

EU Data Act: 101

By IAPP European Operations Coordinator Laura Pliauskaite

Purpose of the Data Act

The Data Act creates new rules on who can access and use data generated in the EU across all economic sectors. It aims to ensure fairness in the allocation of value from data, stimulate a competitive data market, open opportunities for data-driven innovation and make data more accessible to all users. It focuses primarily on industrial, nonpersonal data but is relevant to data protection.

Key changes the Data Act brings

- Providing data access and use rights to users of connected devices and their chosen third parties, while protecting trade secrets and intellectual property.
- Making originally restricted data available for use to specified groups, including small and medium-sized companies, researchers and public bodies in cases of public emergencies.
- Setting new requirements that govern compensation for data use, portability between data processing services and safeguards for nonpersonal data transfers to third countries.

Key challenges posed by the Data Act

- Consistency with personal data protection rules under the EU General Data Protection Regulation, such as those on international transfers, especially where organizations process mixed datasets of personal and nonpersonal data.
- Consistency with other existing instruments, including the Data Governance Act and the Digital Markets Act, as well as the future instruments such as the AI Act.
- Potential friction between Data Act requirements and contractual, competitiveness and trade secret protection rights.

Important dates

- The Data Act enters into force 11 Jan. 2024, and is applicable as of 12 Sept. 2025:
 - Provision on design and manufacturing requirements for simplified data access applies to connected products and related services placed on the market after 12 Sept. 2026.
 - Provisions on unfair contractual terms apply to contracts concluded after 12 Sept. 2025. Such provisions apply from 12 Sept. 2027 to specific contracts concluded on or before 12 Sept. 2025.
 - Provisions concerning statutory data sharing obligations apply regarding EU law or national legislation adopted in accordance with it, which enters into force after 12 Sept. 2025.
- Member states must inform the European Commission about national rules concerning penalties for noncompliance by 12 Sept. 2025.
- The European Commission must develop and recommend nonbinding model contractual terms on data access and use, and nonbinding standard contractual clauses for cloud computing contracts by 12 Sept. 2025.

Additional resources

- [Data Act published in the Official Journal of the European Union.](#)
- [A view from Brussels: EU formally adopts Data Act.](#)
- [Council of the European Union adopts Data Act.](#)

FOCUS AREAS	DATA ACT
ENTITIES WITHIN SCOPE	<p>The Data Act applies to:</p> <ul style="list-style-type: none">→ Manufacturers of connected products, suppliers of related services placed on the market in the EU and their users.→ Data holders that make data available to data recipients in the EU, and such data recipients.→ Member states' public sector bodies and EU institutions, agencies or bodies that request data holders make data available when there is an exceptional need, and the data holders that provide such data in response.→ Providers of data processing services, including cloud services, offering such services to customers in the EU.→ Participants in data spaces, vendors of applications using smart contracts and persons commercially deploying smart contracts for executing data sharing agreements.
COVERED DATA	<p>The Data Act applies primarily to nonpersonal data, specifically data:</p> <ul style="list-style-type: none">→ Generated through the use of connected products or related services, including the metadata necessary to interpret and use that data, and data produced by a related virtual assistant.→ Processed by data processing services such as cloud and edge services.→ Held by the private sector that is necessary to respond to a public emergency or for the performance of a specific task carried out in the public interest. Nonemergency cases only cover nonpersonal data.
KEY REQUIREMENTS	<p>Data holders must:</p> <ul style="list-style-type: none">→ Make data generated through connected products and related services accessible to the user, directly when possible, and the user's chosen third-party; design and manufacture these products and services to ensure data accessibility. Data protected as trade secrets must only be disclosed if confidentiality is preserved by all parties involved. Unfair contractual terms on data access and use are deemed invalid.→ Make data available to a public sector or EU body in case of an exceptional need, such as a public emergency or public interest task. Under certain circumstances, these bodies may share the data for noncommercial scientific research or statistical and analytical purposes.→ Provide data to the user and, in case of a public emergency, the public sector free of charge, and to the data recipient for a contractually agreed reasonable compensation, considering the financial efforts put into its collection, production and accessibility, the size of the data recipient's enterprise, the European Commission guidelines, etc.→ Refrain from using data generated by a connected product or related service to derive insights about the economic situation or undermine the commercial position of the user. <p>The user and/or the third parties receiving data at the request of the user must:</p> <ul style="list-style-type: none">→ Not use the data received in a manner that impairs the security of a connected product or related service. They must also not use or share it to develop a competing product.→ Process the data made available only as agreed upon with the user and subject to law on personal data protection, and not for profiling, unless necessary to provide the service requested by the user.→ Not share the data with another third party, unless contractually agreed with the user and given the confidentiality of trade secrets is preserved, or with a gatekeeper as designated by the Digital Markets Act, and not prevent the user from sharing data with other parties. <p>Data processing service providers must:</p> <ul style="list-style-type: none">→ Enable their customers to switch to a different data processing service provider covering the same service type or use several providers at the same time by removing commercial, technical, contractual and organizational obstacles.→ Take technical, legal and organizational measures to prevent international and third-country governmental access and transfers of nonpersonal data held in the EU when that transfer or access would conflict with existing laws, except in the case of an international agreement. In the absence of such agreement, the transfer may only take place if certain conditions are adhered to. <p>Participants in data spaces, data processing service providers, vendors of applications using smart contracts and persons commercially deploying smart contracts for executing data sharing agreements must meet interoperability requirements.</p>
DISPUTES AND ENFORCEMENT	<p>Member states must establish penalty frameworks for infringements and designate new or existing national competent authorities for application and enforcement. The authorities have the ability to:</p> <ul style="list-style-type: none">→ Investigate complaints of alleged violations and coordinate with another competent authority if necessary.→ Impose financial penalties, including periodic or retroactive penalties.→ Initiate legal proceedings for the imposition of fines.→ Monitor technological developments for making data available and its use. <p>Users, data holders, data recipients, and customers and providers of data processing services may utilize certified dispute-settlement bodies to settle disputes concerning certain rights and obligations regarding data access, use and sharing, as well as switching data processing services. Dispute-settlement bodies must issue their decision within 90 days of receipt of a request for a decision.</p>