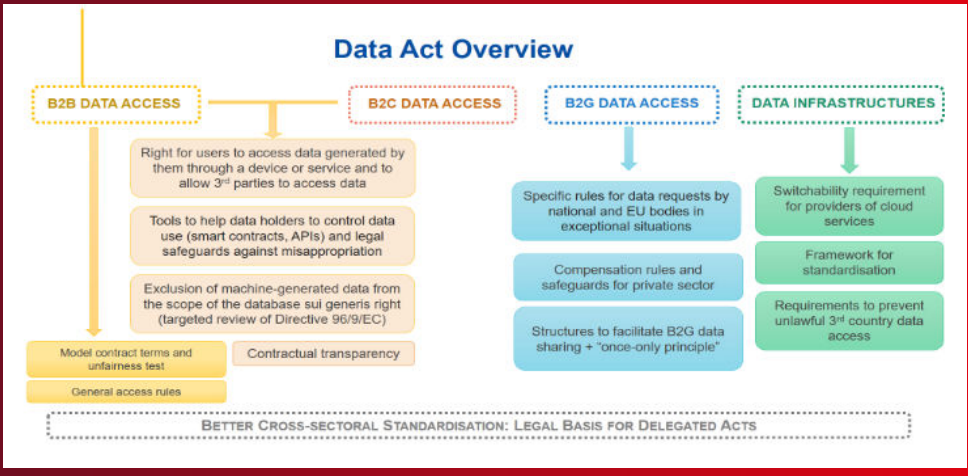
12 Septiembre de 2025: Entra en vigor la "Data Act"



El Reglamento (UE) 2023/2854 (Reglamento de Datos o Data Act) fue publicado en el Diario Oficial de la Unión Europea el 22 de diciembre de 2023 de ese año entrando en vigor el 11 de enero de 2024. Su aplicación general será a partir del **12 de septiembre de 2025**, es decir, en poco más de un mes, si bien parte del articulado (como el diseño de productos para acceso directo del usuario a los datos) se aplican hasta septiembre de 2026 y 2027.

La Data Act establece normas armonizadas sobre el acceso justo a datos generados por productos conectados y servicios asociados, con el fin de promover la innovación, el derecho del usuario a sus datos y la competencia en el mercado interior de datos.

Así la Data Act permite a los usuarios de **productos conectados** (por ejemplo, automóviles conectados, dispositivos médicos y de fitness, maquinaria industrial o agrícola) y **servicios relacionados** (es decir, cualquier cosa que haga que un producto conectado se comporte de una manera específica, como una aplicación para ajustar el brillo de las luces o para regular la temperatura de un refrigerador) acceder a los datos que cocrean utilizando los productos / servicios relacionados conectados.

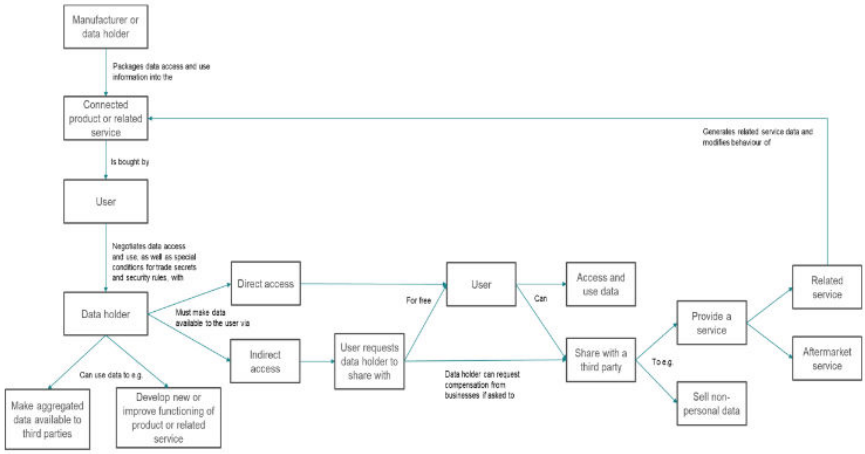
Se aplica tanto a datos personales como no personales, pero en ambos casos siempre sin perjuicio del cumplimiento del RGPD cuando estén en juego datos personales. Además, la normativa tiene efectos extraterritoriales: aplica a entidades no establecidas en la UE si ofrecen productos o servicios en el mercado europeo, debiendo designar representante legal en territorio comunitario.

