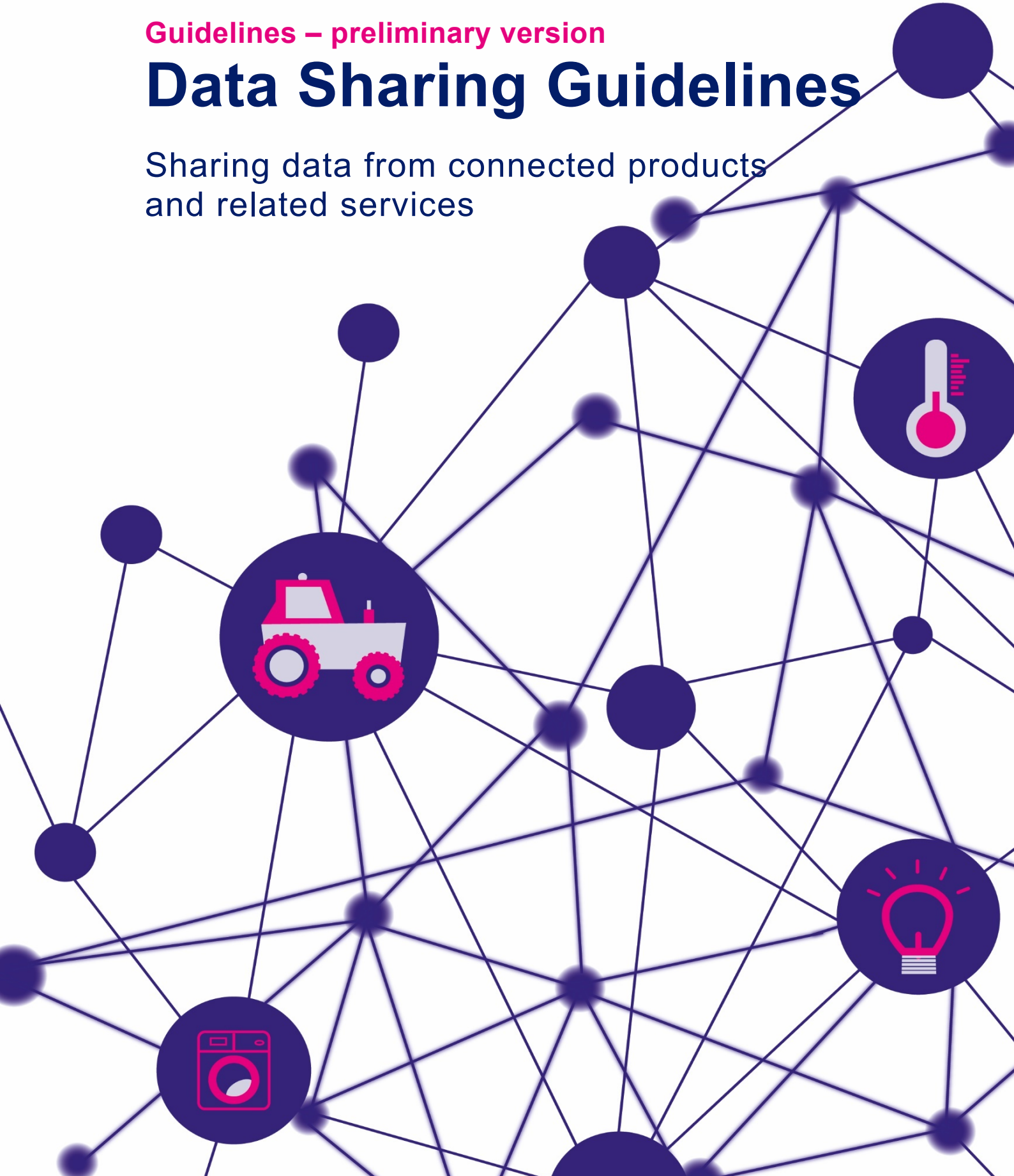
Authority for
Consumers & Markets

Public

Guidelines – preliminary version

Data Sharing Guidelines

Sharing data from connected products and related services



Summary

Purpose of the Data Act

Main objective and background
The Netherlands Authority for Consumers and Markets (ACM) is publishing the preliminary version of these guidelines for the European Data Act, which entered into force on September 12, 2025. This regulation is part of the EU's data strategy, which aims to create a single data market facilitating the free flow of data. To this end, the Data Act establishes rules for data sharing and cloud services, among other things. These guidelines, which are preliminary, only cover the chapters of the Data Act that deal with data sharing. The final version will be published by ACM later this year.

A key premise is that users should have control over the data collected by connected products and related services. Connected products are devices that can exchange data via an electronic communications service (such as the internet), a cable or the device itself. Examples include smart thermostats, modern cars and milking robots. These devices can often be controlled remotely and collect different types of data through sensors. A related service is a digital service tied to a connected product that can affect the functionality, behavior or operation of the connected product, such as an app used to control a smart thermostat.

The Data Act is a directly applicable European regulation with general validity in all member states, and it binds both natural and legal persons (such as companies and organizations). Under certain conditions, the regulation also has extraterritorial effect, making it applicable to organizations outside the European Union (EU) when they offer goods or digital services to users within the EU.

These guidelines are mainly intended for organizations that are subject to certain obligations under the Data Act, such as manufacturers, suppliers, seller, rentors and lessors of connected products and related services within the EU.

Oversight
ACM has been designated as the primary regulator for the Data Act, and as the data coordinator for the Netherlands. The Dutch Data Protection Authority (DPA) has also been given a number of regulatory tasks. These Dutch authorities oversee organizations whose global or European headquarters are located in the Netherlands.

Structure
For the purposes of this summary, the obligations of the Data Act have been categorized into three themes: (1) disclosure obligations; (2) obligations related to providing access to data from connected products and related services; and (3) requirements, conditions and agreements. For each of these themes, a brief explanation of the relevant obligations is provided. Relevant terms are defined only if they are not generally known or if the definitions used differ substantially from the common meaning. A detailed glossary can be found in Section 2.

Theme 1 Disclosure obligations

The Data Act imposes specific disclosure obligations on providers of connected products or related services. The obligations apply before entering into an agreement to purchase, rent or lease a connected product, or to provide a related service.

Disclosure obligations for connected products
In the case of a connected product, the disclosure obligation rests with the seller, rentor or lessor. The following information must be disclosed:

- The type of data generated by the connected product;
- The format and approximate volume of the data, as well as information on continuous and real-time data generation capabilities;
- Where the connected product may store data and how long this data is retained;
- How the user can access, retrieve or delete data. This includes information about the technical resources required to do so, including about the terms of use and quality of these resources;
- The identity of the data holder. This is the person or organization, which has the right or obligation to use or make available data from a connected product or related service, from whom the user can retrieve the data.

Disclosure obligations for related services
In the case of a related service, the provider of the service is responsible for disclosure. The following information must be disclosed:

- The nature of the data collected by the data holder, its estimated volume and the frequency of collection. In addition, the types and quantities of data generated by the related service itself should be disclosed;
- How the data is used. This concerns the expected use of data by the data holder as well as by third parties. The identities of the data holder and other data processing parties must be provided as well;
- The available means of communication;
- How the user can initiate or stop data sharing with a third party;
- The user's right to file complaints with the competent authority;
- Any trade secrets included in the accessible data and who holds them;
- The duration of the contract and termination provisions, including what happens to the data upon termination of the contract.

General requirements

- The disclosed information must be clear and written in either Dutch or English.
- If any information changes during the lifetime of the connected product or the contract period of the related service, the updated information must be provided to the user.

Theme 2 Access obligations

The Data Act provides comprehensive regulations governing access to data generated by a connected product or related service. Access should be easy, secure and free of charge, and data should be made available in an accessible and generally usable format. Access can be provided in two ways: directly (access by design) or indirectly (access upon request).

Direct access (access by design)
Where relevant and technically feasible, connected products and related services should be designed so that users can access data directly and without disproportionate effort. Users must be able to access data using the technical means available to them, without having to rely on third parties. The access obligation applies to the party responsible for the design and production of a connected product or related service, typically the manufacturer or designer. In some cases, it applies to multiple parties.

Technical feasibility is assessed based on the available technology, resources and knowledge, taking into account development costs, security requirements, and the protection of trade secrets and intellectual property. “Relevant” means that the manufacturer may take into account the specific characteristics of different connected products or related services.

Indirect access (access upon request)
If direct access cannot be provided, the data holder must make data available to the user immediately upon their request. The user should be able to submit a request through simple electronic means. The data holder may verify the user’s identity, but must not use excessive means to do so.

The user may also request that the data holder grant a third party access to the data. This option to share data must always be available and is independent of whether the user themselves has direct or indirect access. To provide access to a third party, the data holder must enter into an agreement with the third party to specify the terms and potential fees.

What data must be made available
The access obligation applies to data generated by the use of a connected product or related service. This is data resulting from interactions between the user or their environment and a connected product or related service. This data may have been pre-processed with the goal of making it understandable. It also includes “metadata” that describes the content or use of the data, making it easier to find or use.

The Data Act’s access obligation does not apply to *derived data*, which has been processed by the data holder in such a way that it leads to new, valuable insights. This processing must go beyond simple transformation to improve readability.

Grounds for exception: security risks and trade secrets
Under certain circumstances, data holders and users may restrict or deny data sharing. This can be done in view of security risks or to protect trade secrets. Security risks are a factor in situations where access to data would compromise the security requirements of a connected product.

If there is a risk of trade secret violation, the data holder must determine what constitutes a trade secret. If data sharing is requested, the necessary measures to ensure confidentiality must be agreed upon with the user or third party. If such measures are not agreed upon or complied with, data sharing may be suspended. In exceptional cases, where the data holder can prove that sharing data would be very likely to cause serious financial harm, access to specific data may be denied.

If the data holder refuses to share data, it must notify ACM. This can be done using a dedicated form on

ACM's website. In either situation, the user or third party, if there is a risk of trade secret violation, may file a complaint with ACM. The user or third party may also seek dispute resolution from a certified dispute resolution body or take the matter to court.

Theme 3 Requirements, conditions and agreements

The Data Act contains detailed provisions on the contractual relationship between the data holder and the data recipient. It sets out specific rules for all parties involved regarding the permitted use of data, in addition to regulating what agreements parties may make among themselves.

Requirements for data holders

- The data holder may use data only if this has been agreed upon in advance (contractually) with the user. The data holder may not use this data to harm the commercial position of the user or a third party.
- The data holder may only share data with a third party for purposes specified in the agreement with the user. In the contract with the third party, the data holder must stipulate that the third party may not share the data with other parties.
- Technical protective measures aimed at preventing unauthorized access to the data are allowed. These measures must be proportionate and non-discriminatory.
- The data holder must comply with the General Data Protection Regulation (GDPR) without prejudice. This means that personal data may only be processed if there is a valid legal basis for doing so under the GDPR.

Requirements for users and third parties

- Data may not be used to develop competing connected products, but may be used to develop related or other services.
- Data may not be used to gain insight into the financial situation of a manufacturer or data holder, to pressure the data holder into providing data access, or to modify technical safeguards without the explicit consent of the data holder.

