Data Act explained

A comprehensive overview of the Data Act, including its objectives and how it works in practice.

Why the Data Act ?

The Data Act (https://eur-lex.europa.eu/eli/reg/2023/2854/oj) is a law designed to enhance the EU's data economy and foster a competitive data market by making data (in particular industrial data) more accessible and usable, encouraging data-driven innovation and increasing data availability. To achieve this, the Data Act ensures fairness in the allocation of the value of data amongst the actors in the data economy. It clarifies *who* can use *what* data and under *which* conditions.

In recent years, there has been a rapid growth in the availability of products connected to the internet ('connected products') on the European market. These products, which together compose a network known as the Internet-of-things (IoT), significantly increase the volume of data available for reuse in the EU. This represents a huge potential for innovation and competitiveness in the EU.

The Data Act gives users of connected products (businesses or individuals that own, lease or rent such a product) greater control over the data they generate, while maintaining incentives for those who invest in data technologies. In addition, it lays down general conditions for situations where a business has a legal obligation to share data with another business.

The Data Act also includes measures to increase fairness and competition in the European cloud market as well as to protect companies from unfair contractual terms related to data sharing imposed by stronger players. It also establishes a mechanism through which public sector bodies can request data from a business where there is an exceptional need, for example in public emergency situations, and provides clear rules on how such requests should be made. In addition, it introduces safeguards to avoid that government bodies from third countries can access non-personal data where this would go against EU or national law. Finally, the Data Act defines essential requirements regarding interoperability to ensure that data can flow seamlessly between sectors and Member States, facilitated by Common European Data Spaces (https://digital-strategy.ec.europa.eu/en/policies/data-spaces), as well as between data processing services providers.

The Data Act was published in the Official Journal of the EU (https://eur-lex.europa.eu/eli/reg/2023/2854/oj) on 22 December 2023 and it will become applicable on 12 September 2025.

The Data Act complements the Data Governance Act (https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained), the first deliverable under the European strategy for data (https://europa.eu/!7jbCBV). The Data Governance Act became applicable in September 2023. While the Data Governance Act increases trust in voluntary data-sharing mechanisms, the Data Act provides legal clarity regarding the access to and use of data.

Together with other policy measures and funding opportunities, these two regulations will contribute to the establishment of an EU single market for data, making Europe a leader in the data economy by harnessing the potential of the ever-increasing amounts of data, in particular industrial data, for the benefit of the European economy and society.

Issues addressed

Following the general provisions (Chapter I) which set out the scope of the regulation and define key terms, the Data Act is structured into six main chapters:

Chapter II on business-to-business and business-to-consumer data sharing in the context of IoT: users of IoT objects can access, use and port data that they co-generate through their use of a connected product.

Chapter III on business-to-business data sharing: this clarifies the data-sharing conditions wherever a business is obliged by law, including through the Data Act, to share data with another business.

Chapter IV on unfair contractual terms: these provisions protect all businesses, in particular SMEs, against unfair contractual terms imposed on them.

Chapter V on business-to-government data sharing: public sector bodies will be able to make more evidence-based decisions in certain situations of exceptional need through measures to access certain data held by the private sector.

Chapter VI on switching between data processing services: providers of cloud and edge computing services must meet minimum requirements to facilitate interoperability and enable switching.

Chapter VII on unlawful third country government access to data: non-personal data stored in the EU is protected against unlawful foreign government access requests.

Chapter VIII on interoperability: participants in data spaces must fulfil criteria to allow data to flow within and between data spaces. An EU repository will lay down relevant standards and specifications for cloud interoperability.

Chapter IX on enforcement: Member States must designate one or more competent authority(ies) to monitor and enforce the Data Act. Where more than one authority is designated, a 'data coordinator' must be appointed to act as the single point of contact at the national level.

Chapter II: Business-to-business and business-to-consumer data sharing in the context of the IoT market

Why?

A key objective of the Data Act is to **create fairness in the data economy** and **empower users** to reap value from the data they generate using the connected products that they own, rent or lease.

The Data Act enables users of **connected products** (e.g. connected cars, medical and fitness devices, industrial or agricultural machinery) and **related services** (i.e. anything that would make a connected product behave in a specific manner, such as an app to adjust the brightness of lights, or to regulate the temperature of a fridge) to access the data that they co-create by using the connected products/ related services.

The availability of such data will significantly impact the economy. For example, data generated by connected products and related services can be used to boost aftermarket and ancillary services as well as to create entirely new services, benefiting both businesses and consumers.

