados con la propiedad intelectual.

Las disposiciones principales relativas a las necesidades excepcionales se detallan en el capítulo V. El artículo 14, titulado «Obligación de facilitar datos por motivos de necesidad excepcional», establece que cuando un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión demuestre una necesidad excepcional, tal como se define en el artículo 15, de utilizar determinados datos —incluidos los metadatos pertinentes necesarios para interpretar y utilizar dichos datos—, dichos organismos deberán presentar una solicitud debidamente motivada.

Las personas jurídicas, distintas de los organismos del sector público, que posean los datos pertinentes estarán entonces obligadas a ponerlos a disposición.

El artículo 15 especifica que la «necesidad excepcional» debe estar limitada tanto en el tiempo como en el alcance y solo puede darse en determinadas circunstancias, que se enumeran claramente en una lista fija. Por ejemplo, el artículo 15, apartado 1, letra a), se refiere a la respuesta a una emergencia pública, mientras que el artículo 15, apartado 12, letra b), abarca otras circunstancias que no deben implicar datos personales. Cabe destacar que existe una excepción para las microempresas y las pequeñas empresas en virtud del artículo 15, apartado 2, aunque incluso las pequeñas empresas con un volumen de negocios modesto pueden gestionar cantidades importantes de datos.

El artículo 17 hace hincapié en que el organismo público debe «demostrar» la necesidad excepcional, lo que implica un nivel de prueba más elevado que el simple hecho de calificar una necesidad como excepcional. Este requisito podría excluir situaciones que no son realmente excepcionales. El artículo 17, apartado 1, letra c), menciona específicamente la necesidad de explicar cómo se tratarán los datos personales, lo que podría plantear cuestiones controvertidas en cuanto a su interpretación y aplicación. Además, el artículo 17, apartado 2, letra e), menciona el requisito de la seudonimización, y el artículo 17, apartado 2, letra c), destaca la importancia de la proporcionalidad a la hora de evaluar la necesidad excepcional, lo que limita aún más su aplicación.

El artículo 18, apartado 2, aborda el proceso de respuesta a las solicitudes de datos, incluidos los plazos, las modificaciones y las distinciones entre necesidades excepcionales de emergencia pública y otros tipos de necesidades excepcionales. También se puede considerar la compensación por el suministro de datos, tal y como se describe en el artículo 20. Además, en el artículo 21 se aborda el intercambio de datos para organizaciones de investigación y estadísticas en el contexto de necesidades excepcionales.

Las referencias a las necesidades excepcionales aparecen a lo largo de toda la Data Act, en particular en los considerandos 5, 31, 63, 65, 66, 69, 70-73, 75, 77, 103 y 107, entre otros. Estas referencias y los artículos específicos proporcionan conjuntamente el marco para comprender y aplicar el concepto de necesidad excepcional en el ámbito de esta norma.

Pregunta 17: ¿Cómo se define la elaboración de perfiles en la Data Act?

Tanto el RGPD como la Data Act utilizan la misma definición de elaboración de perfiles, concretamente el artículo 4, apartado 4, del RGPD, que define la elaboración de perfiles como «*cualquier forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales relacionados con una persona física, en particular para analizar o predecir aspectos relativos al rendimiento de esa persona en el trabajo, su situación económica, su salud, sus preferencias personales, sus intereses, su fiabilidad, su comportamiento, su ubicación o sus movimientos*».

Pregunta 18: ¿Está prohibida la elaboración de perfiles en virtud de la Data Act?

En general, la elaboración de perfiles no está prohibida por la Data Act. Sin embargo, no se permite en un contexto muy específico, concretamente cuando *el usuario* (a menudo el interesado) comparte los datos con organizaciones. El artículo 6, apartado 2, letra b), de la norma refuerza los derechos de los usuarios y ofrece otra vía para que estos se protejan mejor de las prácticas de elaboración de perfiles no deseadas.

Esta situación se establece en el artículo 6, apartado 2, letra b), de la Data Act:

6.2 El tercero no podrá:

*… **(b) sin perjuicio de 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, salvo que sea necesario para prestar el servicio solicitado por el usuario;*

Para aclarar la interpretación, a continuación se resumen las partes pertinentes del artículo 22 del RGPD. El artículo 22, apartado 1, establece lo siguiente:

*1. El interesado tendrá derecho **a no ser** objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos que le afecten o le afecten de manera similar.*

A continuación, **el artículo 22, apartado 2, letras a) y c),** del RGPD establece lo siguiente:

(a) El apartado 1 no se aplicará si la decisión: es necesaria para la celebración o el cumplimiento de un contrato entre el interesado y el responsable del tratamiento;
(b) …
(c) se base en el consentimiento explícito del interesado.