Specific requirements for third parties

- The third party may only use received data for purposes authorized by the user and in accordance with the agreed conditions. Data must be deleted as soon as it is no longer needed for the agreed purpose, unless otherwise agreed for non-personal data.
- It should be as easy for the user to deny or stop third party access to the data as it is for them to grant access. The third party should not make it needlessly difficult for the user to exercise their choices or rights.
- The third party may not use the data received to profile individuals, unless this is necessary in order to provide the service requested by the user.
- The third party may not share the data received with another third party, unless the user has agreed to this.
- The third party may not share the data received with companies designated as gatekeepers as referred to in the Digital Markets Act.
- The third party may not use the data received in a way that would negatively impact the security of a connected product or related service.
- The third party is expected to comply with the specific measures agreed with the data holder or trade secret holder. Moreover, the third party is explicitly prohibited from compromising the confidentiality of trade secrets.
- The third party receiving data may not hinder a user who is a consumer, through contract terms or otherwise, from sharing the data with another party.

Remedies
If a data recipient fails to comply with the above requirements, the data holder, user or trade secret holder may invoke remedies. These remedies include erasing data, ceasing production and trading, informing users, and compensating a party who has suffered damage.

Conditions for data sharing with third parties
If the data holder is required to share data with a third party, this should be subject to an agreement with fair, reasonable, non-discriminatory and transparent terms (FRAND standards). In addition, the Data Act stipulates that certain unilaterally imposed contractual provisions are considered unfair and therefore not binding.

Reasonable compensation
The data holder and data recipient may mutually agree on a fee for data sharing. This is permitted only in business-to-business relationships; it is not permitted in relationships between data holders and consumers. The fee should not be construed as payment for the data itself.

When agreeing fees, the main costs to consider should be the technical costs of data sharing and investments in data collection and production. For micro and small enterprises and non-profit research organizations, only the technical costs of data sharing may be included.

Standard contracts
The European Commission has developed and recommended model contractual terms (MCTs) to assist relevant parties in implementing these requirements. These MCTs provide templates for fair, reasonable and non-discriminatory contractual rights and obligations, including with regard to the protection of trade secrets. While the use of MCTs is not mandatory, they offer practical guidelines for ensuring compliance with the Data Act in various types of commercial relationships.

Contents

1 Introduction

1. This preliminary document offers guidelines for sharing data from connected products and related services. With these guidelines, the Netherlands Authority for Consumers and Markets (ACM) aims to help companies that offer connected products or related services understand their obligations under the Data Act.[1] These guidelines focus on the obligations outlined in Chapters II and III of the Data Act, which primarily address the rights and obligations regarding access to and use of data from connected products and related services. This is a preliminary version of the guidelines. The European Commission will publish additional guidance later this year. Once this is available, ACM will finalize the guidelines.

1.1 The Data Act

2. The Data Act entered into force on September 12, 2025, as part of the EU's data strategy. With this strategy, the EU is taking the lead in developing a data-driven economy while working towards a single market for data that will allow data to flow freely between all sectors, across the entire EU.[2] In this context, access to data and the ability to use it are essential drivers of innovation and economic growth.[3]

3. The Data Act provides rules to achieve these goals. A key premise is that users should have control over the data collected by their connected products, also known as smart devices.[4] These are devices that can exchange data via an electronic communications service (such as the internet), a cable or the device itself. Examples include smart thermostats, modern cars and milking robots. These devices can often be controlled remotely and collect different types of data through sensors. Using such a product, or a related service, generates data. The Data Act will give users more control over and, if desired, access to this data.

4. In order to ensure that users properly understand what data is collected through the use of a connected product, they must be provided with this information when they purchase, lease or rent the product in question. Moreover, users must be able to access this data. The data holder – typically the manufacturer or developer of the connected product – is responsible for providing this access. Users may use the requested data for their own analyses, for example. They may also share the data with a third party, or request that the data holder give a third party direct access to the data.

5. These rules apply not only to connected products, but also to related services. A related service is a digital service tied to a connected product that can affect the functionality, behavior or operation of the connected product.[5]

6. The Data Act offers detailed information on how these obligations should be met, including with regard to the types of data involved and how access should be granted. In addition, the regulation includes several safeguards and exceptions to protect data holders, despite their obligation to share data upon user request. ACM explains these rules and conditions in these guidelines.

7. The Data Act also includes a list of provisions on data access and use that are considered unfair if imposed unilaterally by a company. Such provisions are considered invalid and non-binding.[6]

[1] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).
[2] European Commission, *European data strategy: A Europe fit for the digital age*, available at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en.
[3] Recital 1 of the Data Act.
[4] For more information, see also marginal 44 of these guidelines.
[5] For more information, see also marginal 45 of these guidelines.
[6] Chapter IV of the Data Act.

8. The Data Act took effect on September 12, 2025. As of this date, manufacturers and data holders must comply with the rules set out in this regulation, and ensure that the products they offer comply with these rules as well.[7]

9. In addition to the obligations described above, the Data Act contains other regulations, including rules about switching to a different cloud provider and safeguards against the unlawful international transfer of data.[8] There are also other laws that fall under the European data strategy, such as the Data Governance Act,[9] which provides regulations for data intermediation services to ensure their reliability for people and organizations.[10] These regulations are not covered in these guidelines. However, ACM does intend to publish guidelines on the Data Act's cloud provisions later this year.

1.2 The objective of these guidelines

10. The Data Act Implementation Act designates ACM as the primary regulator for the Data Act, and as the data coordinator for the Netherlands.[11] In these roles, ACM works to promote data sharing in the Netherlands. ACM believes that users should have control over their data and be aware of the opportunities that arise from sharing it.

11. ACM is committed to promoting compliance with the Data Act. If ACM's oversight reveals a suspected violation of the Data Act, it may take enforcement action. If enforcement action is taken, the focus is always on the effect of the intervention. This means that ACM will assess which intervention is most appropriate. In doing so, ACM will consider the severity of the violation and the potential harm it could cause.

12. These guidelines are intended to assist organizations in complying with the rules of the Data Act. They may also be useful to consultants, lawyers and industry associations. ACM's explanatory notes set out the relevant considerations of the Data Act. They also provide references to related legislation and guidance from the European Commission, as well as a number of examples.

13. The explanations in these guidelines are closely aligned with the text of the Data Act. In addition, two documents published by the European Commission were used in writing these guidelines: "Frequently Asked Questions about the Data Act" (hereafter: the European Commission's FAQ)[12] and the document "Guidance on vehicle data, accompanying the Data Act" (hereafter: European Commission Vehicle Data Guidance).[13] ACM also used draft versions of upcoming guidelines from the European Commission, which will be published later this year. These sources are referenced where appropriate.

14. Besides ACM, the Dutch Data Protection Authority (DPA) is also responsible for enforcing certain provisions of the Data Act. No provision has more than one regulator. Thus, the regulatory activities of ACM and the DPA are aligned and do not overlap. In carrying out their regulatory tasks, ACM and the DPA work closely together, for example by exchanging information and reports.[14] Since these guidelines were written by ACM,[15] they only explain the provisions regulated by ACM. These

[7] Exceptions to this rule and transitional law are discussed in Subsections 2.2 and 2.3 of these guidelines.
[8] Chapters VI, VII and VIII of the Data Act.
[9] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).
[10] For more information, see ACM, *Databemiddelingsdiensten*, available at https://www.acm.nl/nl/digitale-economie/data/databemiddelingsdiensten (Dutch only). See also European Commission, *Data Governance Act explained*, available at https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.
[11] Act of October 29, 2025, implementing Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).
[12] European Commission, *Frequently Asked Questions about the Data Act Version 1.4*, available at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act.
[13] European Commission, *Guidance on vehicle data, accompanying the Data Act*, available at https://digital-strategy.ec.europa.eu/en/library/guidance-vehicle-data-accompanying-data-act.
[14] For more information about this collaboration, see marginal 60 of these guidelines.
[15] ACM submitted a draft version of these guidelines to the DPA for feedback.

guidelines note when a provision is subject to the DPA's oversight, briefly discussing such provisions for the sake of completeness only.

15. Please note that this document is not a policy rule; it is intended solely as a resource for companies offering connected products or related services. These organizations themselves remain responsible for complying with the requirements of the Data Act and other laws and requirements. In these guidelines, ACM provides additional explanations of the obligations under the Data Act based on its current interpretation of the regulation. The present text is a preliminary version of the guidelines, which will be finalized once the European Commission provides additional guidance later this year. Moreover, interpretations of the regulation are still evolving and subject to change. This means that changing views, legislative developments and court rulings may affect how the provisions are interpreted. ACM aims to periodically update the guidelines based on regulatory experience, new insights and international agreements with other regulators.

1.3 Who are these guidelines intended for?

16. These guidelines are primarily intended for organizations that are or will be subject to requirements under the Data Act. These are all organizations that either bring to market connected products or related services in the EU, or that provide such products or services to users within the EU.[16] Examples include manufacturers of smart cars, sellers, rentors and lessors of such vehicles, and suppliers of applications used to manage car functionalities.

17. Thus, these guidelines are not primarily intended for companies and individuals that can derive user rights from the Data Act. ACM's website offers extensive information about these rights and how to invoke them.[17]

1.4 Reading guide

18. The structure of these guidelines does not reflect the order of the articles of the Data Act. This is because the structure of obligations and rights contained in the regulation is not always consistent with a practical approach. The sections and subsections making up these guidelines have therefore been organized by theme.

19. Section 2 of these guidelines provides general information about the Data Act. It addresses the scope of the Data Act, including to whom the obligations apply and their effective date. It also explains key roles outlined in the Data Act, such as which parties are required to provide information or access. Moreover, it clarifies key terms in the regulation and discusses its relationship to other legislation.

20. Section 3 addresses the various disclosure obligations related to the collection of, and access to, data from connected products and related services.

21. Section 4 discusses the obligations to provide access to data from connected products and related services. It explains the different forms of access, what data should be made accessible, and how access should be granted. It also discusses possible exceptions and the option of seeking dispute resolution.

22. Section 5 outlines the contractual and financial terms for data sharing. It addresses what agreements parties may and must make when exchanging data, as well as how to establish fair fees for accessing data and protections against unfair contractual terms.

[16] Article 1(3)(a) of the Data Act.
[17] See ACM, *Data uit slimme apparaten*, available at https://www.acm.nl/nl/digitale-economie/data/data-uit-slimme-apparaten (Dutch only).

23. Each section begins with a section-specific reading guide.

2 Scope and key terms

2.1 Introduction

24. This section explains the scope of the Data Act, the key actors involved and a number of important concepts. First, Subsection 2.2 sets out who and what the regulation applies to, both geographically and materially. Subsection 2.3 then explains when parties must be in compliance with the obligations set out in the Data Act. Subsection 2.4 discusses the key actors involved. Subsection 2.5 provides definitions of several important terms that are essential for further understanding and interpreting the provisions of the regulation. This is followed in Subsection 2.6 by a further explanation of the relationship between the Data Act and the General Data Protection Regulation (GDPR).[18] Finally, Subsection 2.7 briefly discusses concurrence with other relevant legislation.