Examples of connected products: consumer products (e.g. connected cars, health monitoring devices, smart-home devices), other products (e.g. planes, robots, industrial machines).

Example of a related service: a user buys a washing machine and installs an application that allows them to measure the environmental impact of the washing cycle based on the data from the different sensors inside the machine and adjusts the cycle accordingly. This application would be considered a related service.

Examples of aftermarket and ancillary services: repair and maintenance services, data-based insurance.

Types of data in scope

Chapter II of the Data Act on business-to-business and business-to-consumer data sharing applies to **all raw and pre-processed data generated from the use of a connected product or a related service that is readily available to the data holder** (e.g. manufacturer of a connected product/ provider of a related service), in other words data that can be easily accessed without disproportionate effort, going beyond a simple operation. This applies to both personal and non-personal data, including relevant metadata.

Such data includes data collected from a single sensor or a connected group of sensors, such as temperature, pressure, flow rate, audio, pH value, liquid level, position, acceleration or speed.

Inferred or derived data and content (e.g. highly enriched data, audiovisual material) are out of scope. Furthermore, the Data Act is without prejudice to the laws on the protection of intellectual property rights (https://commission.europa.eu/business-economy-euro/doing-business-eu/intellectual-property-rights_en).

For example, if a user watches a film on their connected TV, the film itself is not within scope but data on the brightness of the screen is within scope.

In practice

Chapter II of the Data Act allows **users** (i.e. any legal or natural person who owns, rents or leases a connected product) to access the data that they generate through their use of the connected product or related service. If the user wishes to share this data with another entity or individual ('**third party**'), they can either do so directly or they can ask the data holder to share it with a third party of their choice (excluding gatekeepers under the Digital Markets Act (https://digital-markets-act.ec.europa.eu/legislation_en)). The **data holder** is typically the company that makes the connected product or that provides a related service. A data holder must have a contract with the user (e.g. sales contract, rental contract, related service contract, etc.) defining the rights regarding the access, use and sharing of the data that is generated by the connected product or related service. It is important to note that the data holder cannot use any non-personal data generated by the product without the user's agreement.

By way of example, and bearing in mind that the relevant contract determines the exact roles:

- *A company operates a bulldozer: the data holder would typically be the bulldozer manufacturer, and the user would be the company that operates the bulldozer.*
- *If someone buys a connected fridge and downloads an app that helps them to regulate the optimal temperature for the content of the fridge, there would potentially be two data holders, namely the entity that placed the fridge on the market and the entity offering the related service (the app), and only the one user (the owner of the fridge).*

The Data Act incudes several mechanisms to make it easier for users to be able to make use of these provisions: data holders must provide the user with information on the type of data that they will generate when using the connected product or related service (including the volume, collection frequency, etc.); users should be able to request access to the data through a simple process, and; data holders must make the data available to users for free.

Limitations on the use of the data

So as not to deter businesses from investing in data-generating products, the data obtained cannot be used to develop a **competing connected product**. The Data Act does not prohibit competition in **related** or **aftermarket services**. Furthermore, there is no obligation under the Data Act for a data holder to share data with third parties based outside the EU.

The Data Act is fully **compliant with data protection rules**, notably the GDPR. Where the user is not the data subject whose data is being requested, personal data can only be made available if there is a valid legal basis (e.g. consent). This is an important consideration as the co-generated data often contains both personal and non-personal data, which may be difficult to separate.

It incentivises the development of connected products and services based on new flows of data, which is of particular value to smaller companies. In addition, **micro and small companies**, as manufacturers or providers of related services, are not subject to the same obligations as larger companies.

To protect **trade secrets** without undermining the goal of the Data Act to make more data available, the data holder and the user/ third party may agree on certain measures to preserve the confidentiality of the trade secrets. Where these measures are not respected, the data holder may withhold or suspend the data sharing. The data holder may only refuse to share data where it can demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets.

The data holder and user may agree to limit data sharing if there is a risk that the **security requirements** of the connected product could be undermined, resulting in serious adverse effects to the **health, safety or security of people**. Such requirements must be laid down in EU or national law.

If the data holder suspends, withholds or refuses to share data on the grounds of trade secrets protection or security requirements, it must notify the national competent authority. Users may challenge such a decision, either in front of the competent court or tribunal of a Member State, via a complaint with the competent authority or upon agreement with the data holder in front of a dispute settlement body.

Chapter III: Rules on mandatory business-to-business data sharing

Why?

