Frequently Asked Questions

Data Act

6 September 2024

Version 1.0

The Data Act (Regulation (EU) 2023/2584) establishes harmonised, horizontal rules to ensure fairness in the allocation of value generated from data across market actors, while safeguarding the interests of those who invest in data-generation technologies.

For an introduction to the Data Act, we invite you to consult the "Data Act Explained" fact page.

This set of more technical Frequently Asked Questions (FAQs), published approximately a year before the entry into application of the Data Act, is designed to assist stakeholders in the implementation of the legal provisions. The FAQs are the product of extensive stakeholder interactions, and this is intended to be a 'living document' that will be updated as and when necessary.

This document should not be considered as representative of the European Commission's official position. The replies to the FAQs do not extend in any way the rights and obligations deriving from applicable legislation nor introduce any additional requirement. The expressed views are not authoritative and cannot prejudge any future actions the European Commission may take, including potential positions before the Court of Justice of the European Union.

Please contact us if you have a question that is not covered here and we will try to get back to you as quickly as possible. For any complaints related to the Data Act's implementation, please consider contacting the data coordinator in your Member State.

Contents

Interaction with other EU law

1. How does the Data Act interact with the General Data Protection Regulation?

The General Data Protection Regulation (GDPR) is fully applicable to all personal data processing activities under the Data Act. The Data Act does not regulate as such the protection of personal data. Instead, the Data Act enhances data sharing and enables a fair distribution of the value of data by establishing clear rules related to the access and use of data within the EU's data economy.

In some cases, the Data Act specifies and complements the GDPR (e.g. real-time portability of data from Internet-of-Things (IoT) objects). In other cases, the Data Act restricts the re-use of data by third parties (e.g. Article 6 of the Data Act). In the event of a conflict between the GDPR and the Data Act, the GDPR rules on the protection of personal data prevail (cf. Article 1(5) of the Data Act).

2. How does the relationship between the Data Act and the GDPR affect the enforcement and protection of personal data?

The Data Act respects the competence of the data protection authorities (DPAs) to enforce rules on personal data protection. The Data Act provides a coherent enforcement and cooperation mechanism between DPAs and other competent authorities.

Article 1(5) of the Data Act establishes that the GDPR applies to the processing of personal data in the framework of the Data Act. In this context, it recalls that the DPAs are competent to enforce the obligations stemming directly from the GDPR.

Article 37(3) provides that, insofar as the protection of personal data is concerned, the DPAs are responsible for monitoring the application of the Data Act and can rely on the tasks and powers laid down in the GDPR. This is also stated in recital 107. The protection of personal data captures, for example, the power to assess: (i) whether a user who is a data subject has received or has been allowed to port all personal data it requests; (ii) whether the data holder correctly qualifies which data should be considered personal data; and (iii) whether a valid legal basis under the GDPR exists for a user who is not a data subject to request and port personal data. Article 37(3) also ensures that data subjects are not required to go to two different authorities in cases where the rights of access and porting would apply under both the Data Act and the GDPR or where there could be any other grievance relating to the protection of their personal data in the application of the Data Act.

More generally, the Commission strives to promote a strong working relationship between the authorities that enforce data legislation in the EU, including through the membership of the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) in the European Data Innovation Board.

3. How does the Data Act interact with existing data-sharing obligations under other EU legislation?

The Data Act is a horizontal piece of legislation that aims to significantly enhance fair access to and use of data across all sectors of the economy. Chapter III, in particular, establishes a framework regarding the conditions, compensation, and technical protection measures for whenever a data holder is obliged under EU or national law to share data with a data recipient.

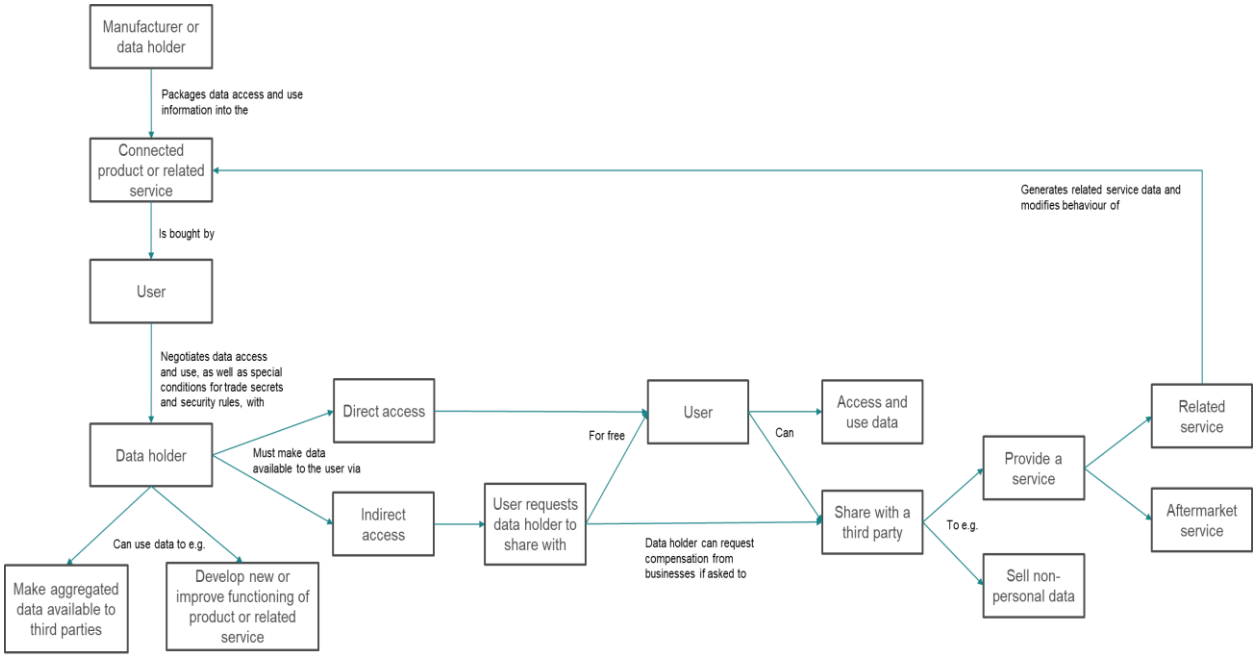
More concretely, Article 44 addresses two key dimensions that structure the interaction between the Data Act and other EU legislation that include rules on data access and use: time of entry into force (Article 44(1)) and sectoral specificities (Article 44(2)).

According to Article 44(1), data-sharing obligations that entered into force on or before 11 January 2024 (the Data Act's entry into force) remain unaffected. If EU legal acts introduce rules on data between 11 January 2024 and 12 September 2025 (the Data Act's entry into application), best efforts should be made to ensure alignment, but there is no legal obligation to do so.

The Data Act sets horizontal rules for data access, sharing and use. However, Article 44(2) allows the Data Act to be complemented by sector-specific legislation, where necessary, with practical and technical modalities (e.g. safety, standardisation, or technical matters) and with specific limits on data holders' access rights or actions. However, the development of such sectoral rules should be approached cautiously and consistent with the principles laid down in the Data Act to the greatest extent possible, thus avoiding unnecessary complexity. The principles of the Data Act apply for all matters related to 'access to data' that are not specifically regulated in such sectoral rules.

Access to and use of data in the Internet-of-Things context

An example of Chapter II in practice



4. Which data are in scope?

Several factors determine which data are covered by the data access rights provided for in Articles 3, 4 and 5 of the Data Act. Generally speaking, raw and pre-processed data (simply put, 'raw but usable' data) that are readily available to a data holder as a result of the manufacturer's technical design are subject to mandatory data-sharing obligations that are regulated by Chapter II.