2.2 Who does the Data Act apply to?

25. The Data Act is a regulation. This means that it has general application, and that all its provisions are binding and directly applicable in all EU member states.[19] Moreover, it applies to both natural and legal persons (such as companies and organizations) based in the EU.[20]

26. Under certain conditions, the Data Act can also apply to organizations outside the EU. It thus has extraterritorial effect, which is to say that it has implications beyond the borders of the EU. This is the case, for example, when a company based outside the EU provides goods or digital services to users within the EU.[21]

27. A connected product must comply with the Data Act if it is "placed on the Union market." This means that, within an EU member state, after production, there is a transfer of ownership, possession or other property right between two economic actors.[22] A connected product can be placed on the market only once. Any subsequent steps, such as resale or distribution – whether in the same member state or a different member state – fall under the category of "making [the product] available on the market."[23]

28. A related service falls within the scope of the Data Act if it is made available in a member state.[24]

29. Only persons and organizations based in the EU are considered users under the Data Act.[25]

30. Enforcement of the Data Act is based on the country-of-origin principle.[26] This means that an organization covered by the regulation is primarily regulated by the relevant authority of the member state in which it is located.[27] These regulators are responsible for enforcing compliance with the regulation, regardless of which other member states the products or services are offered in, or where the person or organization requesting the data is located. The country-of-origin principle promotes legal certainty and prevents the duplication of enforcement efforts. At the same time, the EU has a system of cooperation and information exchange between regulators, with the aim of ensuring consistent enforcement and the equal application of rules in the internal market.

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[19] See also European Commission, *Regulation*, available at https://eur-lex.europa.eu/EN/legal-content/glossary/regulation.html.
[20] Article 1(3) of the Data Act.
[21] Article 1(3) of the Data Act.
[22] Article 2(22) of the Data Act.
[23] Article 2(21) of the Data Act. For more information on this, see also question 8 in the European Commission's FAQ.
[24] Article 1(3)(a) of the Data Act.
[25] For more information on the term "user," see marginal 36 of these guidelines.
[26] Article 37(10) of the Data Act.
[27] Article 37, paragraphs 10 through 13 of the Data Act.

31. Micro and small enterprises are exempt from certain obligations under the Data Act.[28] They are not bound by the disclosure obligations discussed in Section 3 of these guidelines, nor by the access obligations set out in Section 4. The purpose of this exception is to encourage innovation by not placing an undue burden on small companies and start-ups. However, the Data Act also contains general provisions on unfair contractual terms. These provisions do apply to micro and small enterprises.

2.3 When did the provisions of the Data Act take effect?

32. The Data Act entered into force on September 12, 2025. Virtually all of the regulation's provisions took effect on that date. This means that sellers must now comply with the Data Act's disclosure obligations (see Section 3 of these guidelines), and that data holders must be able to grant user access (see Section 4 of these guidelines). Data generated or collected prior to this date does not fall within the scope of the Data Act.

33. An exception applies to the direct access obligation: the access-by-design obligation, which requires that connected products and related services be designed in such a way that data is directly retrievable by the user,[29] applies only to connected products and related services placed on the market after September 12, 2026.[30]

34. The provisions regarding unilaterally imposed terms apply only to: (1) contracts entered into after September 12, 2025; and (2) contracts entered into on or before September 12, 2025, provided these contracts are indefinite or will expire at least 10 years after January 11, 2024.[31]

2.4 Key actors in the Data Act

35. A number of key actors discussed in the Data Act are defined below.

36. **User**:[32] A person or organization with the right to use a connected product or receiving a related service.[33] There must be a stable right of use.[34] This may be a "permanent" right, such as ownership, or a temporary right, such as those obtained through renting or leasing.[35] The European Commission uses the terms "property-type of rights" and "ownership-like contractual right."[36] The user can be an individual consumer, a company or a government agency.[37] Examples of users include consumers who have a smart thermostat in their homes, hospitals that own an MRI scanner, and self-employed professionals who rent smart tractors for specific jobs. In some cases, more than one person may be a user within the meaning of the regulation, such as in the case of a shared car.[38] Examples of persons who use a connected product, but do not qualify as users under the Data Act, include a doctor using an MRI scanner or a passenger on an airplane.[39] Employees who use a connected product also usually do not qualify as users within the meaning of the regulation, as the ownership lies with the employer. Thus, the right to use a connected product granted by an employer is generally

[28] Article 7 of the Data Act. See also Article 2(2) of the Annex to Recommendation 2003/351/EC for definitions. A small enterprise has fewer than 50 employees and generates sales of less than 10 million euros per year. A micro enterprise has fewer than 10 employees and generates sales of less than 2 million euros per year. When counting the number of employees or determining revenue, the revenue and employees of any other legal entities within the same group must also be included.
[29] See also Subsection 4.3 of these guidelines.
[30] Article 50 of the Data Act.
[31] Article 50 of the Data Act. See also question 42b in the European Commission's FAQ and marginals 175 through 177 of these guidelines.
[32] Article 2(12) of the Data Act.
[33] See also question 14 in the European Commission's FAQ.
[34] See also question 14 in the European Commission's FAQ.
[35] Recital 18 of the Data Act. See also questions 14 and 16 in the European Commission's FAQ.
[36] See also question 14 in the European Commission's FAQ.
[37] Recital 18 of the Data Act.
[38] See also question 16 in the European Commission's FAQ.
[39] An airline passenger temporarily uses the aircraft on which they are flying. No "property-type of rights" are transferred to the passenger. In this context, a passenger is therefore not considered a user under Article 2(12) of the Data Act. See also question 14 in the European Commission's FAQ.

insufficient to classify the employee as a user within the meaning of the regulation. An organization can be both a user and a data holder within the meaning of the Data Act, with respect to different connected products or related services. For example, a factory can be a user of manufacturing robots and a data holder for the products it makes with them. A party cannot be both the user and the data holder of the same data at the same time.

37. **Data holder**:[40] A person or organization that, often by contract,[41] has the right or obligation to use or make available data from a connected product or related service. Data holders are typically entities that are involved in the design of the data collection, have control over the storage and distribution of the data, and have a legal (contractual) relationship with the user by receiving the data directly from the connected product or related service. This is often the manufacturer of the connected product or an organization offering a related service, but it can also be another party. However, the regulation also allows manufacturers to contractually transfer the role of data holder to another party.[42] In addition, a product or service may have multiple data holders, such as when the data from a component of a product is also made available by the manufacturer to the supplier of that component. In such cases, both parties are data holders for the data from the component. Not every connected product has a data holder. A connected product may also make data available only to the user, for instance, if the data is stored exclusively on the product itself.[43]

38. **Data recipient**:[44] A person or organization that receives data from the data holder, acts for professional, non-private purposes, and is not a user within the meaning of the Data Act. This could be an organization that uses the data it receives to develop a related service, conduct scientific research or provide consulting services.

39. **Third party**: This term is not defined in the Data Act. ACM defines a third party as a person or organization that has permission from the user to access data. In most cases, a third party will also be a data recipient within the meaning of the regulation. Examples of third parties include service providers, such as maintenance engineers for smart thermostats, energy consultants and research institutions.

40. **Data subject**:[45] A data subject as referred to in Article 4(1) of the GDPR. This must be an identified or identifiable natural person. An identifiable person is considered to be a natural person who can be identified, directly or indirectly, in particular by means of an identifier such as a name, identification number, location data, online identifier or one or more elements that are unique to their physical, physiological, genetic, psychological, economic, cultural or social identity.[46]

41. **Seller**: This term is not defined in the Data Act. ACM's definition aligns with consumer law: a person or organization acting for the purposes of their trade, business, craft or profession.[47] This definition also applies to **lessors** and **rentors**.

[40] Article 2(13) of the Data Act.
[41] See also question 21 in the European Commission's FAQ.
[42] See also question 21 in the European Commission's FAQ.
[43] See also question 21 in the European Commission's FAQ.
[44] Article 2(14) of the Data Act.
[45] Article 2(11) of the Data Act.
[46] Article 4(1) of the GDPR.
[47] Article 2(3) Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC and Article 2, paragraph 2 of Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council, and repealing Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (EU Consumer Sales Directive).

42. **Holder of a trade secret**:[48] A person or organization that possesses trade secrets.[49] In the context of the Data Act, this could include access to algorithms used for data analysis or machine learning, as well as systems that predict maintenance needs based on sensor data.

2.5 Key terms

43. A number of key devices, applications and types of data discussed in the Data Act are defined below.

2.5.1 Smart devices and services

44. **Connected product**:[50] A connected product is a good that obtains, generates or collects data about its use or environment, often through internal measuring instruments or sensors. The product can transmit this data via an electronic communications service (such as the internet),[51] a cable or the device itself.[52] Connected products are also known as smart or connected devices. A connected product is not necessarily a product that is continuously connected; a product that shares data on an ad hoc basis, for instance during maintenance, can also be considered a connected product.[53] Examples of connected products include smartphones, desktop computers and laptops, digital cameras, smart thermostats, smart home appliances, vehicles, medical equipment and industrial machinery.[54] Such products do not qualify as connected products within the meaning of the Data Act if their main function is to store, process or transmit data for a party other than the user.[55] For example, a server may be considered a connected product if it stores, processes or transmits data for the user themself, but not if it does so on behalf of a third party.[56] Prototypes of connected products are also exempt from the rules in the Data Act because the production phase has not yet been completed.[57]

45. **Related service**:[58] A related service is a digital service tied to a connected product that can affect the functionality, behavior or operation of the connected product.[59] This could be an app that allows users to control the temperature in their homes, or software that optimizes the performance of a connected product. Related services can exchange data bidirectionally between connected products and service providers. A digital service that sends data unidirectionally is not a related service within the meaning of the Data Act.[60] Electronic communications services[61] and supporting digital services, such as maintenance and analysis services, are also not included in the Data Act's definition of a related service.[62] This is because unidirectional and supporting services do not affect the operation of the connected product and do not transmit data or commands bidirectionally.[63]

[48] Article 2(19) of the Data Act. This refers to Article 2(2) of Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive).
[49] A trade secret as defined in Article 2(1) of the Trade Secrets Directive.
[50] Article 2(5) of the Data Act.
[51] Recital 14 of the Data Act.
[52] See also questions 7 and 8 in the European Commission's FAQ.
[53] See also question 7 in the European Commission's FAQ.
[54] Recital 14 of the Data Act. See also question 7 in the European Commission's FAQ.
[55] Recital 16 of the Data Act.
[56] See also question 7 in the European Commission's FAQ.
[57] Recital 14 of the Data Act. See also question 7 in the European Commission's FAQ.
[58] Article 2(6) of the Data Act.
[59] See also question 10 in the European Commission's FAQ and Section 13 of the European Commission's Vehicle Data Guidance.
[60] Unidirectional means that data is transmitted or flows in only one direction, from sender to receiver. The opposite is bidirectional data exchange, where data is transmitted or flows in both directions. See also recital 17 of the Data Act, question 10 in the European Commission's FAQ and Section 15 of the European Commission's Vehicle Data Guidance.
[61] Article 2(6) of the Data Act. See also Section 13 of the European Commission's Vehicle Data Guidance.
[62] Recital 17 of the Data Act. See also Section 16 of the European Commission's Vehicle Data Guidance.
[63] *Ibid.*

Table 1: Examples of related and unrelated services

Examples of related services	Examples of services that, in principle, are *not* related services
Remote control functions, such as: • an app used to remotely lock or unlock doors • an app used to pre-heat a vehicle[64]	An app that displays an electric vehicle's charging history without sending control commands[65]
Special maintenance services involving bidirectional data traffic that add to or modify the vehicle's functionalities[66]	A pay-how-you-drive insurance service that analyzes driving behavior data to create a personalized driving profile[67]
Dynamic route optimization services that use vehicle data (such as battery or gas level) to suggest routes and charging or refueling stops on a vehicle's dashboard display[68]	Traditional aftermarket services, such as consulting, analysis, financial services and manual maintenance, such as brake replacements and oil changes[69]

46. **Virtual assistant**:[70] A virtual assistant is typically a related service. It is software that can process commands, tasks or queries, and use these to access other services or control a connected product. An example of a virtual assistant is the onboard computer in a car that can send text messages via voice command, through a smartphone. A virtual assistant can also be used to control a thermostat, for example.