I.- Principales derechos y obligaciones

- Derechos de acceso de usuarios

Los usuarios de productos conectados podrán solicitar acceso a los datos generados por su uso (*raw* y *pre-processed data*) desde el inicio de la aplicación del Reglamento -12 de septiembre de 2025-, pero no sobre datos heredados generados antes de esa fecha. Los datos derivados o inferidos (por ejemplo, enriquecidos analíticamente) quedan excluidos de la Data Act.

La calidad y formato de los datos facilitados debe ser igual a la que el titular se reserva a sí mismo, es decir, en condiciones equivalentes a las de un intercambio intragrupo o interoperable en el sector.



Fuente: FAQs Data Act Comisión Europea.

- Condiciones contractuales: FRAND y compensación

Las condiciones para compartir datos deben ser justas, razonables y no discriminatorias (FRAND), incluyendo mecanismos transparentes sobre compensaciones (art. 9.5 Data Act) por la puesta a disposición de los datos entre empresas.

Los titulares de los datos deben estar de acuerdo con el usuario en el uso de datos no personales (basado en términos transparentes según el considerando 25), lo que exige que los titulares de datos revisen oportunamente los acuerdos pertinentes para seguir utilizando datos fácilmente disponibles. Un tercero que recibe datos a raíz de una solicitud del usuario al titular de datos debe obtener una aprobación contractual similar del usuario para utilizar los datos recibidos.

En cuanto al intercambio de datos por un titular de datos con terceros, la Comisión ha afirmado en sus FAQS[1] que, incluso con el acuerdo contractual del usuario, sólo los datos no personales agregados pueden ponerse a disposición de un tercero. Sólo el usuario puede ser una fuente de acceso a datos no personales granulares del producto conectado o servicio relacionado.

- B2B, B2G, y servicios digitales

La Data Act establece obligaciones en el intercambio B2B

[1] https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act.

para evitar cláusulas abusivas e impedir prácticas contractuales injustas que obstaculicen el acceso o reutilización de los datos. Los proveedores de servicios de procesamiento de datos (por ejemplo, cloud), por su parte, deben facilitar al usuario el cambio de proveedor (portabilidad funcional), garantizando interoperabilidad, interoperabilidad técnica y transferencia de datos sin barreras.

En el contexto de intercambio de datos B2G (empresa-administración), se prevé que la Administración pública podrá solicitar acceso a datos privados en casos de necesidad excepcional (artículo 15).

- Excepciones para microempresas y pequeñas empresas

La Data Act contempla un régimen de exclusión parcial y condicional para determinadas categorías de empresas en función de su tamaño. El objetivo es evitar cargas desproporcionadas para las organizaciones de menor escala económica, esto es:

a) Exclusión general de micro y pequeñas empresas como obligadas a compartir datos: el artículo 7.1 del Reglamento establece que los fabricantes de productos conectados o proveedores de servicios relacionados que sean microempresas o pequeñas empresas, en el sentido del anexo de la Recomendación 2003/361/CE, no están obligados a facilitar el acceso a los datos generados por dichos productos o servicios.

Esto significa que:

- No se les exige implementar interfaces de acceso a datos para usuarios o terceros.
- Tampoco están obligadas a diseñar productos conforme a los requisitos técnicos de acceso establecidos en el artículo 3.
- Están exentas del régimen de condiciones FRAND y de compensación regulado en el artículo 9.

Dicha exención aplica siempre que no pertenezcan a un grupo de empresas que supere los umbrales establecidos en dicha Recomendación. Es decir, si forman parte de un grupo empresarial con alguna entidad que supera esos umbrales, la exención no será aplicable.

A estos efectos, la Recomendación 2003/361/CE establece los siguientes límites:

- Microempresa: menos de 10 empleados y volumen de negocios o balance general ≤ 2 millones €.

- Pequeña empresa: menos de 50 empleados y volumen de negocios o balance ≤ 10 millones €.