Access and use of IoT data – Chapter II of the Data Act		
Factor	**Explanation**	**Reference in the legal text**
Product data	Data obtained, generated, or collected by a connected product and which relates to its performance, use or environment. Purely descriptive data that accompanies the connected product (e.g. in user manuals or on the packaging) is not product data. The only situation in which information 'about' the connected product is relevant is the pre-contractual transparency obligation under Article 3.	Recital 15, Article 2(15)
Related service data	Data representing user action, inaction and events related to the connected product during the provision of a related service.	Recital 15 and 17, Article 2(16)

Readily available data	Product data and related service data that a data holder can obtain without disproportionate effort going beyond a simple operation. The definition of 'readily available data' does not include a reference to the time of their generation or collection. Only data generated/collected after the entry into application of the Data Act should be considered as falling within the scope of Chapter II.	Recitals 20 and 21, Article 2(17)
Level of enrichment of the data	In scope: raw data and pre-processed data, accompanied by the necessary metadata to make it understandable and usable. For example, data collected from a single sensor or a connected group of sensors for the purpose of making the collected data comprehensible for wider use-cases by determining a physical quantity or quality or a change in a physical quantity (e.g. temperature, pressure, flow rate, audio, pH value, liquid level, position, acceleration, or speed). Out of scope: highly enriched data, meaning inferred or derived data or data that result from additional investments (including by way of proprietary, complex algorithms). In addition, content that is often covered by intellectual property rights (e.g. textual, audio, or audiovisual content).	Recital 15
Personal vs non-personal data	Users are entitled to access all data generated by the connected product or related service, whether personal or non-personal. However, personal data processing is governed by GDPR rules, so the user's rights provided by the Data Act have to be exercised in compliance with the GDPR. Users that are not data subjects or data holders must have a valid legal basis under Article 6 of the GDPR for processing personal data. Question 26 examines in further detail non-personal data access, use and sharing.	Recitals 25 and 35
Trade secrets	The Data Act does not modify the relevant legal protections for protection of trade secrets. The 2016 Trade Secrets Directive, for example, continues to apply. The Data Act establishes a new mechanism to protect trade secrets. This mechanism is known as the 'trade secrets handbrake' and is explored further in Question 20.	Recital 31, Articles 4(6), 5(9)

5. What is a 'connected product'?

Connected products are items that can generate, obtain, or collect data about their use, performance, or environment and that can communicate this data via a cable-based or wireless connection. This includes communication of data outside the product on an *ad hoc* basis (e.g. during maintenance operations). Connected products can be found in all areas of the economy and society. They include smart home appliances, consumer electronics, industrial machinery, medical devices, smartphones, and TVs (cf. recital 14).

Products which primarily fulfil the function of storing, processing, or transmitting data (e.g. servers and routers) are outside the scope of the mandatory data-sharing obligations under Chapter II, unless they are owned, rented, or leased by the user.

Similarly, the fact that a connected product (e.g. a wagon, airplane, or vehicle) must use certain infrastructure (e.g. railways, airports, or highways) to function does not entitle the user of that connected product to access data generated by, for instance, sensors that are part of that infrastructure. Access would only be granted if the user has received ownership or contractual rights over the sensors embedded in the infrastructure. Finally, the Data Act specifies that prototypes are out of scope, as their manufacturing stage has not been completed.

6. What determines whether a connected product falls in scope of the Data Act?

A connected product falls within the scope of the Data Act if it has been 'placed on the Union market' (Article 2(22)). 'Placing on the market' concerns the transfer of ownership, possession, or any other property right between two economic actors that occurs after the manufacturing stage. A connected product is 'placed on the market' only once. All subsequent operations are considered as 'making available on the market' (Article 2(21)). The concept of placing on the market refers to each individual product, not to a type of product. The requirements laid out in the Data Act are therefore applicable only to individual products that have been placed on the EU market, and not to all products of that type.

The Commission notice 'The "Blue Guide" on the implementation of EU product rules' (2022) served as inspiration for the Data Act's rules on products and provides comprehensive guidance on this topic. For instance, the Blue Guide identifies situations where a product is not considered to be 'placed on the market'. These include situations where (i) the product is purchased by a consumer in a third country while they are physically present in that third country and brought by that consumer into the EU for their personal use, and (ii) when the product is manufactured in a Member State with a view to exporting it to a third country.

7. What happens if a connected product that is placed on the EU market generates data when it is used abroad?

If a connected product is placed on the market in the EU and then used outside the EU, the data generated by that connected product both inside and outside the EU should be made available to the user in accordance with the Data Act.

As explained in the answer to Question 6, a connected product falls within the scope of the Data Act if it has been placed on the market in the EU. This means that 'mobile' connected products (e.g. ships, airplanes, trains, and cars) should be treated in the same manner as other connected products. The mere circulation of a ship, airplane, train, or car on EU territory or in EU waters is not sufficient for a connected product to be considered as having been 'placed on the EU market' because there has been no transfer of ownership.

The rules of the Data Act build on civil law relations of ownership and lease between a person or entity and an object. The fact that connected products such as cars, rail vehicles or planes are registered in a Member State is an indicator that the connected product in question was placed on the EU market.

8. What is a 'related service'?

A related service is a digital service that can be linked to the operation of a connected product and that affects the functionality of this connected product, for instance by transmitting data or commands to it (e.g. an app to adjust the brightness of lights, or to regulate the temperature of a fridge).

Two basic conditions must be satisfied for a digital service to be considered as a related service:

- there must be a two-way/bidirectional exchange of data between the connected product and the service provider; and
- the service must affect the connected product's functions, behaviour, or operation.

Determining the 'functions' of a connected product is an ongoing and evolving task. Practice and courts' interpretation will play an essential role in further delineating whether a digital service is a related service. The following elements could be useful in further narrowing down whether a digital service is a related service:

- user expectations for that product category;
- marketing accompanying the connected product and/or the digital service;
- contractual negotiations;
- the replaceability of the digital service;
- pre-installation of the digital service on the connected product.

Most but not all digital services will fall under the category of related services. The following digital services cannot be considered as related services: connectivity, power supply and aftermarket services (e.g. auxiliary consulting, analytics and financial services, and regular repair and maintenance) (cf. recital 17).

To offer a related service, a provider must first receive product data. Once a contractual relationship is established between the user and the provider and a related service is rendered that leads to the creation of data, the provider becomes a data holder.

9. What happens if a connected product is resold ('second-hand connected products')?

When it comes to the user's right to access data generated by the use of a connected product, the Data Act does not distinguish between 'first-hand' and 'second-hand' connected products.

If a connected product is being (re)sold, the seller must comply with the 'transparency obligation' outlined in Article 3. This requires the seller to provide the necessary information for the future owner to exercise their new data access rights under the Data Act. As a result, the future owner will be informed as to who the data holders are as well as the modalities to accessing and using the generated data. Other sections of this FAQ address related issues, such as how data holders can identify legitimate users.

10. How do the obligations under Chapter II of the Data Act relate to mechanisms of conformity assessment or type approval?

The Data Act applies to all connected products, including those that are subject to specific type approval or conformity assessment regimes (e.g. motor vehicles, aircraft, and medical devices).

The Data Act does not have specific provisions with respect to mechanisms of conformity assessment, but Data Act obligations apply. As a general rule, therefore, a connected product can only be placed on the market if it complies with all applicable Data Act provisions and if a conformity assessment has been carried out in accordance with applicable legislation. In other words, the specific need for a connected product to undergo a conformity assessment procedure is determined by requirements set in legislation other than the Data Act.

Section on users

11. What are 'users'?

The general principle in Article 2(12) is that a 'user' is a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives a related service.

This implies the user has a stable right on the connected product (e.g. ownership, or a right from a rent or lease contract). Such a user has a legal right under the Data Act over the data being generated by the connected product.

12. Does the Data Act apply to users established outside the EU?

According to Article 1(3)(b), a user must be established in the EU. A user may request access to data on the basis of the Data Act, irrespective of whether the data are stored inside or outside the EU.

13. Can there be multiple users for a single connected product, and how should their access be governed?

Various actors may have a legal right based on the contractual arrangements related to the use of a connected product. It is therefore entirely possible for multiple persons to be users of the same connected product. In such a situation, data holders should have mechanisms in place to ensure that each user can access the data to which they are entitled. Users might also conclude separate agreements (e.g. a user-to-user sub-lease of a connected product).

The following example illustrates, in a non-exhaustive manner, how access to data in a multiple-user scenario could be organised. Other data-sharing arrangements and mechanisms are possible. The Commission's upcoming model contractual clauses will provide further guidance (cf. Question 71).

Example:

Sara goes on holiday to Portugal for 2 weeks and needs to rent a car. The rental agency, Sunny Wheels, owns a fleet of cars bought from Omni Motors, a large car manufacturer. Keen to exercise her rights under the Data Act, Sara asks Sunny Wheels to provide her with a 'connected car'.