2.5.2 Data

47. **Data**:[71] Any digital representation of actions, facts or information and any compilation of such actions, facts or information, including audio, visual and audiovisual recordings.

48. **Personal data**:[72] Personal data as defined in Article 4(1) of the GDPR. This includes any information that can, directly or indirectly, identify a natural person, such as their name, location data or IP address.

49. **Special personal data**: Personal data within the meaning of Article 9(1) of the GDPR. Special personal data is information that is so privacy-sensitive that it could have a significant impact on someone if it were processed. Examples of special personal data include data about a person's race or ethnic origin, biometric and genetic data, and data about a person's health and sexual orientation.

50. **Non-personal data**:[73] Data that does not relate to an identified or identifiable natural person. This includes all data other than personal data.

51. **Trade secrets**:[74] Information that is not publicly available or easily accessible, has commercial value due to its secret nature, and is therefore protected from unauthorized access.

[64] See also Section 17 of the European Commission's Vehicle Data Guidance.
[65] See also Section 15 of the European Commission's Vehicle Data Guidance.
[66] *Ibid.*
[67] *Ibid.*
[68] *Ibid.*
[69] See also Section 16 of the European Commission's Vehicle Data Guidance.
[70] Article 2(31) of the Data Act. See also recital 23 of the Data Act.
[71] Article 2(1) of the Data Act.
[72] Article 2(3) of the Data Act.
[73] Article 2(4) of the Data Act.
[74] Article 2(18) of the Data Act. These are trade secrets as defined in Article 2(1) of the Trade Secrets Directive.

52. **User data**: Data generated by the use of the connected product or related service. This is data resulting from interactions between the user or someone in their vicinity and a connected product or related service. It includes both actively and passively recorded data. It also includes data generated during periods of inactivity, such as when the product is on standby, charging, performing automatic tasks or turned off completely.[75] User data can be divided into three types:
    - **Product data**:[76] This is data that is collected directly by the connected product through its use, its performance or the environment in which it is located. It can be retrieved by the user, the data holder or a third party, or, where appropriate, by the manufacturer, via an electronic communications service (such as the internet),[77] a cable or the device itself, because the manufacturer has designed the connected product to facilitate this.[78] Product data includes both **raw data and pre-processed data** retrieved from the product.[79] Descriptive data about the product, instruction manuals and packaging information *does not* qualify as product data.[80]
    - **Data collected by a related service**:[81] This is data generated during the provision of the related service, as a result of a deliberate user action or as a by-product thereof, and which is related to the connected product.[82] This can be either **raw data** or **pre-processed data**.
    - **Metadata**:[83] These are structured descriptions that make it easier to find or use data by providing insight into its content or usage. A frequently used term within the context of the Data Act is **relevant metadata**.[84] This is metadata that is needed to interpret and use the data, such as basic context and timestamps. It also includes other relevant information that is necessary to understand the circumstances under which the data was collected or generated, such as data format, resolution, delay, sensitivity and location.[85] Other additional information, such as error code tables, may also be viewed as metadata, as long as it is useful for correctly interpreting the data.[86]

53. **Raw data**: Also known as source or primary data, this includes **product data** and **data collected by a related service**. Raw data is unprocessed, automatically generated data,[87] such as data generated as a result of user actions (involving controls, screens or buttons) or data automatically generated by vehicle sensors.[88]

54. **Pre-processed data**: This is data that has been processed for the purpose of making it understandable and usable before further processing and analysis.[89] Like raw data, pre-processed data falls under the **product data** category or the **data collected by a related service** category. With pre-processed data, the nature of the underlying data remains unchanged by the processing.[90] In other words, the data still reflect real events or conditions, even if it has been normalized, restructured, filtered, calibrated, converted, merged, corrected or otherwise measured, calculated or processed.[91] The Data Act takes a functional approach to data processing: the function is to make the data understandable and usable.[92] Factors such as the complexity of the processing or the need to protect investments in the processing do not play a role in the definition of pre-processed data.[93] A

[75] Recital 15 of the Data Act.
[76] Article 2(15) of the Data Act.
[77] Recital 14 of the Data Act. See also question 4 in the European Commission's FAQ.
[78] Recital 15 of the Data Act.
[79] Recital 15 of the Data Act.
[80] See also question 4 in the European Commission's FAQ.
[81] Article 2(16) of the Data Act.
[82] Recitals 15 and 17 of the Data Act. See also question 4 in the European Commission's FAQ.
[83] Article 2(2) of the Data Act.
[84] Articles 3(1), 4(1) and 5(1) of the Data Act.
[85] Recital 15 of the Data Act. See also question 5 in the European Commission's FAQ.
[86] Recital 15 of the Data Act defines this as follows: "combined with other data, such as data sorted and classified with other data points relating to them, or re-formatted into a commonly used format."
[87] See also Section 24 of the European Commission's Vehicle Data Guidance.
[88] See also question 4 in the European Commission's FAQ and Sections 24 and 33 of the European Commission's Vehicle Data Guidance.
[89] Recital 15 of the Data Act. See also Section 25 of the European Commission's Vehicle Data Guidance.
[90] Recital 15 of the Data Act. See also question 4 in the European Commission's FAQ.
[91] Recital 15 of the Data Act. See also Section 34 of the European Commission's Vehicle Data Guidance.
[92] See also Section 25 of the European Commission's Vehicle Data Guidance.
[93] See also Section 26 of the European Commission's Vehicle Data Guidance.

good example of product data that usually falls under the definition of pre-processed data are calculations of averages such as fuel consumption per hour, or speed in kilometers per hour.[94] Other examples include GPS location data and data collected from a connected group of sensors, with the goal of making it understandable for broader use cases by determining a physical quantity or quality.[95]

55. **Readily available data**:[96] This is **product data** and **data collected by a related service** that is, or can be, easily and lawfully obtained by the data holder, without disproportionate effort beyond a simple action.[97] This includes data that the data holder can obtain because of how the product is designed, or because of the agreement with the user to provide a related service.[98] Simple actions include maintaining, performing diagnostics on, updating or repairing a connected product or related service. The timing of data generation or collection does not determine whether the data can be considered readily available. Data that is anonymized or encrypted also falls under the definition of readily available data, as long as there are reasonable means to link the data to a specific user or connected product without substantial system modifications or costs.[99] Readily available data does not include data that is generated through the use of a connected product whose design does not allow the data to be stored or transmitted beyond the component in which it is generated, or beyond the connected product as a whole.[100]

56. **Derived data**: This is data beyond raw or pre-processed data, resulting from additional investment in linking values or insights to raw or pre-processed data.[101] This is primarily done through proprietary complex algorithms, including algorithms that are part of proprietary software.[102] Thus, the concept of derived data goes beyond technical aspects or combinations thereof.[103] The nature of the information in a data point is the defining difference. Through additional investment in existing data, derived data creates new information or insights beyond the original meaning of the data.[104] While it is important that derived data is the result of processing with some complexity and ingenuity,[105] it is not the complexity of the processing that makes data "derived" within the meaning of the regulation, but rather the new valuable insights the data represents.[106] For this reason, predictions of future events, values or conditions also generally fall within the definition of derived data, provided that they are produced through a complex interpretive process.[107]

57. Table 2 uses the functionalities of a smart thermostat as an example to clarify the distinctions between the different types of data.[108]

Table 2: Examples of the types of data collected by a smart thermostat

Type of data	Recorded data

[94] See also Sections 29 and 34 of the European Commission's Vehicle Data Guidance.
[95] Recital 15 of the Data Act. See also Section 25 of the European Commission's Vehicle Data Guidance.
[96] Article 2(17) of the Data Act.
[97] See also Section 38 of the European Commission's Vehicle Data Guidance.
[98] Recital 15 of the Data Act. See also Section 40 of the European Commission's Vehicle Data Guidance.
[99] See also question 13a in the European Commission's FAQ.
[100] Recital 20 of the Data Act. This also means that the Data Act should not be viewed as an obligation to store data on the central processing unit of a connected product. See also question 5a in the European Commission's FAQ and Sections 45 and 76 of the European Commission's Vehicle Data Guidance.
[101] Recital 15 of the Data Act. See also Section 27 of the European Commission's Vehicle Data Guidance.
[102] *Ibid.*
[103] See also Section 31 of the European Commission's Vehicle Data Guidance. Examples of combinations that do not provide entirely new information include linking satellite navigation data (GNSS) with other vehicle data for location-based information, adding a timestamp to a data point, or determining location more accurately by matching GNSS sensor data with maps.
[104] Recital 15 of the Data Act. See also Sections 28 and 31 of the European Commission's Vehicle Data Guidance.
[105] Basic operations such as addition, subtraction, multiplication, division and averaging do not result in derived data. The type of data this produces would be more appropriately categorized as pre-processed data. The application of anonymization and pseudonymization techniques does not result in derived data either. For more information, see also questions 5 and 13 in the European Commission's FAQ and Section 29 of the European Commission's Vehicle Data Guidance.
[106] See also Section 28 of the European Commission's Vehicle Data Guidance.
[107] See also Section 32 of the European Commission's Vehicle Data Guidance.
[108] The examples in Table 1 are provided for illustrative purposes. The precise categorization of data will depend on the circumstances of individual cases. For more examples regarding data from vehicles, see also Sections 33 through 35 of the European Commission's Vehicle Data Guidance.