Puede haber cierta confusión al interpretar ambos textos conjuntamente, especialmente teniendo en cuenta el número de afirmaciones negativas que contienen. La cláusula «sin perjuicio de lo dispuesto en el artículo 22, apartado 2, letras a) y c), del Reglamento (UE) 2016/679» debe entenderse como «a pesar de lo dispuesto en el artículo 22, apartado 2, letras a) y c)». En circunstancias normales, el artículo 22, apartado 2, establece dos excepciones al artículo 22, apartado 1. Sin embargo, estas dos excepciones no se aplican en el contexto del artículo 6, apartado 2, letra b), de la Data Act.

Para mayor claridad, el artículo 6, apartado 2, letra b), debe interpretarse conjuntamente con el artículo 5 de la Data Act. Al hacerlo, queda claro que la elaboración de perfiles está prohibida en situaciones en las que se dan los tres criterios acumulativos siguientes, cuando:

- Los datos personales en cuestión forman parte de un producto (por ejemplo, una máquina de café espresso automática) o de datos de servicio creados mediante el uso de productos conectados, y
- Los datos personales son compartidos por el usuario de la máquina de café espresso con su empresa, y su empresa no es el titular de los datos, y
- La elaboración de perfiles no es necesaria para prestar al interesado el servicio solicitado.

Una vez aclarada esta interpretación, la siguiente cuestión clave radica en determinar qué constituye *«necesario para prestar el servicio solicitado por el usuario»*. Probablemente, esto se interpretará caso por caso. Por ejemplo, un *usuario* de un servicio de streaming de música comparte sus datos de uso con otra empresa de entretenimiento multimedia, para poder disfrutar de las mismas recomendaciones personalizadas. Esto requiere que la empresa de entretenimiento multimedia (*destinataria de los datos*) realice un perfilado. Dado que la solicitud proviene del *usuario* y que el perfilado es necesario para prestar el servicio solicitado, es muy probable que este tipo de perfilado por parte de la *destinataria de los datos* sea admisible. Sin embargo, la empresa de entretenimiento multimedia no puede realizar un perfilado para averiguar a qué hora del día se escuchan los podcasts, con el fin de mejorar sus procesos operativos. Esto probablemente infringiría el artículo 6, apartado 2, letra b).

La hipótesis subyacente puede ser que *los destinatarios de los datos* no son los titulares originales de los mismos, por lo que es muy probable que tengan un control o un conocimiento limitados sobre cómo se recopilaron los datos o cómo pretendía utilizarlos el usuario. La elaboración de perfiles para servicios no relacionados con el producto o servicio al que se ha suscrito el usuario se consideraría una intromisión en sus derechos de protección de datos en virtud del RGPD, y con razón.

Consideremos el siguiente escenario: una empresa de servicios públicos podría utilizar los datos de los termostatos de los hogares residenciales sobre el consumo de energía en beneficio propio. La empresa podría analizar los patrones de consumo de energía e identificar las horas de mayor consumo, es decir, las tardes y los fines de semana, y poner esta información a disposición de los propietarios. Incluso podría comparar los patrones de consumo de energía de hogares o tipos de edificios similares para que los propietarios tuvieran una referencia. Imaginemos una situación en la que un cliente de la empresa de servicios públicos decide cambiarse a otra empresa. Se puede solicitar el intercambio de los datos del termostato para que la nueva empresa de servicios públicos pueda ofrecer consejos de ahorro energético y el cliente pueda aprovecharlos desde el primer día de su cambio a la nueva empresa. Cuando sea necesario crear perfiles para este fin, se permite hacerlo en este escenario.

La nueva empresa de servicios públicos podría entonces considerar la creación de un perfil de fidelidad que se utilice para elegir planes energéticos incentivados que vinculen a la persona a

un contrato de mayor duración con una tarifa reducida. Si el propietario se cambia al nuevo plan, la nueva empresa de servicios públicos se beneficiará de la estabilidad financiera y el propietario verá reducidos sus costes. Sin embargo, dado que la creación de un perfil no es estrictamente necesaria para prestar el servicio al propietario, la Data Act prohíbe que la nueva empresa de servicios públicos elabore este perfil.