Sunny Wheels has a contract with Omni Motors that ensures that Sunny Wheels and its clients can access the data generated by the car. Omni Motors has put in place a data management system that can simultaneously handle data access requests from the thousands of users of their cars.

Sara's rental agreement contains detailed information on the data generated by the car, including how to access it. The following are two possible ways of organising access to data generated by Sara's rented car.

- ➔ **'Corporate accounts':** Sunny Wheels has a corporate account with Omni Motors. Sunny Wheels provides Sara with the details needed to log in to Omni Motors' website and access the rented car's data.
- ➔ **'Individual accounts':** Sunny Wheels informs Sara that she has to set up her own account and enter into a separate data-sharing contract with Omni Motors. Sunny Wheels notifies Omni Motors that Sara will be using the car for 2 weeks.

In both cases, Omni Motors is the **data holder;** Sunny Wheels is a **user** because it owns the rented car and can access the data; and Sara is also a **user** because she has, by virtue of the rental agreement with Sunny Wheels, received temporary rights over the rented car.

14. How can I, as a user, access my data?

Article 3(2) obliges data holders to provide users with information on the data that their connected product or related service generates. This is known as the 'transparency obligation'.

As part of the transparency obligation, data holders must inform users how to access the generated data. Data can be made available 'directly' (Article 3(1)) or 'indirectly' (Article 4(1)). Different configurations are possible (for instance, part of the data could be made available directly, and the rest could be made available indirectly).

Direct access means that the user has the technical means to access, stream or download the data in question without having to request the data holder to do so. For instance, a connected product has a digital interface where the user has control over the access mechanism, controlling the interface and workflows, and where the user can directly extract data from the connected product.

Indirect access means that the connected product or related service is designed in such a way that the user is required to ask the data holder for access (i.e. an approval process). An example would be a web portal where the user can submit a request to access data.

Article 3 leaves some flexibility ('where relevant and technically feasible') to a manufacturer to decide whether or not to design for direct access. This is because not all products (and not all data) are designed in such a way as to make data directly accessible to users. There may be situations where data holders prefer to offer indirect access to the data. The Data Act incentivises data holders to put in place solutions that work best for them when they have to comply with the obligation of making data available to the user.

15. How does the Data Act complement the GDPR's data portability rights?

Article 1(5) clarifies the relationship between the Data Act and the GDPR, namely that Articles 4 and 5 (right to access and share data from IoT devices) complements Articles 15 and 20 of the GDPR (right to access and port personal data). Recital 35 further clarifies this interaction.

The Data Act complements the data portability right established under Article 20 of the GDPR. Under the GDPR, only data subjects can exercise such a right and only when the personal data are processed under certain legal bases (consent or contract) and where technically feasible. The Data Act creates an enhanced portability right specifically for the IoT context. Thanks to the Data Act, users (e.g. data subjects and businesses) can access and port any data (both personal and non-personal) generated by the use of a connected product or related service. They can do so independently of the legal basis and, where applicable, in real time. Data subjects are therefore able to move their personal data between controllers (e.g. entities offering repair and maintenance services) more easily.

16. In which situations can users monetise their non-personal data?

Users are free to conclude agreements both with data holders and with third parties. They may compensate the user for gaining access to and using their non-personal data, including for commercial purposes. Recital 25 explains that, in business-to-business relations, an arrangement between the data holder and the user may even include a waiver of the user's right to use or share data further, provided that such a limitation of the user's rights is properly compensated.

17. What are the options for users, especially consumers, if the right to access and use data is not properly exercised?

The Data Act ensures a high level of consumer protection. Article 1(9) stipulates that the Data Act complements and is without prejudice to EU consumer legislation, particularly to the Unfair Contract Terms Directive (Directive 93/13/EEC), the Unfair Commercial Practices Directive (2005/29/EC) and the Consumer Rights Directive (2011/83/EU).

Several options are therefore available for those who seek to enforce their rights under the Data Act.

- Users (including consumers) can lodge a complaint with the relevant competent authority. If they are unsure about which competent authority to address in their specific case, they should first contact the data coordinator in their Member State (the Commission will make their names and contact details publicly available online.) See Question 64 for more details.
- Users (including consumers) can initiate legal proceedings.
- Users who are consumers can use the instruments available to them under EU consumer protection legislation. They can in particular lodge a complaint with the European Consumer Centres Network in the event that the data holder is established in another Member State from the Member State in which the consumer resides.

- Users who are data subjects can contact the relevant DPA regarding all issues concerning the processing of personal data.

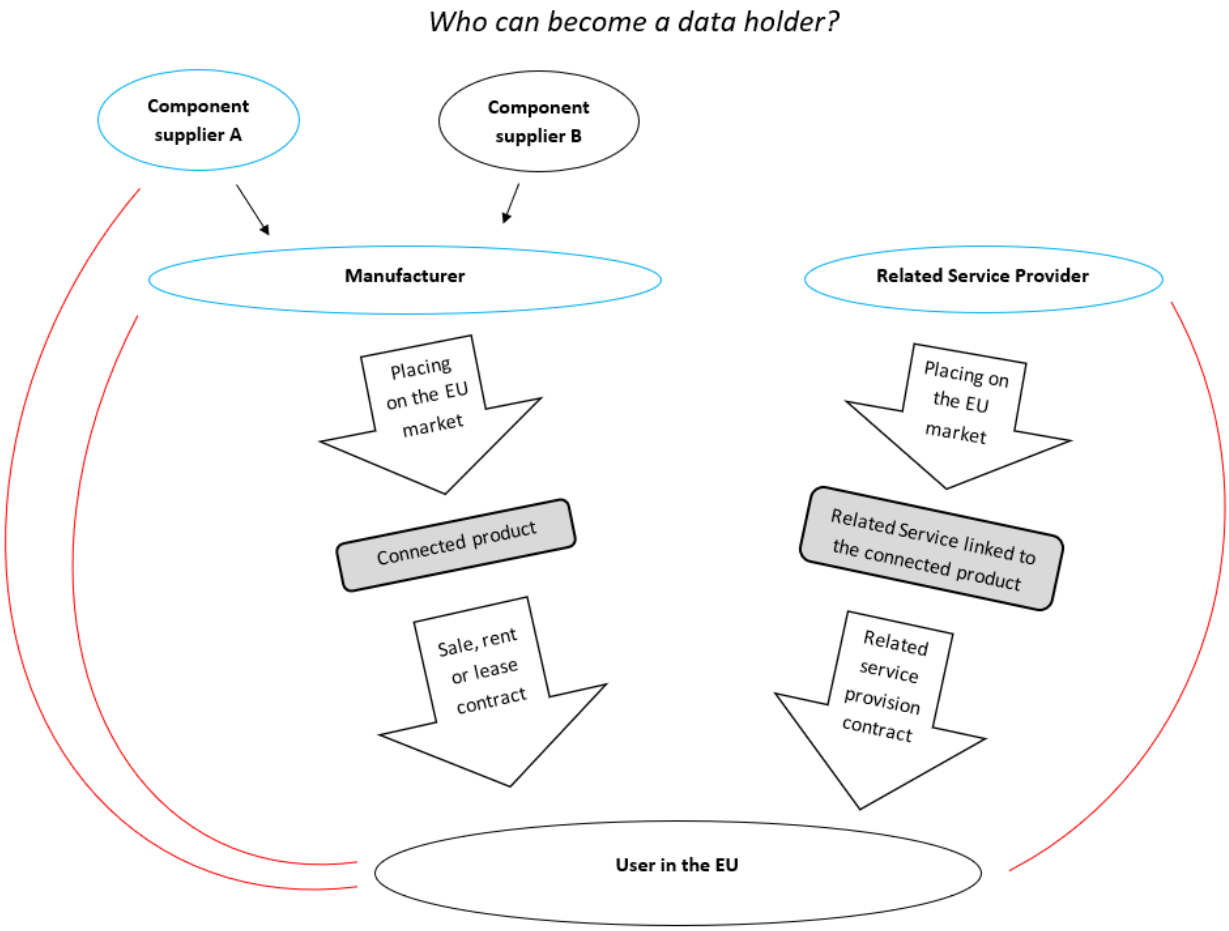
Section on data holders

18. Is a manufacturer always a data holder?

Even though manufacturers will typically be a data holder, this is not always the case. The Data Act allows an entity to 'outsource' the role of 'data holder'. For example, a manufacturer may contract out to another entity the role of 'data holder' for all or part of the manufacturer's connected products.