Personal data	• Name of user • Street name, house number and town/city • IP address of the home network
Non-personal data	• Average monthly temperature • Thermostat temperature history logs
(Potential) trade secrets	• Data from an algorithm that learns when residents are home and automatically optimizes the heating schedule
Product data	• Current room temperature: 21.5 °C • Humidity: 45%
Data collected by a related service	• Energy consumption: 4.0 kWh today • Heating status: Off • Schedule setting: Turn heating on at 18:00 • Pairing status with app, e.g. “Connected to user’s smartphone”
Metadata	• Thermostat location: Living room • Time of measurement: March 10, 2025, 14:05 • Product ID: THRM-2025-XYZ123 • Firmware version of the product: 3.2.1 • Software version: 09.2.1 • Wi-Fi signal strength: 78%
Raw data	• Current room temperature: 21.5 °C • Humidity: 45%
Pre-processed data	• Average temperature today: 22 °C • Energy consumption February: 350 kWh
Readily available data	• Current room temperature: 21.5 °C • Energy consumption: 4.0 kWh today • Thermostat location: Living room • Average temperature today: 22 °C
Derived data	• Personalized scheme recommendation for maximum energy savings based on household energy usage • Outcomes of thermostat data analysis for predictive maintenance

2.6 Relationship with GDPR

58. Using a connected product and a related service may result in the processing of personal data, such as the user’s IP address. The GDPR remains fully applicable to all processing of personal data within the scope of the Data Act.[109] This also applies to mixed data sets.[110] In some cases, the Data Act complements the GDPR, for example with provisions on the portability of personal data collected by connected products, or by placing restrictions on the reuse of personal data by third parties.[111]

[109] Article 1(5) of the Data Act.
[110] Recital 34 of the Data Act.
[111] Article 1(5) of the Data Act. See also recitals 34 and 35 of the Data Act and question 18 in the European Commission’s FAQ.

59. The applicability of the GDPR means that the controller must comply with the obligations it imposes.[112] Thus, in addition to complying with the Data Act, the controller must always adhere to the requirements of the GDPR when processing personal data.[113] In the event of a conflict between these two regulations, the GDPR takes precedence.[114] The Data Act therefore does not affect the GDPR: data sharing obligations do not relieve controllers of their obligations under the GDPR when sharing personal data. Nor does the Data Act affect the existing GDPR rights of data subjects, such as the right to data portability (Article 20 of the GDPR) and the right of access (Article 15 of the GDPR).[115]

60. The Data Act recognizes the power of data protection authorities (such as the DPA in the Netherlands) to enforce compliance with the GDPR. It also provides for a coherent enforcement and cooperation mechanism between these authorities and other competent bodies.[116] Thus, data protection authorities are also empowered within the framework of the Data Act to regulate the processing of personal data. This ensures that data subjects do not have to turn to multiple agencies in the event of a dispute about their personal data.[117] The partnership between ACM and the DPA is anchored in the Data Act Implementation Act[118] and has been formalized in a cooperation protocol.[119] This protocol will include future agreements specifically aimed at Data Act oversight. Finally, ACM and the DPA also plan to publish a document on the relationship between the Data Act and the GDPR later this year.

2.7 Relationship with other legislation

61. The Data Act contains horizontal rules and has a broad scope of application. As it is relevant in the context both of business-to-business and business-to-consumer relationships, the regulation interacts with several other European and national laws. Discussing the Data Act's concurrence with all this legislation would exceed the scope of these guidelines. For a comprehensive analysis, please refer to the Explanatory Memorandum on the Data Act Implementation Act.[120]

62. The regulation contains general rules and explicitly states that it does not affect or supplement European law in areas such as intellectual property law,[121] consumer law[122] and contract law.[123] It also does not affect European law regarding physical design and data requirements, unless the regulation explicitly provides for this.[124]

63. There is substantial overlap between the Data Act and consumer law, which is fundamental to protecting consumers who purchase and use smart devices and related services. For example,

[112] The term "controller" is defined in Article 2(7) of the GDPR. A controller is a natural or legal person, government agency, service or other entity that determines the purposes and means of processing personal data, either alone or in collaboration with others.
[113] Recital 22 of the Data Act does make it clear that a processor as defined in the GDPR is not supposed to act as a data holder.
[114] Article 1(5) of the Data Act. In addition, Article 1(5) and recital 36 of the Data Act refer to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[115] Recitals 31 and 35 of the Data Act.
[116] The European Commission encourages cooperation among enforcement agencies through, among other things, the European Data Innovation Board (EDIB), whose members include the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB).
[117] The term "data subject" is defined in Article 4(1) of the GDPR. A data subject is an identifiable natural person. An identifiable person is considered to be a natural person who can be identified, directly or indirectly, in particular by means of an identifier such as a name, identification number, location data, online identifier or one or more elements that are unique to their physical, physiological, genetic, psychological, economic, cultural or social identity.
[118] Article 6 of the Data Act Implementation Act.
[119] Cooperation protocol for the Netherlands Authority for Consumers and Markets and the Dutch Data Protection Authority, Government Gazette 2025, 3534.
[120] Section 5, Explanatory Memorandum (Data Act Implementation Act), Parliamentary Paper 36733, No. 3.
[121] Article 1(8) of the Data Act. See also recital 13 of the Data Act.
[122] Article 1(9) of the Data Act. See also recital 9 of the Data Act.
[123] Article 1(10) of the Data Act. See also recital 9 of the Data Act.
[124] Recital 11 of the Data Act.

consumer law imposes extensive disclosure obligations on traders.[125] These obligations complement the transparency and access requirements laid down in the Data Act. In addition, consumer law covers topics such as fair contractual terms, protection against deceptive trade practices, and the prohibition of "dark patterns" (misleading design choices that manipulate users into performing or avoiding certain actions).[126] The Data Act and consumer law should therefore be applied in conjunction.

64. The regulation does not preclude additional requirements from being established in European law based on the needs of specific sectors. Such sectoral requirements must be consistent with the Data Act.

65. Sector-specific requirements may include technical requirements for data access, or restrictions on or extensions of the right to access or use certain data, such as the security requirements described in the NIS2 Directive[127] and in Annex I of the Cyber Resilience Act.[128] Sectoral product regulations, such as the Machinery Regulation[129] and the Medical Device Regulation,[130] may impose requirements for processing or securing data as well. There is also other sector-specific legislation related to data sharing that falls within the scope of the Data Act, such as the PSD2 Directive,[131] the Motor Vehicle Regulation[132] and the Electricity Directive.[133]

66. Since the Data Act does not affect European law, regulators of other European legislation, or national legislation derived from it, retain jurisdiction over the respective provisions of this legislation. This means that multiple regulators may have authority to oversee the same connected product or related service, with each regulator focusing on a different aspect. For example, ACM can enforce consumer law and the Data Act, the DPA can enforce the personal data component, and the Dutch Authority for Digital Infrastructure (RDI), the Health and Youth Care Inspectorate (IGJ) or the Netherlands Food and Consumer Product Safety Authority (NVWA) can enforce product safety. ACM strives to coordinate its enforcement with other regulators as much as possible, for example through the Digital Regulation Cooperation Platform (SDT).[134]

[125] See also ACM, *Consumenten informeren*, available at https://www.acm.nl/nl/verkoop-aan-consumenten/consumenten-informeren (Dutch only).
[126] Recital 38 of the Data Act, the DSA Guidelines and ACM's Guidelines on the protection of the online consumer provide more information on dark patterns. For the DSA Guidelines, see ACM, *Guidelines on the Digital Services Act (DSA) for providers of online services*, available at https://www.acm.nl/en/publications/guidelines-digital-services-act-dsa-providers-online-services. For the Guidelines on the protection of the online consumer, see ACM, *Guidelines on the protection of the online consumer*, available at https://www.acm.nl/en/publications/guidelines-protection-online-consumer.
[127] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
[128] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).
[129] Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC.
[130] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.
[131] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
[132] Regulation (EU) 2024/1257 of the European Parliament and of the Council of 24 April 2024 on type-approval of motor vehicles and engines and of systems, components and separate technical units intended for such vehicles, with respect to their emissions and battery durability (Euro 7), amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 715/2007 and (EC) No 595/2009 of the European Parliament and of the Council, Commission Regulation (EU) No 582/2011, Commission Regulation (EU) 2017/1151, Commission Regulation (EU) 2017/2400 and Commission Implementing Regulation (EU) 2022/1362.
[133] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast).
[134] For more information on how ACM works together with other regulators, see also ACM, *National cooperation*, available at https://www.acm.nl/en/about-acm/organization/cooperation/national-cooperation.

3 Disclosure obligations

3.1 Introduction

65. This section discusses the disclosure obligations arising from the Data Act. First, Subsection 3.2 explains exactly what these obligations entail and the situations to which they apply. Next, Subsection 3.3 sets out the kinds of information that must be provided with respect to connected products. Finally, Subsection 3.4 examines what data must be disclosed when providing a related service.

3.2 What do the disclosure obligations entail?

66. Before entering into an agreement to purchase, rent or lease a connected product, or to provide a related service, the user should receive certain information regarding the access and use of data. This is known as the "transparency obligation."[135] With a connected product, the seller, rentor or lessor of the product is required to provide this information;[136] in some cases, this may be the manufacturer itself. With a related service, this obligation, in principle, rests with the provider of the service.[137]

67. The information must be provided before entering into the agreement. This allows the user to make an informed decision to purchase, rent or lease the connected product.[138] The same applies to related services. The information must be provided before the user enters into the agreement. The obligation to provide information before entering into an agreement to provide a related service is separate from the obligation to provide information for the purchase, rental or lease of a related product.[139] Thus, if the related service is provided at a different time than when the associated connected product is purchased, rented or leased, the information may be provided at a different time.

68. If any information changes during the lifetime of the connected product or the contract period of the related service, the updated information must be provided to the user.[140]

69. The information should be provided in a clear and understandable manner. This means that the information must be specific, detailed and unambiguous. It is also important that the information be provided in a language that most Dutch users can understand. Depending on the product, this will usually be Dutch or English.

70. The information can be provided through the terms and conditions of the product or service, a link to the information on a website, a physical or digital manual, or a QR code accompanying the product or service and referring to the relevant information. Users must have the ability to store the information so that it remains accessible for future viewing, reference and reproduction in unaltered form.[141] The type of information that must be provided will depend on whether it pertains to a connected product or a related service. This is explained in the following subsections.

3.3 Information to be provided about connected products

71. The table below shows what information must be provided to users who purchase, rent or lease a connected product. As in Table 2 above, the examples provided here pertain to a smart thermostat.

