

Data Act: Data sharing and competitiveness

The Data Act aims to create value from data generated by connected products and services, by introducing data-sharing obligations. The principles enshrined in the Act have received general approval, but concerns have been expressed about the clarity of certain definitions, the sharing of commercially sensitive data and its regulatory complexity. Most provisions of the Data Act will apply from 12 September 2025.

Why it matters

Combining data with next-generation connectivity and emerging technologies can boost productivity, improve citizens' health and wellbeing, and enhance public services. The [EU's data economy](#) is projected to reach €630 billion this year, accounting for 4.7 % of the EU's GDP. Forecasts suggest it will range between €743 billion and €908 billion by 2030. To unlock the full potential of data, the European Commission introduced the [European strategy for data](#) in 2020. This initiative aimed to create a single market for data, ensuring the EU's competitiveness and data sovereignty. The strategy's core components were the [Data Governance Act](#) (DGA) and the [Data Act](#).

The Data Act in short

While the Data Governance Act establishes a new data governance model, enabling voluntary data sharing across the EU, the [Data Act](#) clarifies the rules for creating value from data and introduces data-sharing obligations. [The Data Act](#) grants businesses and legitimate users of connected products and services the right to access the data – both personal and non-personal – generated through their use. This concerns, for example, data from smart home appliances or industrial data. Manufacturers must ensure the exercise of these rights and create a secure, timely and interoperable data access. This means that manufacturers do not have exclusive rights over data generated by connected machines and devices, which would encourage competition and innovation and improve service options for consumers. Access to data could also enable machine-learning technologies, such as artificial intelligence, to use such data for improving supply-chain management or industrial and agriculture production processes.

The data-sharing obligation gives users the right to transfer their data. For example, they can share it with a repair provider other than the device maker, which could create more competition in the after-sale market and extend the lifespan of machines and devices. However, the data-sharing obligation protects confidentiality, and manufacturers can stop sharing or refuse to share data if it risks exposing trade secrets.

The Data Act introduces new requirements on cloud service providers to ensure customers can easily switch between different providers. It also gives the public sector access to private companies' data in exceptional cases, such as public emergencies, or to fulfil a specific task defined by law (e.g. statistics) or for specific research purposes. In addition, the Data Act includes safeguards against unlawful international transfers of non-personal data, and promotes the development of interoperability [standards](#) for data sharing and processing, using [Common European data spaces](#). Most provisions of the Data Act will apply from September 2025. The obligation to design connected products in a way to make data directly available to users will apply from September 2026 and removal of cloud switching fees from January 2027.

Challenging implementation

[Stakeholders generally welcomed the Data Act](#), but some [major tech](#) companies opposed it. One of the main concerns remains the complexity of digital regulation and offering clear definitions. Even though the Data Act preserves trade secrets and includes a safeguard to prevent development of competing products from data accessed from connected products, [industry](#) did not embrace sharing of data with enthusiasm. Companies can still challenge data-sharing refusals based on protection of trade secrets, which creates



uncertainty. That is why [startups, scaleups and SMEs](#), in particular, favour an approach adapted to the size of the company, which protects innovation while increasing access for users.

A burden or an opportunity for small companies?

Adapting to the new requirements could represent [costs](#) and administrative burdens for small and medium-sized enterprises (SMEs), although the Data Act aims to help SMEs access data held by large companies, encouraging data-driven innovation. To support this, the EU has [developed](#) model contractual terms (MCTs) for data sharing and standard contractual clauses (SCCs) for cloud computing. These voluntary tools will help smaller companies to negotiate and protect them from unfair contracts. MCTs and SCCs were adopted by the [Commission expert group](#) and the Commission 'shall develop and recommend' them '[before 12 September 2025](#)'. They define the roles and responsibilities of data holders and users, compensation for data access and protection of trade secrets. As such, they provide legal clarity in complex data-sharing relations. SMEs, which often lack resources to draft complex contracts, can use these templates directly.

Clarity needed: Non-personal or personal, readily available, pre-processed?

The European Data Protection Board has raised [concerns](#) about the legal clarity of the draft MCTs. Its comments relate to the interplay between the Data Act and the [General Data Protection Regulation](#) (GDPR). The Data Act complements the GDPR but does not override it, and when [personal data](#) is concerned the GDPR prevails. Therefore, clarity in defining who is the data holder and user and which data is considered personal and which non-personal, is decisive. [Experts](#) note that roles, rights and obligations remain unclear. Consequently, companies must carefully decide which law applies when users submit data requests, to ensure compliance. Moreover, according to other [experts](#), the type of data that is within the scope of the law is also ambiguous. Definitions such as data being 'readily available without disproportionate effort' lack clarity, and the difference between data that is pre-processed (within the scope of the law) and processed (outside its scope) also seems vague.

Importance of enforcement

Under the Data Act, Member States need to appoint [competent authorities](#) to enforce the law, but only a [few countries](#) have done this [so far](#). Data protection authorities retain competence for addressing breaches of personal data rules. Member States can appoint the same authority for [the enforcement](#) of two regulations simultaneously: for example, the GDPR and the Data Act regulations, the [AI Act and Data Act](#), or a new, separate authority for the enforcement of the Data Act. Creating new authorities risks inconsistent enforcement, as different bodies interpret the rules differently, so a single authority would simplify compliance for companies. National interpretations and enforcement will ultimately shape the law's impact. While this creates an additional uncertainty regarding its practical application, [stakeholders](#) note that it also offers an opportunity to shape the enforcement landscape.

What's next?

As part of the [digital package](#), the Commission has announced a new [European Data Union Strategy](#). The strategy aims to simplify the EU's digital regulatory framework and boost data sharing by leveraging data to enhance competitiveness. It remains to be seen to what [extent](#) the Data Act will be part of the simplification strategy. Several major companies have requested the Commission to [revise](#) the Data Act and postpone its application, as part of this strategy.