Lo anterior no obsta que sí estén obligadas a compartir datos B2G en caso de emergencia pública con determinadas administraciones cuando "dichos datos por medios alternativos de manera oportuna y efectiva en condiciones equivalentes".

II.- FAQS de la Comisión Europea

Las FAQs de la Comisión Europea, actualizadas el 3 de febrero de 2025, aportan clarificaciones desde una perspectiva práctica, entre otras:

- Ámbito temporal: los derechos de acceso se activan únicamente después del 12.9.2025, no sobre datos anteriores.

- Prohibición de uso por parte del titular, salvo contrato expreso con el usuario, y acceso solo por el propio usuario a datos granulares (otros pueden recibir sólo datos agregados).

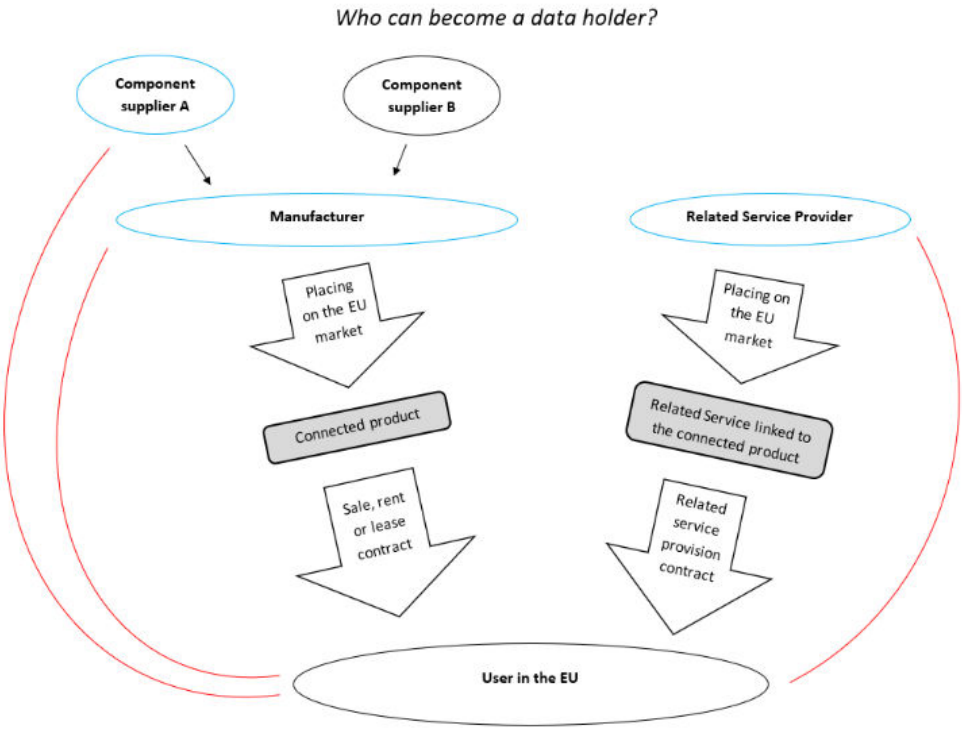
- Obligación de mantener la calidad y formato, equivalentes a los que el titular se reserva internamente o según estándares sectoriales.

- Aplicación de tecnologías de privacidad (PETs): la FAQ 13 aclara que, como se explica en el Considerando 8, la seudonimización y el cifrado desempeñan un papel importante en la aplicación de la Ley de Protección de Datos. La seudonimización o anonimización de los datos personales puede lograrse mediante la aplicación de tecnologías de mejora de la privacidad (PETs). No se puede concluir que los datos resultantes de la aplicación de PETs deban tratarse como datos inferidos o derivados únicamente por la aplicación de estas tecnologías.

- Los modelos contractuales estándar (SCC y MCT) están siendo preparados por la Comisión para *cloud* y acceso a datos, aunque serán no vinculantes y voluntarios.