[135] This obligation is stipulated in Articles 3(2) and 3(3) of the Data Act. See also recital 24 of the Data Act and question 17 in the European Commission's FAQ.
[136] Article 3(2) of the Data Act.
[137] Article 3(3) of the Data Act.
[138] In addition, the obligation to provide information under the Data Act is without prejudice to the obligation of the data controller to provide information to the data subject in accordance with Articles 12, 13 and 14 of the GDPR. See also recital 24 of the Data Act.
[139] Recital 24 of the Data Act.
[140] *Ibid.*
[141] *Ibid.*

Table 3: Overview of information to be provided about a connected product

Mandatory information	Explanation	Smart thermostat examples
Type of product data[142]	The type of product data generated by the product	Temperature measurements, on/off status, times of interactions with product
Format of product data[143]	Information about the structure or format in which product data is recorded	Data structures, data formats and vocabularies, classification schemes, taxonomies, code lists JSON, XML, CSV, Dublin Core, SKOS, Schema.org, DCAT, etc.
Estimated volume of product data[144]	The estimated amount of product data generated	10 MB on daily energy consumption and 2 MB on user settings
Ability to generate data continuously and in real time[145]	Whether the connected product can generate data continuously (without interruption) and in real time (immediately)	Generation occurs every minute, every hour or when the temperature settings are changed
Ability to store data and retention period[146]	Whether the connected product can store data locally or remotely, and how long data is stored	Storage: Locally, in the cloud (e.g. in data centers in the EU or a third country) Retention period: 1 year, 6 months, until the user deletes the data
Ability to access, retrieve or delete data[147, *a]	How the user can access, retrieve or delete the data	In the product's settings, the user can access and view the generated data, and use it independently or share it
Identity of the data holder for the ability to access, retrieve or delete data[*b]	The identity of the responsible data holder that can enable the user to access, retrieve or delete data (e.g. trade name and address)	Warmte IQ B.V., 123 Example Street, 1234 AB Example City

Re (a): This includes information on the technical resources required to access or delete data, such as an API or software development kit. Terms of use and information on the quality of these resources must also be provided.[148]

Re (b): Unlike the disclosure requirements for related services, this element is not explicitly included in the Data Act itself. Before signing a purchase, rental or lease contract for a connected product, users should be informed about how to access, retrieve and delete their data. Unlike with related services, this does not require identification of all data holders for different product components, unless this is strictly necessary for the exercise of the user's rights. It is sufficient that there is a responsible data holder that grants access to the data, as required by the Data Act. If this access does not meet the requirements of the regulation, the responsible data holder must identify additional data holders to which the user can submit access requests.

[142] Article 3(2)(a) of the Data Act.
[143] *Ibid.*
[144] *Ibid.*
[145] Article 3(2)(b) of the Data Act.
[146] Article 3(2)(c) of the Data Act.
[147] Article 3(2)(d) of the Data Act.
[148] Recital 24 of the Data Act.

3.4 Information to be provided about related services

72. The table below shows what information must be provided to users of related services. As in Tables 2 and 3 above, the examples provided here pertain to a smart thermostat.

Table 4: Overview of information to be provided about a related service

Mandatory information	Explanation	Smart thermostat examples
Type of product data collected by data holder[149, *a]	The type of product data assumed to be obtained by the potential data holder	Daily energy consumption, outdoor versus indoor temperature, user settings, manual adjustments
Estimated volume of product data collected by data holder[150, *a]	The estimated amount of product data assumed to be obtained by the potential data holder	10 MB on daily energy consumption and 2 MB on user settings
Frequency of collection of product data by data holder[151, *a]	The amount of product data collected over a period of time, which the potential data holder is assumed to obtain	Collection occurs every minute, every hour or when the temperature settings are changed
Type of data generated by related service[152, *a]	The type of data generated by a related service	Analysis of heating patterns, heating schedules
Estimated volume of data generated by related service[153, *a]	The estimated amount of data generated by a related service	100 MB on heating pattern analyses
Expected use of readily available data by data holder[154]	Whether the potential data holder expects to use readily available data, and for what purposes	The manufacturer uses the data to improve the energy saving algorithm
Expected use of readily available data by third parties[155]	Whether the potential data holder expects to allow third parties to use the readily available data for purposes agreed with the user	Data is also shared with an energy supplier if the user has given permission to do so
Identity of data holder and other data processing parties[156]	The identity of the potential data holder and any other parties processing the data (e.g. trade names and addresses of all entities involved in data processing)	Warmte IQ B.V., 123 Example Street, 1234 AB Example City
Fast and efficient means of communication[157]	The means of communication by which the user can quickly and efficiently contact the potential data holder	Customer service available via email, phone and live chat on weekdays from 8:00 to 18:00
Way for the user to initiate or stop data sharing with third parties[158]	How the user can initiate or stop sharing data with a third party	The app's settings include an option to enable or disable data sharing; the user can revoke their permission to

[149] Article 3(3)(a) of the Data Act.
[150] *Ibid.*
[151] *Ibid.*
[152] Article 3(3)(b) of the Data Act.
[153] *Ibid.*
[154] Article 3(3)(c) of the Data Act.
[155] *Ibid.*
[156] Article 3(3)(d) of the Data Act.
[157] Article 3(3)(e) of the Data Act.
[158] Article 3(3)(f) of the Data Act.

		share their data with third parties for reuse at any time
Right to file a complaint with the competent authority[159]	The user can file a complaint with ACM if they suspect that their rights under the Data Act are being abused or violated	Disclaimer informing the user of their rights
Data on trade secrets and their holders[160, *b]	Whether a potential data holder holds a trade secret that is part of the data accessible through the connected product or related service	Collected algorithmic analysis contains company-sensitive information; holder is Warmte IQ B.V.
Duration of the agreement and termination provisions[161]	The duration of the agreement between the user and the potential data holder and provisions for terminating the agreement	Contract continues until user deactivates account; upon termination of the contract, data will be deleted within 30 days, unless otherwise required by law

Re (a): This includes methods that allow the user to access or retrieve this data. The potential data holder's data storage methods and retention period should also be disclosed.[162]

Re (b): If a party other than the potential data holder is the holder of a trade secret within the meaning of this requirement, their identity must be disclosed.[163]

[159] Article 3(3)(g) of the Data Act.
[160] Article 3(3)(h) of the Data Act.
[161] Article 3(3)(i) of the Data Act.
[162] Article 3(3)(b) of the Data Act.
[163] Article 3(3)(h) of the Data Act.

4 Access to data collected by a connected product or related service

4.1 Introduction

73. The Data Act stipulates that users must have access to the data generated as a result of the use of connected products or related services. This section provides a systematic overview of the rules on such access.

74. Subsection 4.2 begins with a discussion of the distinction between the two types of data access: direct and indirect access. This includes an explanation of when which type applies. Next, Subsections 4.3 and 4.4 examine direct and indirect access in more detail, distinguishing between access requests by the user themselves and by third parties. The scope of the obligation and the requirements for verifying the identity of individuals requesting data access are discussed as well. Following this, Subsection 4.5 explains exactly what data may fall under the obligation to provide access. Subsection 4.6 discusses the mode of access provision itself and the quality requirements imposed by the regulation on the mode of access provision, for both direct and indirect access. Subsection 4.7 then sets out the grounds for exception to the obligation to provide access, such as security risks and trade secrets. Finally, Subsection 4.8 examines legal protection through dispute resolution in greater detail.

4.2 Direct and indirect access provision

75. This section focuses on data access. In general, it is up to the manufacturer or data holder to ensure that data is made available. There are two ways to provide this access: the manufacturer or data holder can give the user access to the data either directly or indirectly.[164]

76. With direct access, the manufacturer must design the product so that the data can be accessed directly by the user without the intervention of any other party (including the data holder).[165] ACM calls this the **access-by-design obligation**.[166]

77. Where **relevant** and **technically feasible**, the data should be directly accessible to users.[167]

78. **Technically feasible** means that it is technically possible to provide access. This means that the necessary technology, resources and knowledge are available to develop and implement the product in a way that enables direct access. Access may not be technically feasible for the manufacturer if:
    1. the required technical modifications would be too costly;
    2. the security of trade secrets or intellectual property rights would be compromised; or
    3. the security of the connected product or related service cannot be adequately guaranteed.[168]

    Feasibility should be assessed objectively, based on industry standards, best practices and the current state of the art.[169]

[164] Articles 3(1) and 4(1) of the Data Act describe this as direct access. See also Section 36 of the European Commission's Vehicle Data Guidance.
[165] Article 3(1) of the Data Act. See also question 22 in the European Commission's FAQ.
[166] Articles 3(1) and 4(1) of the Data Act describe this as direct access. See also Section 36 of the European Commission's Vehicle Data Guidance.
[167] Article 3(1) of the Data Act. See also Section 37 of the European Commission's Vehicle Data Guidance. For more information on the distinction between direct and indirect access, see question 22 in the European Commission's FAQ.
[168] See also question 22 in the European Commission's FAQ.
[169] See also question 22a in the European Commission's FAQ. The term "state of the art" is often used to refer to the most advanced and widely accepted technologies, methods or practices within a specific field at any given time. In the context of products and systems, the term refers to the most widely available and commonly used technologies currently viewed as the standard.

79. **Relevant** means that the manufacturer may take into account the specific contexts and characteristics of different connected products or related services.[170] The manufacturer can also consider the user's perspective. In short, there will be situations in which providing direct access to data collected by a connected product or related service is illogical, inappropriate or unfeasible.[171] This may be the case, for example, if doing so would require excessive technical effort, or if the design of the product in question does not allow for direct access without major modifications. In these situations, the data holder must provide **indirect access** immediately upon request.[172]

80. Indirect access means that users cannot obtain the data directly from the product or a website. Instead, they must submit a request to the data holder. The data holder must then take action to immediately make the requested data available, in an understandable format. In other words, if a user does not have direct access, the data holder is obliged to provide the data to the user upon request.[173] ACM calls this **indirect access upon request**.

81. Indirect access upon request includes the ability for a user (or party acting on behalf of a user) to request that the data holder allow a third party, such as a consulting firm, to access the data.[174] Thus, the ability of a third party to gain indirect access to data at the user's request does not depend on the type of access the user has themselves.[175] This means that it should always be possible for the user to have the data shared with a third party, regardless of whether the user themselves has direct or indirect access to the data.

82. It is up to the manufacturer to make a well-considered decision on whether direct or indirect data access is most appropriate for a particular product. In its FAQ, the European Commission notes that the Data Act provides some flexibility in this regard by allowing manufacturers – where relevant and technically feasible – to decide whether or not to design for direct or indirect access. The Data Act encourages data holders to implement solutions that best suit their needs when complying with the obligation to make data available to users.[176]

83. Regarding the data retention period, the regulation states that data holders cannot be expected to retain data indefinitely.[177] The Data Act does require data holders to have a reasonable retention policy, consistent with the storage limitation principle of the GDPR where applicable.

84. The choice between direct and indirect access affects the conditions that access must meet, as there are different obligations for each type of access. These obligations and other requirements on the provision of access are explained in the next two subsections. The relationship between these two types of access and the associated process is shown schematically below.

[170] See also question 17 in the European Commission's FAQ.
[171] See also question 22 in the European Commission's FAQ.
[172] Article 4(1) of the Data Act.
[173] *Ibid.*
[174] See also Section 38 of the European Commission's Vehicle Data Guidance.
[175] See how Article 5(1) of the Data Act is worded. See also question 31 in the European Commission's FAQ and Section 38 of the European Commission's Vehicle Data Guidance.
[176] See also questions 17, 22 and 22a in the European Commission's FAQ and Sections 37 and 78 of the European Commission's Vehicle Data Guidance.
[177] Recital 24 of the Data Act.

