Data Act Glossary

July 2026

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

B

C

compensation
Compensation for making data available:

Data holders can request reasonable compensation for making data available to data recipients.

- Any compensation must be non-discriminatory and reasonable and may include a margin.
- When determining any compensation, the costs incurred in making the data available (including the costs for formatting, dissemination and storage) and investments in the collection and production of data must be taken into account.
- However, microenterprises, SMEs and not-for-profit research organisations must not be charged more than the costs incurred in making the data available.
- Data holders must make the calculation of the compensation transparent to data recipients.

The European Commission plans to publish guidelines on calculating reasonable compensation.

Compensation for making data available in cases of an exceptional need:

In the case of a public emergency, data holders do not receive any compensation unless they are a microenterprise or small enterprise.

If the data requested are necessary for the fulfilment of a task carried out in the public interest that has been provided for by law, all data holders are entitled to fair compensation.

- The compensation must cover the technical and organisational costs (including the costs of data anonymisation, etc) and may include a reasonable margin.

- Data holders are not entitled to compensation if the task carried out in the public interest is the production of official statistics and if the purchase of data is not allowed by national law.
- Upon request by the public sector body, the European Commission, the European Central Bank or the Union body, data holders must provide information about the basis for the calculation of the costs and the reasonable margin.
- If the public sector body, the European Commission, the European Central Bank or the Union body disagrees with the level of compensation requested by a data holder, it can lodge a complaint with the Bundesnetzagentur.

connected product
Connected products are objects that can record data about their use, performance or environment (in particular through sensors) and transmit the product data via a cable-based or wireless connection (for example via an internet connection such as WLAN or 5G or another type of access such as a USB port or an NFC interface). The products covered by this definition are mostly products that are commonly referred to as Internet-of-Things (IoT) devices and that exchange data via the internet.

Connected products can be found in all areas of the economy and society and include infrastructure, vehicles, ships, aircraft, lifestyle equipment, home equipment and consumer goods, medical and health devices, and agricultural and industrial machinery.

> Examples of connected products
>
> Connected products can be found in various product categories, including smart household appliances (such as fridges, fire alarms, door locks), smart electronic equipment (such as televisions and smartwatches), connected vehicles (such as cars and aircraft), , medical devices (including monitoring and diagnostics), connected industrial machinery (such as robots, wind turbines, pumps and agricultural machinery). Connected products do not include products whose main function is to store, process or transmit data (such as servers and routers) or prototypes.

D

data access
Direct data access:

If direct data access is enabled, connected products must be designed so that the data can be directly retrieved from the data storage medium on a device (via an interface such as cable or Bluetooth) or via a server (such as a digital interface). A user can then directly retrieve the data for the product without the need for any further or additional action by the data holder. Data must be made “easily” available to users and third parties. This means that access must be granted in a simple way and without undue obstacles, costs or procedural hurdles. The product design obligation applies to connected products and related services placed on the market after 12 September 2026, provided that direct access is relevant and technically feasible.

Indirect data access:

If users cannot retrieve the data directly from the product (for technical reasons, etc), the data holder must enable indirect access. In this case, the user has to ask the data holder for access to the data (for example via an appropriate web portal). The data holder must also make the relevant data available to third parties at the user's request. In general, accessing the data should be made as easy as possible.

Data Act
The Data Act entered into force as an EU Regulation on 11 January 2024 and became applicable in the European Union on 12 September 2025. The Data Act is a key pillar of the European Commission's European strategy for data alongside the Data Governance Act.

The Data Act aims to boost Europe's data economy. One of its main objectives is to increase data-based value creation and promote innovation in Europe.

Data from connected products and related services are at the centre of the Data Act. Connected products within the meaning of the Data Act are mostly Internet-of-Things (IoT) devices. These devices include connected vehicles, trains, aircraft, household appliances, industrial and agricultural machinery, production units and private terminal equipment. Related services are software (such as apps) used to control these devices. The Data Act puts users in the focus of data-based value creation. It establishes new data access, use and sharing rights for users for their connected products and related services.

The Data Act specifies under which conditions certain terms in contracts related to data access and use between enterprises are unfair and therefore not binding.

The Data Act also lays down rules and relevant interoperability requirements that make it easier for customers of data processing services to switch from one data processing service to another or use several data processing services at the same time. Data processing services are mostly cloud services.

In cases of an exceptional need, data covered by the Data Act must be made available to public sector bodies such as authorities or bodies governed by public law.

The Data Act also establishes rules to protect non-personal data held in the European Union from unlawful access by and transfer to third-country governmental authorities.

data holder
A data holder (typically a manufacturer) is a natural or legal person with product data or related service data at their disposal. It is not a question of who has manufactured individual (software or hardware) components but rather who has the right or obligation to use data or make data available. Users must be informed in advance (for example before they buy a product) who the data holder is, in other words who is required to provide the data.

data processing service
The term "data processing service" is defined in Article 2(8) of the Data Act. It covers a large number of digital services with a very large range of different application purposes, functions and technical structures. The definition mirrors common definitions of cloud computing services. It was designed to also cover the popular delivery models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). It is also a condition that the service is provided to a "customer" within the meaning of Article 2(30) of the Data Act and is used as such. It does not, therefore, include services where only a function made possible by data processing is

used, such as music or video streaming. There is, however, openness to future technological innovation in the field of data processing service delivery.