In addition, a data holder who is not a manufacturer might be a company that provides a related service linked to a connected product. This means that the business offering the related service might be a data holder and be different from the company that actually made the connected product.

Determining who the data holder is does not depend on who produced the hardware or software, but on who controls access to the readily available data. See the flowchart below for an example of role distribution.



The flowchart illustrates a situation where a user enters into two contracts (e.g. for the sale of the connected product and for the provision of the related service) that establish a legal relationship (in red)

between the user and three separate data holders (circled in blue). The user must always be informed of the identity of the data holder(s) before signing such contracts.

1. The manufacturer is interested in receiving and using the data, and therefore establishes itself as a data holder in the sales contract, in line with Articles 3(2) and 4(13).
2. Both component suppliers A and component supplier B deliver data-generating components. However, only A (unlike B) wishes to receive and use the data generated by its component. Unless supplier A can use the data received from the manufacturer, in accordance with the contract concluded between the user and the manufacturer, supplier A needs to become a data holder and agree with the user on the use of the data in accordance with Article 4(13).
3. Whenever a user also acquires a related service linked to the connected product, the related service provider must necessarily enter into a contract with the user, in line with Articles 3(3) and 4(13). The related service provider therefore becomes a data holder.

19. Does Article 3(1) oblige manufacturers of connected products to design or redesign their connected products so that users can access the data directly?

No. Article 3(1) does not oblige manufacturers to grant **direct access** to data in all situations and for all connected products. Data should be '**directly accessible**' to the user '**where relevant and technically feasible**'.

The formulation '**where relevant and technically feasible**' is meant to reinforce the manufacturers' discretion to decide whether to design a connected product in a way that provides users with 'uncontrolled' access (i.e. without any intervention by any other party) or in a way that provides access with additional controls (typically via a remote server). For this purpose, a manufacturer may assess, for example, whether direct access is technically possible; the costs of potential technical modifications; and the difficulty of protecting trade secrets or IP, or of ensuring the connected product's security. One could also consider whether direct access is relevant in a specific scenario from the perspective of the connected product, user, or data holder. Based on this assessment, manufacturers may choose to design the connected product in such a way that all or part of the product data is directly accessible or may enable only indirect access. If agreed upon, data holders can also access product data made directly accessible to a user.

Data are '**directly accessible'** when:

- The user is able to access the data without the intervention of any other party, notably the data holder (this is an alternative to making requests under Articles 4 and 5, which do require data holder intervention).
- The user has the technical means to stream or download the data as a result of the design of the connected product. Recital 22 explains that the location where the data are stored is irrelevant: data can be 'directly accessible' from a storage point on the device itself or from a remote server under the control of the manufacturer or a data holder.

Put simply, for data to be '**directly accessible'**, the user must therefore be able to access it without the involvement of the data holder, regardless of where the data are stored. Even if there is direct access and a remote server, the data holder is obliged to provide the means (i.e. appropriate interfaces, such as an API) to allow the user to easily access the relevant data (cf. recital 35, which compares Article 3(1) of the Data Act with Article 20 of the GDPR).

By the date of entry into application of the Data Act (12 September 2025), products already on the market and new products (when placed on the market) must allow for data to be accessed by the user. By this date, manufacturers have to decide whether such access will be made **directly** or **indirectly** (cf. Article 4(1))**.** Companies will find practical ways to incentivise the use of the solution that works best for them. Sectoral legislation can be more specific.

20. Does the new data access right affect the protection of trade secrets?

The Data Act provides a framework that balances data sharing with the need to preserve the protected nature of the data (including with respect to the protection of trade secrets, whose confidentiality continues to be ensured). The Data Act does not modify the applicable legal protections (including the 2016 Trade Secrets Directive, which already provides a legal framework for the protection of trade secrets).

However, a data holder can unilaterally determine which data are trade secrets, so the claim that certain data are trade secrets is not enough to prevent the exercise of the data access rights provided by the Data Act. This does not mean that the Data Act leads to the forfeiture of trade secret protection. Rather, it carefully balances the need to prevent illegitimate restrictions on the user's new data access rights against the need to uphold the legal protection provided to trade secrets.

The data holder therefore has the right, prior to disclosure, to require users and third parties to preserve the confidentiality and secrecy of the trade secret encumbered data by agreeing to and implementing safeguards necessary to that end. As an additional layer of protection, the Data Act introduces a new mechanism (commonly known as the 'trade secrets handbrake') that frames the conditions under which a data holder can withhold, suspend or, exceptionally, refuse to share data.

How can data holders handle trade secrets and activate the 'trade secrets handbrake'?

When a data holder receives a request to access data, it must **identify** the trade secrets that need to be shared and **agree** with the user/third party on the necessary measures to preserve their confidentiality (Articles 4(6) and 5(7)). These safeguards need to be in place prior to the sharing of data. Possible measures could include model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.

The data holder may **withhold** or **suspend** the sharing of trade secrets if there is no agreement, if the user or third party does not implement the agreed measures, or if the confidentiality of the trade secrets is undermined (Articles 4(7) and 5(10)).

In exceptional circumstances, the data holder may **refuse** to share trade secrets if it can demonstrate, on the basis of objective evidence, that it is highly likely that serious economic damage would result from the disclosure of trade secrets (Articles 4(8) and 5(11)). 'Serious economic damage' means serious and irreparable economic loss. Such decisions need to be made on a case-by-case basis.

If the data holder considers that it must withhold, suspend, or refuse to share data, it must **notify** the competent authority of the respective Member State, and communicate the reasoning behind the decision to the user or third party without undue delay.

The user or third party can seek redress and challenge the data holder's decision before a court or tribunal of a Member State or agree with the data holder to refer the matter to a dispute settlement body. The user or third party can also lodge a complaint with the competent authority. The competent authority should, without undue delay, decide whether and under which conditions data sharing should start or resume (Articles 4(9) and 5(12)).

21. Can trade secret protection also apply in relation to data made directly available in the sense of Article 3(1)?

It is important to first underline that the Data Act allows manufacturers to choose, when designing a connected product (or a related service), whether readily available data can be made accessible by the user directly, indirectly or a combination of both (see Question 14). When making this choice, the protection of trade secrets can be a consideration, especially since, in a direct access situation, the manufacturer will be less involved (or not at all) than in an indirect access situation in how a user will exercise their access rights.

However, direct access does not mean that it has to be unconditional. The manufacturer could contractually oblige the user to protect certain data that are made directly accessible, in order to ensure the protection of trade secrets. Disabling direct access based on the considerations in Articles 4(7), 4(8), 5(10) and 5(11) (referred to as the 'trade secrets handbrake') is not prohibited by the Data Act but is a matter to be negotiated on a contractual basis. Any such contractual conditions cannot undermine the user's rights, as per Article 7(2).

It would nevertheless seem inappropriate to invoke the Data Act as an argument to renegotiate contractual obligations around direct access that were agreed in contracts concluded before the Data Act entered into force. The Data Act does not change the situation as regards the protection of trade secrets for legacy products and respective contractual agreements.

22. Does a data holder have to share data if there are safety/security concerns?

Pursuant to Article 4(2) of the Data Act, users and data holders can agree to restrict or refuse to share data 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. Sectoral authorities may provide users and data holders with technical expertise in order to determine whether restrictions are necessary or warranted.

This mechanism (i.e. the possibility of restricting or prohibiting data access on the basis of safety or security considerations), is referred to as the 'safety and security handbrake'.

If, under the conditions explained above, the data holder intends to activate this handbrake, it must notify the competent authority of the respective Member State. Moreover, users may challenge the data holder's refusal to share data before the competent authorities, courts, or a dispute settlement body.

23. A non-compete clause for connected products has been introduced. Does this also apply to related services?

No. According to recital 32, a key objective of the Data Act is to allow service providers to have access to new data and compete on an equal footing with comparable services offered by manufacturers. The prohibition on developing competing related services could have a discouraging effect on innovation and the provision of other services (not necessarily 'related services').

As a result of the limitation of the non-compete clause to connected products only, businesses and consumers will see a reduction in the cost of switching to alternative services. They will also benefit from more competition for value-added services (e.g. predictive maintenance), which depend on access to such data; and be able to make more informed consumer decisions (e.g. buying more sustainable products and services).