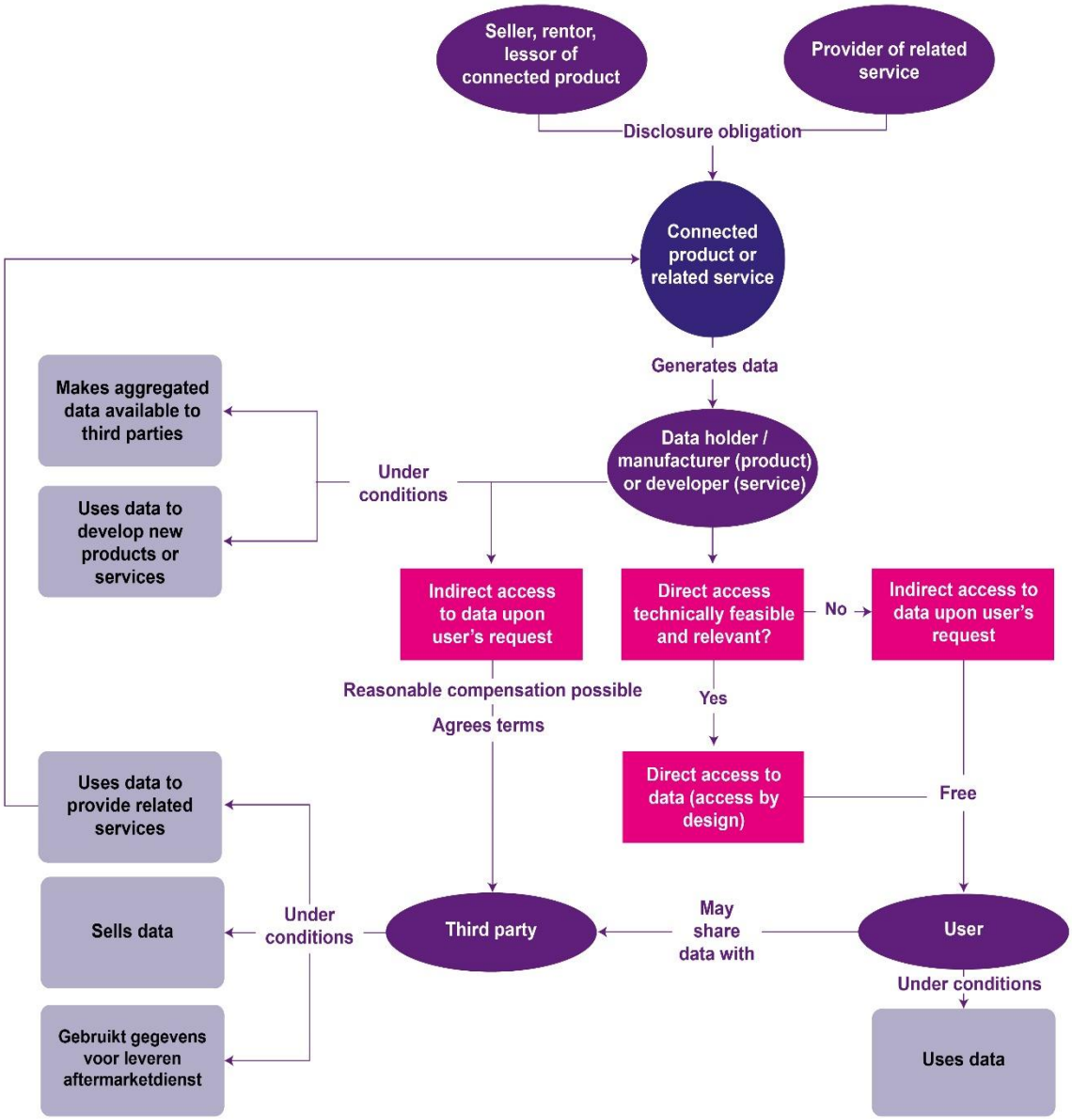


Figure 1: Schematic representation of direct and indirect access (this figure is based on the figure from the European Commission's FAQ and shows all the steps explained in this section)

4.3 Direct access to data (access by design)

4.3.1 What do the disclosure obligations entail?

86. The connected product and related service should be designed or made so that product data, data from a related service and associated metadata are directly accessible to the user, where relevant and technically feasible.[178] ACM calls this the **access-by-design obligation**.

87. Users have direct access if:
    1. they are able to export the data from the connected product without the intervention of another party; and
    2. they have the technical means to export the data from the connected product as a consequence of its design and manufacturing process, regardless of whether the data is stored on the connected product itself or on an external server.[179]

88. With direct access, the user can access the data independently, for example by streaming or downloading it, without having to contact the data holder. This can be done through a device, interface or API. Even when a login is required, there is still direct access if the user can access the data independently after logging in, without having to request it from the data holder.[180] An example of direct access is a situation where a connected product has a digital interface, where the user has control over the access mechanism, manages the interface and work processes, and can export data directly from the connected product.[181]

89. Access must be provided to the product data and related service data, and to the metadata required to interpret and use this data.[182] These terms are further explained in Subsections 2.5.2 and 4.5 of these guidelines.

90. Access to the data should be provided in a standard, convenient, secure and cost-free manner. The data must be made available in a comprehensive, structured, commonly used and machine-readable format.[183] This is explained in further detail in Subsection 4.6 of these guidelines.

4.3.2 Who does the obligation apply to?

91. The obligation applies to parties responsible for the design and production of the connected product or related service. In practice, this will typically be the manufacturer or designer of the connected product.[184] However, there may be other parties with influence on the technical design of the product. In the case of related services, this will often be the developer.[185]

92. This obligation can also apply to multiple parties. A connected product may contain several data-generating components that do not originate from the manufacturer, or the design and assembly of a connected product may be performed by different parties. Similarly, related services are also typically developed in collaboration by multiple parties. In situations like these, a case-by-case assessment is necessary to determine which party has actual control and influence over design and production. If multiple parties share equal responsibility, they are all potentially obligated to ensure access by design.[186]

[178] Article 3(1) of the Data Act.
[179] Recital 22 of the Data Act. See also question 22 in the European Commission's FAQ.
[180] See also questions 17 and 22 in the European Commission's FAQ.
[181] See also question 17 in the European Commission's FAQ.
[182] Article 3(1) of the Data Act.
[183] *Ibid*.
[184] Recital 20 of the Data Act.
[185] For the sake of readability, this group will hereafter be referred to simply as "manufacturers."
[186] Recital 20 of the Data Act. See also question 21 in the European Commission's FAQ.

Example of direct access: an energy saving app

Example of direct access: an energy saving app

A company has developed an application that gives customers insight into the power generation of their solar panels. The app reads data from the solar panels and can also turn the panels on and off at favorable times. In addition, the app offers the ability to pair with other smart devices, such as certain types of thermostats, washing machines and dishwashers. The company has designed the app to ensure that it has access to the collected data.

The company provides direct access: the application is designed so that the data collected by the related service, as well as the relevant metadata, are directly accessible to the user. The data can be accessed, for example, using an export button in the app.

4.4 Indirect access (access upon request)

93. If the user does not have direct access, the data holder must make the readily available data and associated metadata available at the user's request.[187] ACM calls this **indirect access upon request**. In addition, regardless of whether the user has direct or indirect access to the data themselves, they can always request that a third party be granted indirect access to the data.[188] This third party may be a consulting firm, for example. Subsection 4.4.1 below discusses the provision of indirect access to the user themselves; Subsection 4.4.2 explains the provision of indirect access to third parties.

4.4.1 Indirect user access

94. A user can submit a request to access data. The data holder must then make this data available immediately. The quality of the data must be equal to the quality of the data held by the data holder.[189]

95. Thus, the main difference between indirect access upon request and direct access is that direct access does not require the intervention of the data holder, whereas indirect access upon request does. This is the case when the connected product is designed so that the user must ask the data holder for access to the data.[190] It should be easy for users to submit such requests electronically,[191] for example through a web portal[192] or an application related to the connected product.

96. The data holder must provide the user with access to the readily available data, and to the metadata needed to interpret and use this data.[193] These terms are further explained in Subsections 2.5.2 and 4.5 of these guidelines.

97. Where relevant and technically feasible,[194] data should be accessible continuously and in real time. The data must be made available in a convenient, secure and cost-free manner, and in a comprehensive, structured, commonly used and machine-readable format.[195] This is explained in further detail in Subsection 4.6 of these guidelines.

[187] This obligation is stipulated in Article 4(1) of the Data Act. See also recital 26 of the Data Act.
[188] See how Article 5(1) of the Data Act is worded. See also question 31 in the European Commission's FAQ and Section 38 of the European Commission's Vehicle Data Guidance.
[189] Article 4(1) of the Data Act. See also Sections 41 and 42 of the European Commission's Vehicle Data Guidance.
[190] See also question 17 in the European Commission's FAQ.
[191] *Ibid.*
[192] See also question 17 in the European Commission's FAQ.
[193] Article 4(1) of the Data Act.
[194] See also marginals 77 through 79 of these guidelines for explanations of these terms.
[195] Article 4(1) of the Data Act.

Example of indirect user access: smart manufacturing machines

Example of indirect user access: smart manufacturing machines

An industrial machinery manufacturer supplies smart manufacturing machines to factories. These machines continuously collect data on various metrics, such as running time, temperature and malfunctions. The manufacturer uses this data for analysis and maintenance purposes.

As the data holder, the manufacturer makes the readily available data generated by the use of the machines, as well as the relevant metadata, available to the user upon request. This can be done, for instance, by giving the user – upon receiving a simple electronic request – access to a secure API or an online portal, enabling continuous and real-time data retrieval.

4.4.2 Indirect third party access

98. A user, or a party acting on behalf of a user, may request that the data holder share data with a third party. The data holder must then make this data available immediately. The quality of the data must be equal to the quality of the data held by the data holder.[196]

99. If the data holder is required to make data available to a third party, it must agree with the third party on the terms under which data will be shared, including any fees.[197] More information on such agreements is provided from Subsection 5.2 of these guidelines.

100. The data holder is not required to make data on the connected product or related service available to a third party when testing a new connected product, or when testing substances or processes that have not yet been placed on the market,[198] unless the use by the third party is contractually authorized.[199]

101. A third party as referred to in these guidelines may not and cannot be a gatekeeper as defined in the Digital Markets Act (DMA).[200] The DMA uses the term “gatekeeper” to refer to the largest digital platform providers.[201] Additional restrictions apply to gatekeepers: they may not receive data from the user that the user has otherwise obtained by exercising their rights under the Data Act.[202]

102. The data holder must provide access to the readily available data, and to the metadata needed to interpret and use this data.[203] These terms are further explained in Subsections 2.5.2 and 4.5 of these guidelines.

103. Where relevant and technically feasible,[204] data should be accessible continuously and in real time. The data must be made available in a convenient, secure and, for the user, cost-free manner, and in a comprehensive, structured, commonly used and machine-readable format.[205] This is explained in further detail in Subsection 4.6 of these guidelines.

104. The third party may only use the data for purposes explicitly agreed with the user. Moreover, the third party may not use the data to develop competing products or services.[206] The obligations for

[196] Article 5(1) of the Data Act. See also Sections 41 and 42 of the European Commission’s Vehicle Data Guidance.
[197] Article 5(1) of the Data Act and Articles 8 and 9 of the Data Act.
[198] Article 5(2) of the Data Act.
[199] *Ibid.*
[200] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).
[201] For a current list of gatekeepers, see also European Commission, *Gatekeepers*, available at https://digital-markets-act.ec.europa.eu/gatekeepers_en?prefLang=nl.
[202] Article 5(3) of the Data Act. See also question 36 in the European Commission’s FAQ.
[203] Article 5(1) of the Data Act.
[204] See also marginals 77 through 79 of these guidelines for explanations of these terms.
[205] Article 5(1) of the Data Act.
[206] Article 6(2)(e) of the Data Act.

third parties receiving data at the user's request are discussed in more detail in Subsection 5.3 of these guidelines.