Not all services are covered by the full set of switching and interoperability rules. Article 31 of the Data Act provides for exemptions from obligations. Exemptions apply to:

- data processing services that have been designed or developed to accommodate individual needs and that are not offered on a broad commercial scale; and
- data processing services that are provided as a test version for a limited period of time.

However, this does not mean that custom-built services are fully exempt from the scope of Chapter VI (Article 30(5) in conjunction with Article 31(1) of the Data Act). Providers of custom-built services must, for example, make open interfaces available and ensure that data are exported in a structured, commonly used and machine-readable format.

Providers making use of exemptions are obliged to properly inform their customers before concluding a contract about the obligations of Chapter VI of the Data Act that do not apply to them.

data recipient/third party
A data recipient, or third party, can generally be any natural or legal person other than the actual user of the connected device or related service. A data recipient can therefore be an enterprise commissioned by the user to develop new applications (for example aftermarket and ancillary services such as analysis, repair and maintenance services) on the basis of the data provided. A data recipient can generally also be a competitor of the data holder. However, third parties are not allowed to use the data provided to develop products that compete with the connected product. One general exception is made for enterprises designated as gatekeepers under the Digital Markets Act (DMA): these enterprises may not obtain any data on the basis of the Data Act on account of their dominant market positions. An up-to-date list of designated gatekeepers is available at https://digital-markets-act.ec.europa.eu/gatekeepers_en.

dispute settlement
Parties can agree to settle certain disputes about rights and obligations under the Data Act in an out-of-court dispute settlement procedure involving certified dispute settlement bodies. This is a simple, swift and cost-effective way of settling disputes arising about rights or obligations under the Data Act.

E

F

G

H

I

interoperability
Interoperability is a basic building block of the Data Act and generally describes the ability of all participants in a data space to exchange and use data safely and securely. The use of common (standardised) protocols and semantic representation of data ensures that all participants also interpret the data correctly.

in-parallel use of data processing services
The provisions of Article 34 of the Data Act aim to facilitate the in-parallel use of data processing services and to further reduce barriers to multi-cloud and multi-service applications. The objective is to ensure interoperability between different services and enable the simultaneous use of several providers.

J

K

L

M

medium-sized enterprise
An enterprise that employs fewer than 250 persons and has an annual turnover not exceeding €50mn or an annual balance sheet total not exceeding €43mn and that is not a microenterprise or a small enterprise (Commission Recommendation 2003/361/EC).

microenterprise
Up to nine employees and up to €2mn annual revenue/annual balance sheet total (Commission Recommendation 2003/361/EC).

N

O

out-of-court dispute settlement body
Out-of-court dispute settlement bodies are independent, non-governmental bodies. They have a high level of expertise and are required to carry out their work in an impartial, swift and fair manner, based on transparent rules. The quality of a dispute settlement body's work is ensured through certification by the competent governmental supervisory authority in the Member State where the dispute settlement body is established. In Germany, these bodies are formally certified by the Bundesnetzagentur. Parties are generally free to select any dispute settlement body in the European Union that has been certified by a competent supervisory authority. The European Commission publishes a list of all certified dispute settlement bodies in the European Union; the list will also be made available here.

It is generally possible for all users, data holders, data recipients and providers of data processing services and their customers to have access to out-of-court dispute settlement. The dispute settlement procedure is a voluntary procedure. Dispute settlement by a certified dispute settlement body is therefore only possible if the parties agree to the procedure. In addition, a decision by a dispute settlement body is only binding for the parties if the parties explicitly agree to the decision being binding before the dispute settlement procedure begins.

P

placing on the market
"Placing on the market" means the first making available of a connected product on the Union market. Making available means the permanent or temporary transfer or granting of property and usage rights, in particular through sales, rental or leasing contracts. If, for example, a manufacturer sells or rents out a connected product to a user in the European Union for the first time after the manufacturing stage, the product is considered as having been placed on the market in the European Union.

- A connected product can be placed on the market only once.
- The concept of placing on the market refers to each individual product, not to a type of product.
- In the case of connected products that have been placed on the market in the European Union but are used in third countries, both the data generated in Europe and the data generated outside Europe must be made available. However, only users established in the European Union may request provision of the data. In the case of an aircraft belonging to a European airline, for instance, the data generated by the aircraft in third countries outside the EU must also be made available.
- The rules do not cover products that have been bought in a third country and imported into the European Union or products that have been produced in the European Union for export and placed on the market outside the European Union. A smartwatch bought in the US and brought to the European Union afterwards, for example, is therefore considered as having been placed on the market in the US.

product data
Data obtained, generated or collected by a connected product relating to the product's performance, use or environment, for example via integrated sensors. It must actually be possible for the data to be retrieved from the product.

public emergency
A public emergency means a situation declared as such under national or Union law. A public emergency can be a public health emergency resulting from a natural disaster or a human-induced disaster such as a cybersecurity incident. A public emergency is an exceptional situation that is limited in time, negatively affects the population and, for instance, also substantially and immediately increases the risk of serious and lasting repercussions for living conditions and economic or financial stability.