Pregunta 19: ¿Por qué es fundamental la transparencia en virtud de la Ley de Datos?

Cuando pensamos en datos y transparencia, nos enfocamos en las reglas de transparencia relacionadas con dar detalles por adelantado sobre cómo se usarán los datos personales y obtener un consentimiento claro y justo para su recolección. La transparencia también juega un papel importante en garantizar que las personas conozcan sus derechos sobre los datos y puedan ejercerlos. Además, la transparencia es crucial en los contratos, políticas y términos y condiciones sobre datos entre entidades, así como entre entidades y personas.

Sin embargo, en el contexto de la Data Act, el objetivo de la transparencia cambia ligeramente. Si bien se mantienen las normas tradicionales de protección de datos, la norma hace hincapié en la transparencia en el contexto del intercambio de datos entre entidades. Por ejemplo, el artículo 5 destaca la necesidad de transparencia y de condiciones justas y no discriminatorias cuando los titulares de datos ponen los datos a disposición de los destinatarios de datos, en particular en las transferencias de datos entre entidades. En este caso, la transparencia puede estar más en consonancia con las normas de competencia que con las normas tradicionales de protección de datos.

Pueden surgir desacuerdos con respecto a esta interpretación, pero es muy probable que estas cuestiones se aclaren a medida que los órganos de resolución de litigios establecidos en virtud del artículo 10 comiencen a pronunciarse sobre cuestiones como la transparencia. Será importante ver si estas normas de procedimiento solo tienen en cuenta la Data Act o si también tendrán en cuenta las normas de protección de datos.

El artículo 28 de la Data Act se refiere al modelo tradicional de proporcionar información previa, en particular en lo que respecta a las obligaciones contractuales relacionadas con el acceso y la transferencia internacional de datos. Aunque en este artículo no se menciona explícitamente la «transparencia», las obligaciones de proporcionar información previa a través de sitios web son claras, y los profesionales deberán cumplir plenamente estos requisitos para evitar posibles problemas.

La transparencia también se aborda en el artículo 19, que introduce «obligaciones de transparencia» que pueden exigir la conservación de datos en determinadas circunstancias, lo que podría prevalecer sobre los requisitos de supresión o borrado de datos. Esto se aplica especialmente a los organismos del sector público.

Además, incluso cuando no existen requisitos explícitos de transparencia, dichos requisitos pueden ser necesarios o implícitos para que otras disposiciones funcionen eficazmente. Por ejemplo, puede resultar difícil justificar una acción si ciertos aspectos se han producido de una manera poco transparente. Esto está estrechamente relacionado con el concepto de comprender y respetar las expectativas razonables de las personas. Un ejemplo práctico es considerar si el uso histórico de los datos puede extenderse a una nueva aplicación de IA sin violar estas expectativas.

Por último, la transparencia también se menciona en varios considerandos de la Data Act, incluidos los considerandos 5, 24, 25, 34, 42, 51, 65, 69 y 73, que los lectores pueden consultar para obtener más contexto.

Enlaces útiles

- Texto de la Ley de Datos https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng
- Información sobre la Estrategia Europea de Datos https://digital-strategy.ec.europa.eu/en/policies/strategy-data
- Sitio web de la Comisión Europea sobre la Ley de Datos https://digital-strategy.ec.europa.eu/en/policies/data-act, que incluye una sección de preguntas frecuentes sobre la Ley de Datos en https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked- questions-about-data-act
- Reglamento sobre el marco para la libre circulación de datos no personales en la Unión Europea https://eur-lex.europa.eu/eli/reg/2018/1807/oj
- Orientaciones sobre el Reglamento relativo al marco para la libre circulación de datos no personales en la Unión Europea https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN
- RGPD https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Orientaciones de la CNIL: Recomendación sobre el uso de interfaces de programación de aplicaciones (API) para el intercambio seguro de datos personales (en francés) https://www.cnil.fr/sites/cnil/files/2023- 07/recommandation_api.pdf

Disclaimer

La información proporcionada en estas preguntas frecuentes tiene únicamente fines informativos y educativos. No debe interpretarse como asesoramiento jurídico. Para obtener orientación específica sobre su situación, consulte a un profesional jurídico cualificado.

Este documento ha sido creado por CEDPO originalmente en inglés. La traducción al castellano se ha realizado mediante herramientas de traducción automatizada con revisión pormenorizada por parte de APEP1A para facilitar su lectura.
En caso de duda consultar original en https://cedpo.eu/publications/