- Los fabricantes suelen ser titulares de datos, pero no siempre es así. Por ejemplo, en el caso de que un fabricante subcontrate a otra entidad la función de titular de datos para la totalidad o parte de sus productos conectados. Además, un titular de datos que no sea fabricante podría ser una empresa que presta un servicio relacionado con un producto conectado. Esto significa que la empresa que ofrece el servicio relacionado podría ser titular de datos y ser distinta de la empresa que realmente fabricó el

producto conectado. Determinar quién es el titular de datos no depende de quién produjo el hardware o el software, sino de quién controla el acceso a los datos fácilmente disponibles, esto es, gráficamente:



III.- Algunos aspectos controvertidos

La distinción técnica entre datos personales y no personales puede ser compleja, especialmente en contextos mixtos (vehículos conectados, IoT). Las empresas tendrán dificultades técnicas y jurídicas para segregarlos de forma adecuada. Asimismo, la exclusión de los datos derivados/inferidos deja margen para el debate: definir cuándo una transformación puede calificarse como "derivada" no siempre es obvio, y puede generar conflictos interpretativos.

Por otro lado, los modelos contractuales de la Data Act son no obligatorios, lo que podría derivar en cierta disparidad de prácticas y falta de uniformidad entre Estados miembros, hasta que la Comisión o el EDIB promuevan buenas prácticas armonizadas.

IV.- Relación entre la Data Act y el RGPD[2]

1.- Principio de primacía del RGPD

La Data Actreconoce expresamente que *"no afecta ni al RGPD ni a la Directiva ePrivacy"* y que, en caso de conflicto irreconciliable, prevalecerán estas normas de protección de datos sobre cualquier disposición del Data Act. Ambas normas comparten el mismo rango jerárquico, pero cuentan con cláusulas de conflicto que garantizan la primacía del RGPD cuando sea necesario para proteger datos personales.

A estos efectos, resulta útil establecer una comparativa entre distintos conceptos de la Data Act cuya definición puede entrar en conflicto con las del RGPD:

[2] Basado en el artículo de Sergi Ariño en el blog de Citizen8: https://citizen8.eu/la-data-act-ya-esta-aqui-y-el-silencio-es-ensordecedor/.

Concepto	DATA ACT	RGPD	OBSERVACIONES
Datos	"Cualquier representación digital de actos, hechos o información y cualquier compilación de tales actos, hechos o información, incluso en forma de grabación sonora, visual o audiovisual" (art. 2.1).	No define "datos" en general.	La Data Act define datos de modo tecnológicamente neutro e incluye datos personales y no personales. El RGPD solo regula datos personales.
Datos personales	Remite a la definición del RGPD art. 4.1	"Toda información sobre una persona física identificada o identificable..."	La Data Act no redefine; integra el concepto del RGPD. Cuando se apliquen ambos, prevalece el RGPD para el tratamiento de datos personales.
Datos no personales	"Aquellos que no sean datos personales" (art. 2.4).	-	Categoría en la Data Act; clave porque gran parte de las obligaciones (p. ej., B2B/B2C, cambio de proveedor cloud) afectan a todo tipo de datos, con salvaguardas adicionales para los personales.
Tratamiento	"Toda operación o conjunto de operaciones realizadas sobre datos o conjuntos de datos... recogida, registro, organización... consulta, utilización, divulgación, interconexión, limitación, supresión o destrucción" (art. 2.7).	Definición casi idéntica pero referida a datos personales (art. 4.2).	En la Data Act el término se aplica a cualquier dato, no solo personales. En RGPD, el mismo elenco de operaciones queda circunscrito a datos personales. Atención al riesgo de confusión terminológica en contratos.
Interesado	"El interesado tal como se indica en el art. 4.1 del RGPD".	Definido en art. 4.1 RGPD junto con "datos personales".	La Data Act remite al RGPD; no crea un concepto distinto.
Titular de los datos (data holder)	"Persona física o jurídica que tiene el derecho o la obligación, con arreglo al presente Reglamento, al Derecho de la Unión o a la normativa nacional conforme al Derecho de la Unión, de utilizar y poner a disposición datos, incluidos los extraídos o generados durante la prestación de un servicio relacionado" (art. 2.13).	-	Figura propia de la Data Act. No equivale al «responsable del tratamiento» del RGPD: el titular puede ostentar un derecho/obligación sobre datos personales o no personales (p. ej., fabricante de un producto conectado), mientras que el responsable decide fines y medios del tratamiento de datos personales. En la práctica, un mismo sujeto puede ser titular de datos y, a la vez, responsable RGPD.
Destinatario de datos	"Persona física o jurídica que actúa con un propósito relacionado con su actividad comercial... distinta del usuario... a la que el titular pone datos a disposición o a la que un tercero los pone en virtud del Derecho de la Unión o nacional" (art. 2.14).	"Persona física o jurídica... a la que se comuniquen datos personales, se trate o no de un tercero", con exclusión de autoridades públicas cuando reciban datos en una investigación concreta (art. 4.9).	En la Data Act el concepto abarca cualquier dato y se inserta en esquemas B2B/B2C de puesta a disposición con condiciones FRAND, en el RGPD se centra en la comunicación de datos personales a cualquiera distinto del responsable.
Usuario (user)	"Persona física o jurídica que posee un producto conectado o a la que se le han transferido derechos temporales de uso, o que recibe servicios relacionados" (art. 2.12).	-	Actor central del Data Act: obtiene derecho de acceso a los datos generados por el uso del producto/servicio.
Servicio de tratamiento de datos	"Servicio digital... que permite acceso de red ubicuo y bajo demanda a un conjunto compartido de recursos informáticos... de carácter centralizado, distribuido..." (art. 2.8).	-	No confundir con "tratamiento" del RGPD. La Data Act regula, entre otros, cambio de proveedor y portabilidad de estos servicios (arts. 23-31).
Datos del producto / de servicios relacionados	"Datos generados por el uso de un producto conectado..." (art. 2.15) / "Datos que representan la digitalización de acciones del usuario o eventos relacionados con el producto conectado..." (art. 2.16).	-	Categorías funcionales propias del Data Act que delimitan el derecho de acceso/compartición del usuario y las obligaciones del titular.
Elaboración de perfiles	Remite al RGPD art. 4.4.	"Cualquier forma de tratamiento automatizado... para evaluar aspectos personales de una PF...". Art. 4.4.	Misma noción, si hay datos personales, rige RGPD.