24. How are the interests of data holders protected?

The interests of data holders are protected in various ways. The following are four examples.

i. The Data Act limits the scope of data which is subject to mandatory sharing obligations under Chapter II to raw and pre-processed data. This minimises adverse effects on data-related investments and on the protection of trade secrets or IPR.

ii. Specific provisions address the situation where data requested by the user are considered trade secrets by the data holder/trade secrets holder or where the use of data is linked to considerable safety risks.

iii. Data access from connected products under the Data Act cannot be used to develop a competing product.

iv. The data holder is able to request compensation from third parties (when prompted by the user to share data), or from data recipients (when there is a legal data-sharing obligation).

25. Does the Data Act apply to manufacturers of connected products and providers of related services that are established outside the EU?

Yes. The Data Act does not require the manufacturer or related service provider to be established in the EU. The Data Act establishes a right for users in the EU to access, use and share the readily available data they are entitled to. All connected products and related services placed in the EU must therefore be designed in such a way that this right can be exercised.

All legal requirements must be met when the connected product is placed on the EU market or when the related service is offered. The related service is linked to the connected product's functioning, so the place of establishment of the provider of the related service is not a factor in determining whether they fall within the scope of the Data Act.

26. Are there any limitations on the data holder's use of the data generated by the user?

While the GDPR governs processing of *personal* data, Articles 4(13) and (14) of the Data Act cover the use of *non-personal* data by the data holder.

Articles 4(13) stipulates that the data holder can use the non-personal data for any purpose, provided that (i) this is agreed with the user; and (ii) the data holder does not derive insights about the economic situation, assets and production methods of the user in any other manner that could undermine the commercial position of that user on the markets in which the user is active.

Recital 25 further specifies that any contractual term regarding the data holder's intended use of data should be transparent to the user. Possible purposes of data usage by the data holder include the improving of the functioning of the connected product or related service or making aggregated data available to a third party, provided that these data do not allow identification of granular data. The user is the sole source of access to granular non-personal data from the connected product or related service.

Article 4(14) addresses the specific aspect of data usage by the data holder that involves the sharing of non-personal data with third parties, which should only take place if contractually agreed with the user (in line with the Article 4(13)).

27. How would a data holder be able to verify a legitimate user?

Article 4(5) stipulates that, for the purpose of verifying a person as a possible user, 'a data holder shall not require that person to provide any information beyond what is necessary'. Recital 29 explains that 'Data holders may require appropriate user identification to verify a user's entitlement to access the data.'

The 'information' that a user may be requested to provide must therefore conclusively demonstrate that a person is a user (i.e. someone who 'owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services' (Article 2(12)).

Given users' vested interest in accessing the data, it is reasonable to expect that they will try to properly identify themselves.

Recital 21 provides guidance on how a data holder can verify users. According to this recital, access should be granted to the user:

> *on the basis of simple request mechanism granting automatic execution and not requiring examination or clearance by the manufacturer or data holder. (…) Where automated execution of the data access request is not possible, for example via a user account or accompanying mobile application provided with the connected product or related service, the manufacturer should inform the user as to how the data may be accessed.*

Data holders are therefore free to set up the specific process to identify users but must still comply with Articles 4(4) and (5). Data holders can assess, for instance, (i) what best fits the type of product; (ii) the type of user (consumer vs industrial); (iii) the number of likely users (owner of an elevator vs multiple users in car rental); (iv) the expected frequency of data access requests; (v) presence of specific mechanisms of demonstrating ownership (e.g. car holder registration); (vi) the cost of setting up differentiated user accounts; and (vii) the ease of use of such accounts for the actual consumers. Where applicable, solutions such as the EU Digital Identity Wallet could be envisaged.

With respect to personal data, recital 34 explains that 'Personal data may only be requested by a controller or a data subject (…) Where the user is not the data subject but an enterprise, including a sole trader, and not in cases of shared household use of the connected product, the user is considered to be a controller.'

Recital 34 recalls that users that are data subjects can always access personal data concerning themselves. It also clarifies that users who are not data subjects are controllers under the GDPR and must comply with their obligations under the GDPR when requesting personal data from IoT devices.

28. Does a data holder still need to share data with a third party upon request of the user where it has granted direct access to the user?

Yes. Users also have a right under Article 5 to request the data holder to transfer data to a third party when the user has direct access to the data in the sense of Article 3(1). This pre-supposes that there is a data holder with data readily available to them. Article 5 is not conditional upon the type of access that the user has.

29. Can users request access to historical data that a data holder might be storing (e.g. when buying a second-hand sensor/machine)?

The Data Act can be read as giving users the right to access and port readily available data generated by the use of a connected object, including data generated by other users before them. Such subsequent users might have a legitimate interest in such data (e.g. in respect of updates or incidents), while keeping in mind the 'reasonable retention policy' referred to in recital 24.

However, the rights of previous users and other applicable law (e.g. with respect to their personal data or commercially confidential information, including their request for data to be deleted) would have to be respected. In that sense, the granularity or scope of 'historical data' would be limited in order to preserve the rights and interests of others.

30. Can users request that data holders delete their non-personal data before selling a product to another user?

The Data Act does not establish a specific 'right to be forgotten' for non-personal data similar to the GDPR. However, nothing prevents parties from contractually agreeing on the possibility of deleting data before the sale of a connected product. If this has been agreed, then information on how data can be erased is one of the requirements pursuant to Article 3(2)(d), and Recital 21 gives guidance on account solutions in the case of multiple usership, where users should be allowed to delete the non-personal data related to their account. At the same time, depending on the product, sectoral legislation might provide differently (for example, when a certain type of data is meant to 'follow' the product for safety reasons).

31. Can a company be both a user and a data holder at the same time?

Under Chapter II, a company cannot be a user and a data holder for the same data. It can, however, be a user and a data holder with respect to different connected products or related services. For example, a manufacturing company can be both a 'user' of the robots used in its factory, and a 'data holder' for the connected products it manufactures).

In addition, the Data Act allows a person to be a user of a connected product without there being a data holder. If a user acquires a connected product where the data are, for example, stored directly on the device or transferred from the device to the user's computer, and the manufacturer does not have access to any of the data, then there is no data holder since only the user has access to the data.

Section on third parties

32. What can a third party do with the data they receive from a user/data holder in the context of Chapter II?

The general principle, according to Article 6(1), is that a third party can use the data for purposes that were agreed with the user (usually in the context of providing a service to the user). Article 6(2) includes a closed list of actions which are prohibited for the third party. This list includes using data to develop a competing product and sharing the data with a gatekeeper (as defined under the Digital Markets Act).

33. Can users oblige data holders to share data with Digital Markets Act gatekeepers?

No. DMA gatekeepers, which are defined as undertakings that provide core platform services under the Digital Markets Act (DMA), typically have no difficulties in gaining access to large amounts of data. Data already tend to gravitate towards these large undertakings due to their gateway position, control over platform ecosystems and superior bargaining power. Requiring mandatory data sharing for IoT data with DMA gatekeepers would therefore be unfair to those who must comply and unnecessary given the goals of the Data Act. DMA gatekeepers cannot therefore be third parties in the sense of the new IoT data access right established under the Data Act.

This does not mean DMA gatekeepers are entirely excluded from the IoT (data) market. DMA gatekeepers are prohibited from relying on the specific mandatory data sharing mechanisms created by Articles 4 and 5. All other mechanisms (including regarding voluntary data sharing arrangements) remain unaffected.

34. Can someone established in a third country receive data on the basis of the data-sharing obligations under Chapter II?

No. The scope of the Chapter II data-sharing obligation on data holders is limited to entities and persons, including consumers, in the Union (cf. Articles 1(3)(b), 1(3)(d) and 2(14)). Giving data access to operators that do not have a presence in the EU cannot be justified based on the Data Act.

Irrespective of its place of establishment, a data holder has a legal obligation to share data with an EU-based entity or person at the request of an EU user. A user may ask a data holder to share data with an entity or person that is not established in the EU, but the data holder is not obliged to grant that request.

Fair, reasonable, and non-discriminatory (FRAND) conditions, compensation and dispute resolution

35. Is it possible to differentiate between the data recipients and apply different licensing conditions?

Article 8(3) implements a general principle that it is not admissible to differentiate between entities that are in the same situation (non-discrimination). Analysing whether two recipients are in a comparable category must be done on a case-by-case basis.