The Data Act introduces rules for situations where a business ('data holder') has a legal obligation under EU or national law to make data available to another business ('data recipient'), including in the context of IoT data. Notably, the data-sharing terms and conditions must be fair, reasonable and non-discriminatory.

As an incentive to data sharing, data holders that are obliged to share data may request 'reasonable compensation' from the data recipient.

Types of data in scope

Chapter III of the Data Act applies to all data (both personal and non-personal) held by a business, including situations covered in Chapter II of the Data Act.

In practice

Data holders may request **reasonable compensation** for making the data available to a data recipient. This could include costs incurred for making the data available as well as technical costs related to dissemination and storage. However, micro companies, SMEs and non-profit research organisations cannot be charged more than the costs incurred for making the data available.

In order to protect data holders, the Data Act includes a non-exhaustive list of measures to remedy situations where a third party or user has unlawfully accessed or used data. For example, a data holder could require that an infringing party stops producing the product in question or destroys the data that it has unlawfully obtained, or it could seek compensation.

Any data-sharing obligations that precede the Data Act remain unaffected. Obligations in **future (sectoral) legislation should be aligned** with the provisions of Chapter III of the Data Act.

Chapter IV: Unfair contractual terms

Why?

Contractual freedom is central to business-to-business relationships. However, the Data Act aims to protect all European businesses seeking to acquire data, in particular SMEs, against unfair contractual terms through its measures to intervene in situations where, for example, one of the businesses is in a stronger bargaining position (e.g. due to its market size) and imposes a non-negotiable term ('take-it-or-leave-it') related to data access and use on the other.

Types of data in scope

These rules cover all data, both personal and non-personal, held by a private entity that is accessed and used based on a contract between businesses.

In practice

Unilaterally imposed take-it-or-leave-it terms may, where they relate to making data available, be subject to an unfairness test.

The Data Act establishes a non-exhaustive list of terms that are **always considered to be unfair** (e.g. that would exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence) and of terms that are **presumed to be unfair** (e.g. that would inappropriately limit remedies in the case of non-performance of contractual obligations or liability in the case of a breach of those obligations, or extend the liability of the enterprise upon whom the term has been unilaterally imposed). If a term is considered to be unfair, it is no longer valid – where possible, it is simply severed from the contact. If it is presumed to be unfair, the entity that imposed the term can try to demonstrate that the term is not unfair.

Chapter V: Business-to-government data sharing

Why?

Data held by private entities may be essential for a public sector body to undertake a **task of public interest**. Chapter V of the Data Act allows public sector bodies to access such data, under certain terms and conditions, where there is an **exceptional need**. The latter refers to a situation which is unforeseeable and limited in time, where the data held by a private entity are necessary for the performance of the public interest task, notably to improve evidence-based decision making. Situations of exceptional need include both **public emergencies** (such as major natural or human-induced disasters, pandemics and cybersecurity incidents) and **non-emergency situations** (for example, aggregated and anonymised data from drivers' GPS systems could be used to help optimise traffic flows).

The Data Act will ensure that public authorities have access to such data in a timely and reliable manner, without imposing an undue administrative burden on businesses.

Types of data within scope

Under Chapter V, all data are in scope, with a focus on non-personal data.

Chapter V of the Data Act on business-to-government data sharing differentiates between two scenarios:

- In order to respond to a public emergency, a public sector body should request non-personal data. However, if this is insufficient to respond to the situation, personal data may be requested. Where possible, this data should be anonymised by the data holder.
- In non-emergency situations, public sector bodies may only request non-personal data.

Key stakeholders

The entities entitled to request data include public sector bodies of the Member States as well as certain EU Institutions, bodies and agencies. These entities may also share the data with research-performing and -funding organisations under certain conditions.

In the context of business-to-government requests, data holders are typically private entities, but may also include public undertakings.

In practice

A public sector body may, under certain conditions, oblige a data holder to make available certain data without undue delay to

respond to a public emergency. The Data Act defines a public emergency; but its existence is determined according to national or EU procedures or laws.

For exceptional needs which are not related to a public emergency, a public sector body may request non-personal data to fulfil a specific task that is in the public interest and that has been provided by law, if the public sector body can prove that it has not been able to access the data via other means.

In both cases (emergency and non-emergency), requests must respect a number of **strict principles and conditions**. For example, requests must be specific, transparent and proportionate, trade secrets must be protected, and the data must be deleted once it is no longer needed.

The table below summaries what businesses may request for providing data to a public sector body in this context.