Como vemos, la definición de "datos" en la Data Act incluye automáticamente los datos personales, lo que implica que todo tratamiento efectuado bajo ese marco ha de sujetarse al RGPD. Si en un mismo conjunto de datos existen datos personales y no personales indisolublemente vinculados, el RGPD debe prevalecer en su tratamiento.

2. La Data Act no es una base jurídica independiente

El Reglamento de Datos no constituye una base legal (art. 6.1) RGPD) autónoma para el tratamiento de datos personales. Simplemente impone obligaciones de compartir datos entre titulares y usuarios o terceros designados. La legitimidad del tratamiento debe apuntalarse siempre en una base conforme al artículo 6 del RGPD (consentimiento, contrato, interés legítimo, etc.). Lo anterior es aplicable tanto para el acceso a los datos por parte de los mismos interesados como en relación con las comunicaciones de datos a terceros que puedan producirse.

3. Rol del usuario como responsable del tratamiento

Cuando el usuario de datos no es el interesado, se le considera responsable del tratamiento conforme al RGPD. En tal caso, si solicita datos personales, debe contar con una base jurídica clara (ej. consentimiento, interés legítimo, contrato) e incluir la Evaluación de Impacto (EIPD) o medidas pertinentes, en función del riesgo. Asimismo, puede ocurrir que, en algún supuesto, el titular de datos y el usuario sean corresponsables, lo que requerirá un acuerdo contractual detallado que delimite responsabilidades en materia de protección de datos.

4. Privacidad por diseño, anonimización y seudonimización

En base al principio de privacidad desde el diseño y por defecto (Art. 25 RGPD), los responsables deben implementar técnicas como la seudonimización o anonimización, especialmente cuando transmitan datos no estrictamente necesarios o identificativos. A estos efectos, debe recordarse que la propia anonimización es un tratamiento en sí mismo y, consiguientemente, requiere de una base de legitimación y/o, en su caso, poder acreditar que se considera un tratamiento "compatible" con el principal.

Gerard Espuga Torné
Abogado.
gerardespuga@betalegal.com