36. Is there an upper limit to reasonable compensation?

No. There is no upper (nor lower) limit to compensation as such. Rather, the Data Act imposes certain transparency requirements in order to ensure that calculation of compensation is based on certain objective criteria (e.g. costs incurred, or the volume of data being made available). Reasonable compensation cannot include a profit margin if the recipient is an SME or a non-profit research organisation.

37. Who can rely on the dispute settlement mechanism established by the Data Act and under which conditions?

Users, data holders and data recipients can refer their disputes to the dispute settlement bodies designated by Member States in accordance with the Data Act, which can help them to conclude a contract on data sharing or settle disputes arising after the conclusion of the contract. These dispute settlement bodies will be competent (i) for disputes relating to the 'safety and security handbrake' and to the 'trade secrets handbrake' (see Questions 20, 21 and 22) in business-to-consumers and in business-to-business relations, (ii) for disputes relating to the fair, reasonable and non-discriminatory terms and conditions for, and transparent manner of, making data available in business-to-business relations, where the data holder is legally obliged to make data available (including in accordance with the Data Act) and (iii) for dispute relating to the fairness of contractual terms related to data access and use in business-to-business relations.

The rules on dispute settlement are applicable to disputes relating to the fair, reasonable and non-discriminatory terms and conditions for (and transparent manner of) making data available in business-to-business relations, where the obligation to share data is enshrined in law (including the Data Act itself). The dispute settlement rules can also be used by customers and providers of data processing services to settle disputes relating to breaches of the provisions of the Data Act dealing with such services.

A decision to have recourse to a dispute settlement body is voluntary and should be agreed by both parties to the dispute. In addition, a decision of a dispute settlement body binds the parties only if they have explicitly consented to its binding nature prior to the start of the dispute settlement proceedings.

A dispute settlement body may not be tasked with resolving a dispute if it has already been brought before another dispute settlement body or before a court or tribunal of a Member State.

Unfairness in business-to-business data-sharing contracts

38. What special provisions exist to help SMEs, given that they are often in a weaker negotiating position?

Chapter IV does not specifically address SMEs, but the prohibition on unfair contractual terms is expected to benefit businesses upon whom a contractual term was unilaterally imposed.

Given that SMEs often have limited market power and weaker negotiating positions, Chapter IV will therefore provide particular support to them, especially when they seek access to data held by larger companies. If an SME needs to submit a complaint or raise a concern, it can, for instance, contact the data coordinator in its Member State (see the answer to Question 64).

The European Commission will recommend model contractual terms for data sharing that reflect the rights and obligations of the Data Act and that will be intended to help SMEs negotiate better. These models will be voluntary. The Commission will have adopted them by the time the Data Act starts to apply.

39. I think that the data-sharing contractual terms in my contract are unfair. What can I do?

Firstly, it should be ascertained that the terms in question are covered by Article 13 of the Data Act:

a) they concern access to and the use of data or liability and remedies for the breach or termination of data-related obligations;

b) they do not reflect mandatory provisions of EU law, or provisions of EU law that would apply if the contractual terms did not regulate the matter;

c) they are unilaterally imposed; and

d) both parties to the contract are enterprises.

Secondly, it should be assessed whether the terms grossly deviate from good commercial practice in data access and use, contrary to good faith and fair dealing. A non-exclusive list of such terms is provided in Article 13(4). Such terms should always be considered unfair.

Thirdly, the terms in question might fall into a different category: terms which are only presumed to be unfair. The party imposing them can rebut such a presumption by presenting evidence to the contrary. Such terms are listed in Article 13(5).

If the conclusion of the above assessment confirms that a term in a contract is unfair or presumed to be unfair, the party imposing such a term should be asked to withdraw from the contract. In any case, a term found to be unfair will not be binding on the party on which it is imposed. The remaining contract terms will continue to be binding if the unfair term can be separated from them (i.e. it is sufficiently stand-alone).

If the imposing party disputes the outcome of the assessment and does not withdraw the term, the matter can be brought in front of a competent authority, the courts or (if the other party agrees) a dispute settlement body.

Business-to-government data access

40. What qualifies as 'mitigation of or recovery from' a public emergency?

The Data Act does not clarify these concepts, but Article 15 clearly distinguishes them from 'public emergency response' (Article 15(1)(a)), which suggests that they are distinct from the actual occurrence of a public emergency, in particular in terms of timing. The factors to be considered when identifying an activity as 'mitigation or recovery from a public emergency' are likely to be laid down in national law, because mitigation or recovery from a public emergency must be designated as a "specific task carried out in the public interest, that has been explicitly provided for by law" in order to be relevant for Chapter V requests.

41. What does the term 'equivalent conditions' mean in the context of Article 15(1)(a)?

'Under equivalent conditions' could be read in the context of this Article as a rule requiring a public sector body wishing to use its rights under Chapter V to first verify whether the same data could not be obtained elsewhere, while at the same time requiring a comparable amount of effort. The last sentence of recital 64 provides some examples in this regard.

42. Could the new rights under the Data Act endanger data holders' existing business models because a public sector could request the data instead of purchasing it?

There is little risk of current business models being seriously affected. This is because - in all situations other than an exceptional need for data to directly respond to a public emergency, and where an option of purchasing non-personal data is available to the public body - the data will need to be purchased at the market price (note the exception in Article 15(3)). A public sector body can rely on the process outlined in Article 15(1)(b) only if it has been unable to obtain the non-personal data - either because the data cannot be purchased or because the public sector body made an unsuccessful attempt to buy it at the market rate (e.g. via procurement).

43. How can a data holder verify that a Chapter V request is justified and lawful?

Data holders should verify the following:

- Is the requesting entity a public sector body of a Member State or one of the EU-level entities listed in Article 17(1)?
- Is there sufficient and clear justification regarding the choice of the data holder, the scope of specific data, the existence of an exceptional need, the duration of use, the nature of the public task and the purpose for requesting the data (as per Article 17(1)(a)-(j))?
- Is the request proportionate (e.g. in terms of data scope and granularity) to the exceptional need described?

- If personal data are requested – are the necessary conditions described in Articles - 17(1)(g) and 17(2)(e) fulfilled?
- Have all the necessary authorities been notified (e.g. if the request is made by a public sector body from a different Member State)?
- In the case of justified doubts as to the conditions listed above, the data holder should be able to ask for clarification and, ultimately, refuse the request or ask for its modification. In such a case, the requesting entity may ask the competent authority to settle the matter.

44. Can a public body in one country request data from a data holder in a different country? Are the rights of the data holder fully protected in such a case?

Yes. The Data Act includes the right for a public sector body to request data from data holders (companies) located in a Member State that is not the Member State of the requesting public sector body. This right may be important in the case of cross-border emergencies (e.g. natural disasters).

As always, the request needs to fulfil all the requirements under Article 17. This means that it must be formulated in clear, concise, and plain language that the data holder can understand.

Article 22 of the Data Act contains a specific procedure for cross-border requests to ensure the data holder's protection. Such requests are always notified to the competent authority of the data holder's Member State for *ex ante* examination.

45. Once data are made available following a request, do they become public sector information? Can the public sector body use them in any way it sees fit?

No. The requested data do not become public sector information that has to be made openly re-usable under Directive (EU) 2019/1024 (the Open Data Directive). In principle, the data can only be used for the specific purpose set out in the request and only by the requesting body. However, the requesting body may require the involvement of another public sector body or third party in carrying out a public sector task for which the data were requested. If so, the relevant public body or third party should already be identified in the request - as per Article 17(1)(f).

Article 21 describes two situations in which the requested data can be shared onwards: (i) for carrying out scientific research or analytics compatible with the purpose for which the data were requested and (ii) for the production of official statistics. The data holder should be notified if such a transfer takes place, so that they have the opportunity to lodge a complaint with the competent authority.

Data that are shared under the mechanism described in Article 21 must be deleted no later than 6 months after the fulfilment of the original purpose for which the data had been requested.