Compensation for making data available under Chapter V of the Data Act

	Businesses other than micro and small companies can ask for:	***Micro and small companies can ask for:***
Public emergency	Businesses may ask for their data contribution to be acknowledged and publicly recognised by the receiving public sector body	Reasonable remuneration not exceeding technical and organisational costs incurred + public acknowledgement, upon request
Non-emergency situation	Reasonable remuneration not exceeding technical and organisational costs incurred (except for the production of official statistics)	N/A (exempt from the obligation to provide data)

To minimise the burden on businesses, the same data cannot be requested more than once **('once-only principle')** by more than one public sector body. For this reason, all requests must be made publicly available by the data coordinator (unless there is a security concern).

Chapter VI: Switching between data processing services

Why?

In order to ensure a competitive market in the EU, customers of data processing services (including cloud and edge services) should be able to switch seamlessly from one provider to another. However, customers currently face a number of barriers to this, including high charges associated with, for example, data egress, lengthy procedures and a lack of interoperability between providers that can result in a loss of data and applications.

The Data Act will make switching free, fast and fluid. This will benefit customers, who can freely choose the services that best meet their needs, as well as providers, who will benefit from a larger pool of customers.

Scope

Chapter VI of the Data Act applies to providers of data processing services (i.e. digital services enabling ubiquitous and on-demand network access, such as networks, servers or other virtual or physical infrastructure and software). Data that is key for switching comprises input and output data, including metadata, generated by the customer's use of the service, excluding data protected by intellectual property rights or constituting a trade secret of the service provider.

In practice

To overcome the imbalance of power between providers and customers in the cloud market, the Data Act sets **minimum requirements for the content of cloud contracts**. In particular, customers from the private and public sector will benefit from much greater contractual transparency.

The Data Act includes measures to ensure that customers can switch from one provider of data processing services ('source provider') to another ('destination') provider quickly and smoothly, and without losing any data or the functionality of applications. For example, providers of Platform and Software as a Service must make open interfaces available and, at a minimum, export data in a commonly used and machine-readable format. Providers of Infrastructure as a Service must take measures to facilitate that, where a customer switches to a service of the same type, the customer gets materially comparable outcomes in response to the same input for features that both services share ('functional equivalence'). As an example of such a measure, the source provider may have to use tools for shifting computing workloads from one virtualization technology to another.

All providers are required to remove obstacles that their customers may face when they want to switch to another provider or use several services at the same time.

The Data Act will also **entirely remove switching charges**, including charges for data egress (i.e. charges for data transit), from 12 January 2027. This means that providers won't be able to charge their customers for the operations that are necessary to facilitate switching or for data egress. However, as a transitional measure during the first 3 years after the Data Act's entry into force (from 11 January 2024 to 12 January 2027), providers may still charge their customers for the costs incurred in relation to switching and data egress.

Chapter VII: Unlawful third country government access

Why?

Sometimes, a decision or judgment issued by a country outside the EU ('third country') seeks to allow government access to and transfer of non-personal data processed and stored within the EU. However, in certain instances, granting access to or transfer of such data may actually be unlawful, in particular where the request conflicts with EU laws and guarantees on the protection of the fundamental rights of individuals, national security interests or commercially sensitive data.

The Data Act follows the Data Governance Act with respect to the provisions aimed at preventing unlawful third-country governmental access and transfer of non-personal data held in the EU. Such provisions have no impact on regular business-to-business data sharing. They increase transparency and legal certainty regarding the process and conditions under which non-personal data can be accessed by or transferred to non-EU government bodies.

Types of data in scope

Any non-personal data held in the EU by a provider of a data processing service.

In practice

The Data Act does not prohibit cross-border data flows, but ensures that the **protection afforded to data in the EU travels with any data transferred outside the EU**.

In this context, the Data Act establishes rules and safeguards for access requests by a foreign public sector body to non-personal data held in the Union. Legitimate international cooperation in relation to law enforcement is not affected by these provisions.

If there is no international agreement regulating access by a third country government to non-personal data located within the EU, the data can only be transferred or accessed under specific conditions. These conditions refer to certain guarantees safeguarding European rights that need to be met by the third country's legal system, including a requirement to set out the reasons and to assess the proportionality in the decision. The provider of data processing services addressed by such a decision may contact the relevant national body to help assess whether the conditions set out in the Data Act are met. To help assess whether these conditions have been met, the European Commission will develop guidelines together with the European Data Innovation Board (an expert group established under the Data Governance Act (https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained) to facilitate the sharing of best practices and prioritise cross-sectoral interoperability standards).

