EU Data Act (DA)

TaylorWessing

Purpose

The Data Act promotes equitable and dependable access to data generated by the use of connected devices and related services, aiming to remove barriers for both consumers and businesses in accessing this data. It establishes universal principles for data sharing applicable across various industries, enhancing data sharing between businesses and with consumers. The Data Act does not alter existing data access obligations (such as under the GDPR).

Key objectives of the Data Act include:

- Empowering users of connected devices.
- Boosting data availability for business innovation.
- Enabling public sector data reuse in critical situations.
- Enhancing the cloud/edge computing sectors' trust and fluidity.
- Laying down a framework for data interoperability across sectors.

Scope

The Data Act applies to data from connected products or services in the EU, impacting manufacturers, service providers, data holders, and processing providers globally, while users and data recipients must be in the Union. It also covers public sector bodies and participants in data spaces within the EU.

Application

The Data Act came into force on 11 January 2024. The compliance deadline for the bulk of obligations is September 2025.

	B2C and B2B data sharing	B2G data sharing	Switching between data processing services	Safeguards on access to data in an international context
Access to data	The Data Act introduces rights for both individuals and companies to access and share data generated from connected products and/or related services, including IoT devices. This data portability covers personal and non-personal data. Upon request, data holders must make certain data accessible to the user and (at the user's request) share this data with third parties, thereby enhancing user control over data they have generated.	The Data Act allows public sector access to enterprise-held data for urgent needs, specifically for: ■ Responding to public emergencies. ■ Prevention and recovery efforts from such emergencies. Public authorities may obtain data through market transactions or alternative methods under the Act.	The Data Act stipulates the minimum regulatory requirements to facilitate customers switching between providers of data processing services quickly smoothly, and without losing any data or functionality.	Public authorities or private institutions in non-EU countries may request access to non-personal data held in Europe. If an international agreement, such as a mutual legal assistance treaty, exists between the EU or a Member State and the third country, court decisions or administrative requests requiring access to such data are binding. In the absence of such an agreement, non-personal data can only be transferred if the reasons and proportionality of the decision are clearly outlined, a formal decision or judgment exists, a sufficient link to specific suspected persons or infringements is established, and the request allows for judicial review in the third country while ensuring EU legal protections are respected. Only the minimum necessary data may be provided, and the provider must inform the customer before complying, unless doing so would compromise ongoing law enforcement activities.
Restrictions and limitations	The Data Act: ■ Applies only to readily accessible data without involving disproportionate effort or breaching the Trade Secrets Directive. ■ Prohibits data use for developing competing products. ■ Exempts micro/small enterprises from data access obligations. ■ Bars 'gatekeepers' under the DMA from accessing user data and maintains the integrity of voluntary data sharing agreements.	The prevention, investigation, detection, and prosecution of criminal or administrative offenses are explicitly excluded from the scope of exceptional needs.	N/A	The Data Act states that the sui generis right established in the Database Directive, does not apply to databases containing data from or generated by the use of IoT products or related services.
Obligations	■ Data needs to be available under fair, reasonable, and non-discriminatory terms, and in a transparent manner. ■ Data holders may receive compensation for making data available (subject to compliance with transparency obligations on its calculation methods). ■ An unfairness test might be conducted in certain cases to protect micro-enterprises and SMEs.	Businesses that are data holders: ■ Must provide data promptly and without charge. ■ Can receive compensation for costs incurred in data sharing, plus a reasonable margin. Public Bodies that are data holders are authorised to share data with entities for scientific research, analytics, or other institutional purposes.	Providers must: ■ Remove barriers to terminating contracts. ■ Detail switch obligations in contracts. ■ Transfer data within 30 days, ensuring smooth migration and functional consistency. ■ Lower switching costs. ■ Follow interoperability standards or export data in common formats.	Providers of data processing services must implement appropriate technical, legal, and organisational measures, including contractual agreements, to prevent the international transfer or governmental access to non-personal data stored within the Union.