Q

R

readily available data
Product data and related service data that a data holder can obtain without disproportionate effort.

related service
A related service is a service that is linked to a connected product and affects the functionality of the product, for example by transmitting data or commands. There is therefore a bidirectional exchange of data between the connected product and the related service. Services that can only retrieve data are not considered to be related services.

> Examples of related services
>
> These include services that influence a connected product in a certain way, such as an app to adjust the brightness of lights or regulate the temperature of a smart fridge or an app for smartwatches that records and analyses sports activities.

related service data
Data of a related service representing actions and events relating to the use of a connected product.

right to lodge a complaint
Natural and legal persons have the right to lodge a complaint with the competent authority responsible for their habitual residence, place of work or establishment if they consider that their rights under the Data Act have been infringed (Article 38(1) of the Data Act).

Irrespective of this right to lodge a complaint, it is always possible for players to take civil action within the framework of their contractual relationships.

S

same service type
The provisions on switching between data processing services only apply if the provider from which and the provider to which a customer is switching cover the "same service type" (Article 23 of the Data Act). According to the definition in Article 2(9) of the Data Act, this means that the data processing services must share the same "primary objective", the same "main functionalities" and the same data processing service model.

small enterprise
Up to 49 employees and up to €10mn annual revenue/annual balance sheet total (Commission Recommendation 2003/361/EC).

smart contract
The Data Act promotes the automated and interoperable execution of data use contracts by laying down essential requirements regarding smart contracts. Smart contracts are computer programs used for the automated execution of a contract or part of a contract (Article 2(39) of the Data Act). The Data Act lays down the following requirements for vendors of smart contracts in Article 36(1):

- robustness to avoid functional errors and withstand manipulation by third parties;
- mechanisms for the safe termination and interruption of transactions;
- data archiving and continuity;
- strict access control mechanisms.

Setting minimum requirements and, if appropriate, standards aims to promote interoperability between different fields of application for smart contracts. Vendors of smart contracts must perform conformity assessment to demonstrate fulfilment of the essential requirements and, on fulfilment of the requirements, must issue an EU declaration of conformity. The Commission may adopt common specifications covering any or all of the essential requirements (Article 36(6) of the Data Act).

SMEs
Micro, small and medium-sized enterprises (Commission Recommendation 2003/361/EC).

standard
Standards refers to a common approach to solving a problem and, if appropriate, implementing the solution. The aim is to develop open standards that promote manufacturer-neutral and technology-neutral solutions. These include interface requirements (APIs) relating to the data formats, processes or protocols to be used. Data space participants can ensure their own compliance with the essential requirements by complying with and implementing standards.

standard contractual clauses (SCCs)
The European Commission's standard contractual clauses (SCCs) provide a structured, adaptable and legally secure basis for putting the new requirements into practice efficiently, while allowing scope for individual and sector-specific adjustments. The SCCs aim to support customers and providers of data processing services in implementing their rights and obligations under the Data Act in contracts. They are suitable for all cloud models (IaaS, PaaS and SaaS) and provide model clauses that providers can include in their individual contracts. Use of the SCCs is voluntary.

Structure of the SSCs:

- The SCCs consist of modular clauses that can be used as a complete set or separately.
- They are not intended as a full contract but as a supplement to a comprehensive contract for data processing services. Other aspects outside the scope of the Data Act need to be set out in additional clauses.
- An integral part with definitions based on the Data Act aims to ensure uniform interpretation.
- For ease of reference, the SCCs include cross-references that link certain clauses to relevant provisions in the Data Act or to other clauses.

Flexibility:

- Although not necessary, the European Commission recommends using the entire set of modular clauses.
- It is possible to use only some of the clauses or make changes to them, but this requires a careful, legal assessment to ensure that there are no gaps or contradictions.

switching charge
The Data Act includes rules on switching charges, which are the charges that are imposed on users switching to a different provider. These charges will gradually be withdrawn:

- In the transitional period from 11 January 2024 to 11 January 2027, providers may only charge costs that are directly linked to the switching process.
- From 12 January 2027, no switching charges at all may be imposed (Article 29(1) of the Data Act).

Before entering into a contract, providers are required by the Data Act to provide prospective customers with clear information about the standard service fees for operation of a service and the reasonable compensation for early termination that may be imposed and about the reduced switching charges applicable during the transitional period from 11 January 2024 to 12 January 2027 (Article 29(4) of the Data Act).

T

U

user
A user (private, business or public) is a natural or legal person that has a (temporary) right to use a connected product (in particular as a result of purchase, rent or lease) or that uses a related service. The rights under the Data Act only apply to users established in the European Union.

V

W

X

Y

Z