Providers of data processing services should take all reasonable measures (e.g. encryption, audits, adherence to certification

schemes) to prevent access to the systems in which they store non-personal data. These measures should be published on their websites. In addition, wherever possible, they should inform their customers before giving access to their data.

Chapter VIII: Interoperability

Why?

Standards and interoperability are key to ensuring that data from different sources can be used within and between Common European Data Spaces (https://digital-strategy.ec.europa.eu/en/policies/data-spaces) to foster research and develop new products or services. To this end, the Data Act establishes some essential requirements with which participants in data spaces must comply and which can be further specified by the European Commission by way of delegated acts (https://commission.europa.eu/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts_en).

It also aims to ensure interoperability between data processing services; this is essential if customers are to benefit from easier switching.

Key stakeholders

This chapter targets participants of data spaces that offer data or data-based services to other participants and that facilitate or engage in data sharing within the data spaces.

It also addresses vendors of smart contracts as well as data processing services providers.

In practice

Data space participants should comply with several **essential requirements to allow data to flow within and between data spaces.** For example, a description of the data structures, data formats and vocabularies, where available, should be publicly accessible. In addition, means to ensure the interoperability of data-sharing agreements, such as smart contracts, should be ensured.

The Data Act also prepares the ground for increasing the interoperability of data processing services through **harmonised standards and open interoperability specifications**.

In addition, it lays out requirements for vendors of smart contracts for the automated execution of data-sharing agreements, for example to ensure that they correctly carry out the provisions of the data-sharing agreement and withstand manipulation by third parties.

The Commission will assess barriers to interoperability and prioritise standardisation needs, based on which it may ask European standardisation organisation(s) to draft harmonised standards that comply with the abovementioned requirements.

If the request does not lead to a harmonised standard or if the standard is insufficient to ensure conformity with the Data Act, the Commission can adopt common specifications as a fall-back solution. These should be developed in an open and inclusive way, considering feedback from the European Data Innovation Board.

Chapter IX: Enforcement and overarching provisions

Member States will designate one or more (new or existing) **competent authorities** to ensure the efficient implementation of the Data Act. Wherever there are multiple competent authorities, Member States must designate one of them as **'data coordinator'**. The data coordinator will act as a 'one-stop shop' for all issues related to the implementation of the Data Act at

the national level, facilitating is application both for businesses and public authorities. For example, if a business seeks redress for the infringement of their rights under the Data Act, the data coordinator should (upon request) provide all the necessary information to help them lodge their complaint to the appropriate competent authority. The data coordinator will also facilitate collaboration in cross-border situations, such as when a competent authority from a given Member State does not know which authority it should approach in the data coordinator's Member State.

The Commission will maintain a public register of competent authorities and data coordinators.

The European Data Innovation Board (https://europa.eu/!f8xmhh) will facilitate discussions between competent authorities, for example to coordinate and adopt recommendations on the setting of penalties for infringements of the Data Act. Penalties are set by competent authorities, and according to the Data Act there should be effective, proportionate and dissuasive penalties.

Member States may, if they wish, set up **certified dispute settlement bodies** to assist parties who cannot agree on fair, reasonable and non-discriminatory terms for making data available. Parties are free to address any dispute settlement body – either in the Member State in which they are established or in another.

Certified dispute settlement mechanisms and specialised competent authorities will make it easier for companies, particularly small businesses, to enforce their rights under the Data Act as they offer a simple, fast and low-cost solution to the parties involved.

What's next?

The European data strategy sets out the path for the EU to become a leader in the data economy. This will be achieved through the creation of a European single market for data in which data can flow between sectors and Member States in a safe and trusted manner for the benefit of the economy and society. By ensuring fairness in the allocation of the value of data amongst stakeholders, the Data Act is a key element to achieving this vision.

The Data Act will become applicable on 12 September 2025.

To help businesses navigate these new rules, the Commission will recommend a set of model contractual terms to help businesses conclude data-sharing contracts that are fair, reasonable and non-discriminatory (Chapters II and III of the Data Act). These terms will also provide guidance on reasonable compensation and the protection of trade secrets. The Commission will also recommend a set of non-binding standard contractual clauses for cloud computing contracts between cloud service users and providers. An expert group has been set up to help the Commission draft such terms and clauses and it plans to recommend them by autumn 2025.

Within 3 years of its entry into application, the Commission will carry out an evaluation of the impact of the Data Act. On this basis, if necessary, the Commission may propose an amendment to the Act.