46. Can a request under Chapter V be made repetitively or simultaneously by different public sector bodies?

A data holder cannot be expected to respond to repetitive requests for the same data. Public sector bodies should first check if the data are already available within the public sector. The Data Act therefore empowers a data holder to refuse a request if (i) a similar request for the same purpose has been previously submitted by another public sector body or the Commission, the European Central Bank, or another EU body and (ii) the data holder has not been notified of the erasure of the data pursuant to Article 19(1)(c) of the Data Act.

47. Could Chapter V be used by governments in a way that puts citizens' fundamental rights in danger?

The co-legislators have carefully drafted the text of Chapter V to limit the possibility for public sector bodies to put the rights of the citizens and companies at risk, even unintentionally. Specific provisions ensure that the need to request data justified by an exceptional need cannot in any way lower the protection of personal data or of trade secrets. These provisions primarily include Article 17 with a detailed list of requirements for a valid request, as well as Articles 18(4), 19(1)(b) and 19(3)-(4).

Any alleged infringement of the provisions of Chapter V of the Data Act can be brought to the relevant courts or to the competent authority of the Member State in which the data holder is established.

48. Can a public sector body be a 'user' of a connected product/related service under Chapter II?

Yes. Nothing prevents a public sector body (as a separate legal entity) from becoming a user in the sense of Chapter II (see recital 18).

Switching between data processing services

49. Which services are excluded from the scope of Chapter VI?

Articles 23-32 and 34-35 apply to providers of data processing services. The definition of a data processing service is laid down in Article 2(8) and mirrors common definitions of cloud computing services. The concept is designed to cover the popular delivery models - Infrastructure as a Service (IaaS), Platform as a service (PaaS) and Software as a Service (SaaS) - while also remaining open to technological innovation.

Article 31 introduces a specific regime for (i) data processing services that are custom-built and not offered on a broad commercial scale and (ii) for data processing services that are provided as a testing/beta version. However, this does not mean that custom-built services are fully excluded from the scope of Chapter VI. The provisions not listed in Article 31(1) still apply. For example, providers of such services must make open interfaces available and ensure that data are exported in a structured, commonly used and machine-readable format.

50. What is the difference between exportable data and digital assets? What do these concepts mean?

According to Article 2(38), the concept of "exportable data" covers input and output data. It also includes metadata directly or indirectly generated, or co-generated, by the customer's use of the respective data processing service. These concepts exclude data protected as intellectual property and trade secrets of the provider or a third party.

"Digital assets" are defined in Article 2(32). They are elements that the customer needs in order to be able to effectively use their data in the environment of a new service provider to which they have switched. Digital assets therefore cover other types of metadata, for example those related to the configuration of settings, security and access and control rights management. Applications as well as virtualisation technologies (e.g. virtual machines and containers) can also count as digital assets. As part of the switching process, digital assets can be ported from a source provider to a destination provider if the customer has the right to use these assets, independent from their contractual relationship with the provider of data processing service that the customer intends to switch from.

51. What is the deadline for providers to reduce switching charges so that they are limited to the costs they incur?

Pursuant to Article 29(2), providers of data processing services must reduce any switching charges (including egress charges) from 11 January 2024 onwards. Concretely, they must limit any switching charges to the costs that they incur in order to make the respective switching operation happen. From 12 January 2027 onwards, providers will no longer be allowed to charge for switching (including data egress).

A special rule applies when a customer does not switch but instead asks a provider to provide services in parallel with other services, (e.g. in a multi-cloud deployment model). In such cases of in-parallel use, the provider may still bill the customer for the costs incurred for data egress, even after 12 January 2027. This is because a multi-cloud deployment may imply a constant data egress as opposed to the one-off data egress that can be expected for a switching operation.

52. What does 'free-tier offering' mean?

Article 23(c) clarifies that customers who have benefited from a free-tier offering can also benefit from switching. A free-tier offering (sometimes referred to as cloud credits) is a free offer of data processing services from a provider to a customer. Free-tier offerings are intended to allow customers to test a data processing service or to assist start-up companies.

53. How do the notice period and the transition period relate to one another?

Article 25 provides that the notice period begins once the customer notifies the provider of data processing services of their desire to switch to another provider or to an on-premises ICT infrastructure. Switching should be completed by the end of the transition period, which starts after the end of the notice period (maximum 2 months).

During the transition period (maximum 30 calendar days), the provider must carry out the actions needed to enable the customer's switching – in close cooperation with the customer themselves and, where applicable, with the customer's new provider. The customer has the right to replace the 30-day transition period with a longer period. The provider can only extend the transition period if the provider can, within 14 days during the notice period, prove that a transition period of maximum 30 days would be technically unfeasible. In this case, the transition period can last a maximum of 7 months.

54. How will the Commission create the common Union repository for the interoperability of data processing services?

The process is laid down in Article 35.

The repository will take the form of an online platform. It will become a one-stop-shop for providers to see which harmonised standards or common specifications (on the basis of open interoperability specifications) apply to the type of service they offer. Providers must ensure that the interfaces that they make accessible to customers are compatible with the standards/specifications referenced in the repository. The aim is to ensure that cloud services are interoperable so that customers can benefit from switching without losing functionalities, and to make it easier for providers to support their customers in the switching process.

As a first step, the Commission will map existing harmonised standards and open interoperability specifications that qualify for recognition in the repository. Before the Commission can take a harmonised standard or a common specification up in the repository, it must adopt an implementing act. Following the

mapping, the next step will be the preparation of the implementing act, which will be adopted in a comitology procedure.

The repository will be a living document and will be continuously updated with new relevant harmonised standards and common specifications per service type.

55. What is the status quo of the standard contractual clauses for cloud computing contracts and what will they cover?

As per Article 41 of the Data Act, an Expert Group on B2B data sharing and cloud computing contracts, jointly managed by DG JUST and DG CNECT, is currently developing model contractual terms for data sharing and standard contractual clauses for cloud computing contracts.

The standard contractual clauses for cloud computing contracts are non-binding and can be adapted by the parties according to their contractual needs. Based on the Report of the Expert Group, the Commission will adopt a recommendation. This is expected to happen before 12 September 2025.

The standard contractual clauses for cloud computing contracts will cover elements related to switching & exit, term & termination, non-dispersion, non-amendment, security & business continuity and to liability. These elements mirror the aspects covered by Chapter VI but also include other aspects that are relevant for fulfilling the objective of Art. 41, which is to assist parties in drafting and negotiating contracts with fair, reasonable, and non-discriminatory contractual rights and obligations.

Unlawful access to and transfer of non-personal data held in the EU by third country authorities

56. Will the Data Act create data localisation requirements?

The Data Act does not limit companies' ability to transfer non-personal data internationally. It does not change the prohibition of national data localisation requirements as presented in the Free Flow of Non-personal Data Regulation.

Users of cloud services will continue to be free to choose a cloud provider of their liking and to decide where to store their data.

57. What is the aim of Article 32?

Article 32 ensures that customers of cloud service providers that choose to store their non-personal data in the EU are protected from having their data unlawfully accessed by or transferred to non-EU governments. To this end, the cloud service provider must put in place all adequate technical, organisation and legal measures in order to prevent unlawful or illegitimate government access to or transfer of the customer's data (cf. Article 28).

An unlawful access to or transfer of data may occur when such access or transfer would clash with obligations under EU or Member State law, such as regarding the protection of fundamental rights of the individual, or the protection of commercially sensitive data, including trade secrets and intellectual property rights (cf. recital 101).

In case of access or transfer request made by a third country authority to a customer's non-personal data, the cloud service provider is obliged to verify its lawfulness. Lawfulness exists, for instance, where the request is based on an international agreement such as a mutual legal assistance treaty. In the absence of an international agreement, the request must comply with certain procedural safeguards that are aligned with fundamental rules and norms in the EU legal order, such as proportionality of the request and judicial review.

The definition of 'government' or 'public authority' should not be too narrow when evaluating whether a particular body falls in that category.

58. Does Article 32 cover international data transfers between or inside businesses?

No. Similar to the Data Governance Act's Article 31, the Data Act's Article 32 covers only a very small and specific subset of international data flows – those which result from an unlawful access to or transfer of non-personal data by non-EU public authorities.

These Articles do not cover data transfers between private entities on both sides of the EU border. Rather, they prevent access to or transfers of non-personal data by non-EU public authorities that are contrary to EU or Member State law. International transfers of personal data are regulated under the GDPR.

59. What measures should data processing service providers implement to prevent unlawful governmental access to or transfer of data?

Recital 102 states that data processing service providers "should take all reasonable measures to prevent access to systems on which non-personal data are stored, including, where relevant, through the encryption of data, frequent submission to audits, verified adherence to relevant security reassurance certification schemes, and by the modification of corporate policies." The Commission encourages the development, deployment, and regular update of these measures.

The Commission may in the future decide to offer further guidance on this point to the competent authorities, following the advice of the EDIB.

60. Which bodies can a data processing service provider consult before deciding whether to grant access or transfer data following a request from third country authorities?

To identify the "relevant national body or authority competent for international cooperation in legal matters" under Chapter VII of the Data Act, a data processing service provider must check which administrative entity in their Member State is normally responsible for the implementation of Mutual Legal Assistance Treaties (MLATs). In the case of France, it could for example be the Bureau de l'entraide pénale internationale, which is a unit within the French Ministry of Justice. In Germany, the Bundesjustizamt acts as the central point of international collaboration.

In case of doubt, the addressee may also consult the Member State's data coordinator.

Interoperability

61. Can the Commission impose common specifications instead of standards?

The Data Act expresses a clear preference for standards to be developed by the EU standardisation bodies instead of imposing common specifications. Recital 103 confirms that "*Common specifications should be adopted only as an exceptional fall-back solution to facilitate compliance with the essential requirements of this Regulation, or when the standardisation process is blocked, or when there are delays in the establishment of appropriate harmonised standards*".

Moreover, the Commission can, taking into account the advice of the European Data Innovation Board, supplement the Data Act by adopting delegated acts which further specify those essential requirements laid down Article 33(1) that cannot produce the intended effect unless they are further specified by EU law.

For interoperability of data processing services (Article 35), the Data Act establishes the central Union standards repository for the interoperability of data processing services. References to both harmonised standards and common specifications can be published in the repository. Common specifications can be adopted based on open interoperability specifications if these comply with the requirements laid down in Article 35(1) and (2). In line with Article 30(1), providers of data processing services other than those of the Infrastructure as a Service delivery model must ensure compatibility with the common specifications and harmonised standards referenced in the repository, at least 12 months after the publication therein. See Question 54.

62. Is the Commission intending to replace existing (e.g. sectoral) standards?

No. There is no such intention. Instead, the Data Act requires that sectoral specification should only be developed based on those sectors' specific needs, which should be carefully assessed. In addition, the Data Act should be without prejudice to more specific EU rules, such as in the context of the development of common European data spaces.

63. Do the essential requirements in Article 36 affect national contract law?

The essential requirements applicable to smart contracts do not affect national contract law. The definition of 'smart contract' makes it clear that only computer programs used for executions of agreements - and not the agreements as such - are regulated by the Data Act.

Enforcement

64. What bodies should Member States put in place to ensure that the Data Act is enforceable?

The Member States are required to designate at least one competent authority to deal with the enforcement of the Data Act and carry out the tasks listed in Article 37(5). The competent authority may be newly created but it can also be an already existing public sector body. It is possible that Member States will appoint more than one such competent authority. If so, they will also have to designate from among them a 'data coordinator' - an additional competent authority whose role will be to facilitate cooperation between competent authorities and help entities wishing to have their rights under the Data Act enforced (as a 'single point of contact'). In practice, the data coordinator will be expected to receive questions from companies or consumers and guide them to the authority which will be the right 'competent authority' in their specific case.

It is important to note that the DPAs remain responsible for monitoring the application of the Data Act insofar as the protection of personal data is concerned.

Moreover, it is crucial that the Data Act is applied efficiently across all sectors. Competent authorities must therefore cooperate with sectoral authorities to ensure the Data Act is enforced consistently with other EU or national laws.

The Commission will work closely with these authorities, including through the European Data Innovation Board, to ensure the seamless and uniform application of the Data Act. This effort may include issuing sector-specific guidelines for the effective application of data access and use rules.

65. Which public authority can help me if I consider that my rights under the Data Act are not respected?

If a Member State designates only one competent authority, this authority will oversee all matters relating to the application of the Data Act. In any event, the name of the competent authorities for each Member States along with the corresponding tasks and powers will be displayed on a publicly available register maintained by the Commission. In case of doubt, applicants can always direct their queries to the data coordinator in their Member State, because it should act as the single point of contact for all issues related to the application of the Data Act. In certain cases, the data coordinator may facilitate cooperation between competent authorities.

Natural and legal persons should lodge complaints with the relevant competent authority in the Member State of their habitual residence, place of work or establishment, including with respect to cross-border matters. The competent authorities have a duty to cooperate and assist each other not only within the same Member State but also across borders.

66. What is the role of the Commission in the enforcement of the Data Act?

The enforcement of the Data Act is primarily the responsibility of the Member States' authorities, but the Commission plays a supportive role. It hosts the European Data Innovation Board (EDIB), an expert group which facilitates cooperation between competent authorities, promotes best practices and common approaches in enforcement. In addition, the Commission provides publicly available information on the competent authorities and on national legislation and measures in relation to penalties. To support market players in observing the rights and obligations introduced by the Data Act, the Commission will also recommend model contract terms for data sharing agreements and standard contractual clauses for cloud computing contracts that reflect the provisions of the Data Act.

67. Are penalties harmonised across the EU?

The Member States are responsible for setting penalties and all the necessary measures relative to their application. However, to ensure high consistency across the EU, the EDIB will be used as a platform to evaluate, coordinate, and adopt recommendations on setting penalties for infringements of the Data Act.

DPAs may within their scope of competence impose fines in accordance with the GDPR for the infringements of the obligations laid down in Chapter II, III and V of the Data Act. The EDPS may, within its scope of competence, impose administrative fines in accordance with Regulation (EU) 2018/1725 for infringements of the obligations laid down in Chapter V.

68. When should a legal representative be designated? Is such a legal representative liable for non-compliance with the Data Act by companies outside the EU?

The legal representative's role is to facilitate compliance with the Data Act by entities that make their services or products available in the EU market but are established outside the EU. All such entities must designate an EU-based representative. The competent authorities can address such a representative in all matters related to the implementation of the Data Act instead of or in addition to the non-EU entity. However, their liability is limited to their obligations as representatives under the Data Act. The role and responsibilities of legal representatives under the Data Act is similar to that of legal representatives under the GDPR (cf. European Data Protection Board Guidelines 3/2018).

Next steps and future actions

69. When will the Commission publish the guidance on reasonable compensation?

In line with Article 9(5) of the Data Act, the EDIB must be consulted on the guidelines on calculating reasonable compensation for making data available before their adoption. The EDIB will only have the competence to pronounce itself on the matter after the Data Act becomes applicable.

70. What are the next steps regarding interoperability?

In support of Article 33 of the Data Act on requirements related to interoperability in data spaces, the Commission has prepared a standardisation request called the "European Trusted Data Framework".

The request covers five EU standards/standardisation deliverables that are closely aligned with the recommendations of the data interoperability workstream of the High-Level Forum on European Standardisation.

The request is currently under consultation with the European standardisation organisations (CEN, CENELEC and ETSI), the EU stakeholder organisations representing consumers, environmental interests, trade unions and SMEs in standardisation (SBS, ETUC, ANEC and ECOS), and the European Data Innovation Board.

It is expected that the request will be formally adopted by the end of 2024.

71. What is the status quo of the model contractual terms for data sharing and the standard contractual clauses for cloud computing contracts?

As per Article 41 of the Data Act, the Expert Group on B2B data sharing and cloud computing contracts, which is jointly managed by DG JUST and DG CNECT, is currently developing model contractual terms for data sharing and standard contractual clauses for cloud computing contracts.

The model contractual terms for data sharing will cover contracts between data holders and users, data holders and data recipients, and between users and data recipients.

The standard contractual clauses for cloud computing contracts will cover elements related to switching & exit, term & termination, non-dispersion, non-amendment, security & business continuity and to liability. These elements mirror the aspects covered by Chapter VI but also include other aspects that are relevant for fulfilling the objective of Art. 41, which is to assist parties in drafting and negotiating contracts with fair, reasonable, and non-discriminatory contractual rights and obligations.

The contracts are non-binding and can be adapted by the parties according to their contractual needs. Based on the Report of the Expert Group, the Commission will adopt a recommendation, which is expected to happen before 12 September 2025.