Example of indirect third party access: smart farming equipment

Example of indirect third party access: smart farming equipment

A manufacturer of smart farming equipment provides a system that continuously collects data on crop moisture, temperature and soil conditions. As the data holder, the manufacturer uses this data to optimize irrigation. The farmer is the user of the system and can access the data through an online platform.

As the data holder, the manufacturer makes the readily available data, as well as the relevant metadata, available to a third party designated by the farmer. This could be an analyst or technology partner who further analyzes the data. The manufacturer makes agreements with the third party regarding the provision of the data, in accordance with the conditions set by the Data Act.[207] The third party processes the provided data only for the purposes and under the conditions agreed upon with the farmer and the manufacturer.

4.4.3 Who does the obligation apply to?

105. The obligation to share data rests with the data holder. The data holder is the person or organization that, often by contract, has the right or obligation to use or share data.[208]

4.4.4 User verification by the data holder

106. The data holder must provide access to users. This may involve a verification process and information request to ensure that the person submitting an access request is actually a user of the connected product and thus entitled to access the data. This verification process should not make it unnecessarily difficult to gain access to the data,[209] and the data holder should not request more information than is necessary for this verification.[210] The data holder must also not retain more information about the user (such as log data) than is necessary for the provision of access and for the security and maintenance of the data infrastructure.[211]

107. Within the aforementioned limits, the data holder is free to design the verification process as it sees fit. In doing so, the following aspects could be considered:
- the most appropriate verification process for the type of product in question;
- the type of user (e.g. consumer or business user);
- the number of expected users (e.g. in the case of a shared car);
- the existence of various mechanisms to prove ownership (e.g. car registration);
- the cost of setting up multiple user accounts;
- the ease of use of a user account.[212]

108. Ideally, the verification process consists of a simple, automated request mechanism that does not require review or approval by the data holder.[213]

109. If a connected product has multiple users, it would make sense for the data holder to implement mechanisms to authenticate each user individually, for instance by allowing multiple user accounts to

[207] Article 8(1) of the Data Act. See also Section 5 of these guidelines.
[208] Article 2(13) of the Data Act. See also marginal 37 of these guidelines.
[209] Article 4(4) of the Data Act.
[210] Articles 4(5) and 5(4) of the Data Act. See also recital 29 of the Data Act.
[211] See also question 30 in the European Commission's FAQ.
[212] *Ibid.*
[213] Recital 21 of the Data Act. See also question 30 in the European Commission's FAQ.

be created. Allowing users to create multiple accounts also enables them to exercise their individual rights under the Data Act.[214]

110. When it comes to requesting access to personal data, the GDPR is and will continue to be guiding, as this involves a processing act. The GDPR stipulates that personal data may only be requested by the data controller or by the data subject in question.[215] If a user requests the personal data of another data subject, a valid legal basis for processing this data must be established under Article 6 of the GDPR. If special categories of personal data are involved, this basis must be established under Article 9(2) of the GDPR. Sharing personal data with third parties also requires a valid legal basis. Additionally, it is sometimes possible to provide anonymized data.[216] The Data Act does not provide a basis for processing personal data generated through the use of a connected product or related service.[217] The DPA will be responsible for enforcing this obligation.

4.5 What data must be made available

111. With regard to direct and indirect access, the Data Act uses different terms for the data that must be made accessible. For direct access, this is "**product data and related service data, including relevant metadata**"; for indirect access, this is "**readily available data, as well as the relevant metadata**." For a detailed explanation, a discussion of the differences between these terms, and related examples, see Subsection 2.5.2 of these guidelines.[218]

112. The Data Act's access obligation does not apply to "**derived data**,"[219] which is data that goes beyond the scope of raw or pre-processed data and represents new, valuable insights.[220] This distinction is designed to protect the innovations of the data holder, while allowing users and third parties to retain access rights to the underlying data generated by the use of the connected product or related service.[221] The Data Act aims to give users and third parties access to (co-)generated data on an equal footing with the data holder, enabling them to develop innovative products and services. Therefore, the underlying data that serves as input to innovative processing generally remains within the scope of the law, unless it is considered derived data itself.[222]

113. Not all data generated on or via a connected product falls within the scope of the regulation. For example, data generated by an application that is not a related service, but is accessible through a connected product, often falls outside the scope of the regulation. An example of this would be data generated by using a word processor on a desktop computer or laptop, or data generated by social media or a video game on a smartphone.

114. Data generated during a user's interaction with a virtual assistant does fall within the scope of the regulation. However, the regulation only applies to data that directly results from interacting with the connected product or related service via the virtual assistant. Data produced by the virtual assistant itself and not related to the use of a connected product or related service is not covered by the regulation.[223]

115. A user of a connected product may not be the first user of that product. In some cases, data generated by previous users will also be relevant to the current user and subject to obligations under the Data Act. Such "historical data" is relevant, for example, with respect to previous updates or past

[214] Recital 21 of the Data Act. See also question 16 in the European Commission's FAQ.
[215] Article 4(12) of the Data Act.
[216] See also question 25a in the European Commission's FAQ.
[217] Recital 7 of the Data Act.
[218] For examples of the different types of data from vehicles, see also Sections 33 through 35 of the European Commission's Vehicle Data Guidance.
[219] Recital 15 of the Data Act. See also Section 27 of the European Commission's Vehicle Data Guidance.
[220] See also Section 28 of the European Commission's Vehicle Data Guidance.
[221] Recital 15 of the Data Act. See also question 5 in the European Commission's FAQ.
[222] See also Sections 30 and 31 of the European Commission's Vehicle Data Guidance.
[223] Article 1(4) of the Data Act. See also recital 23 of the Data Act.

incidents involving the product. When granting access to historical data, the data holder should always take into account the rights of previous users, for example with respect to protecting their personal data under the GDPR. It is reasonable, therefore, that a user's access to historical data will often be more restricted than their access to data generated from their own use.

116. Finally, the regulation also makes it clear that certain types of textual, audio and audiovisual data do not fall within its scope. The English-language version of the regulation and the European Commission refer to this data as "***content***."[224] This exception distinguishes markets for connected devices and related services from markets for unrelated software and digital content. Content includes material that is similar to copyrighted material and is thus the result of a creative process.[225] It may be, but does not have to be, copyrighted material.[226] An essential characteristic of content is that it is intended for human appreciation or consumption.[227] Excluding content from the scope of the Data Act maintains existing legal protections and trading mechanisms for data representing content, while facilitating markets for other types of data, such as measurements and non-creative output.[228]

Example: smart digital camera for personal use

Example: smart digital camera for personal use

In most cases, a digital camera capable of recording, transmitting or displaying photos or videos will fall under the definition of a connected product. Thus, the data holder can be expected to make available the data generated by the camera's sensors, such as usage patterns, battery level, timestamps and location data. However, the data holder cannot, in principle, be expected under the Data Act to also make available the audiovisual content itself, such as photos or videos.[229]

Example: cameras in smart vehicles

Example: cameras in smart vehicles

There are also cameras that, combined with the right software, function as advanced sensors that make recommendations or perform actions. Cameras in connected vehicles are a good example. These cameras can analyze images and provide collision warnings or control emergency braking systems. Another example are cameras in agricultural machinery that measure plant health, allowing an agricultural machine to automatically apply fertilizers or pesticides. The images generated by these types of cameras may fall within the scope of the regulation, as they are not intended for human consumption and lack creative elements.[230]

4.6 Requirements for access provision

116. The Data Act imposes several requirements on the method of access provision. Some requirements apply only to direct access (access by design) and others only to indirect access (access upon request). A number of requirements apply to both types of access provision. Subsection

[224] Recital 16 of the Data Act. See also question 6 in the European Commission's FAQ.
[225] See also question 6 in the European Commission's FAQ.
[226] Recital 16 of the Data Act. See also question 6 in the European Commission's FAQ.
[227] See also question 6 in the European Commission's FAQ.
[228] *Ibid.*
[229] *Ibid.*
[230] *Ibid.*

4.6.1 begins by explaining these common requirements. Next, Subsections 4.6.2 and 4.6.3 discuss the requirements that apply only to direct access and indirect access, respectively.

4.6.1 Requirements for both direct access (access by design) and indirect access (access upon request)

117. Data access should always be **easy and intuitive**, **secure** and **free (for the user)**. There are also requirements for the **format** in which data is provided.[231] The Data Act does not provide further explanations of these terms.[232] Therefore, ACM offers general explanations of each term to facilitate their practical application below.

118. Data access should be **easy and intuitive**. This means that the data must be presented in a clear and accessible manner so that users without technical skills can easily access and manage their data.[233] This should require minimal effort, for instance thanks to user-friendly interfaces that provide data access through a simple action. If access is restricted to a specific location or depends on certain tools, this should not create unreasonable complications for users or third parties. Restrictions could include limited access times, location-based limitations or disproportionate costs.[234] In some cases, a specialized tool is required to retrieve data through a vehicle's OBD-II port, which must be purchased by the user.[235] In such situations, the data holder itself is required to provide the tool in question, free of charge, or to provide the data through other means.[236]

119. Data access must be **secure**. This means that authorized users must have secure access to data and metadata, which must be protected against unauthorized access, manipulation and misuse. This requires appropriate security measures and compliance with applicable legal standards.[237] Gaining access to the data should not expose the user to new risks. User access to smart lighting consumption data, for example, must not result in access to the control functions of the lighting by unauthorized parties.

120. Data access must be **free for the user**. This means that no fee may be charged for providing access. This includes direct compensation, financial or otherwise, as well as indirect compensation (i.e. raising other costs). It is not allowed, for example, to grant users access to their data only on the condition that the data holder may also share it with third parties, nor is it allowed to add a surcharge to a price quotation.

121. The Data Act sets out general requirements for the **format** in which data must be made accessible. Data must be provided in a **comprehensive**, **structured**, **commonly used** and **machine-readable** format. What is meant by this is explained below.

- **Comprehensive format**: the format must be complete. This means that the data should be shared in one uniform format, and not as a combination of multiple data sets in different file formats.
- **Structured format**: the format should be such that the data can be separated in a logical and clear manner. The recipient must be able to find and interpret specific data. A format is not structured, for example, if all the data is delivered in one long, unorganized row with no separations.

[231] Articles 3(1), 4(1) and 5(1) of the Data Act. See also question 22a in the European Commission's FAQ and Section 43 of the European Commission's Vehicle Data Guidance.
[232] See also Section 41 of the European Commission's Vehicle Data Guidance.
[233] See also Section 43 of the European Commission's Vehicle Data Guidance.
[234] See also question 22a in the European Commission's FAQ.
[235] See also Section 44 of the European Commission's Vehicle Data Guidance. See additionally, in the context of vehicle repair information, the European Court of Justice's ruling of October 5, 2023, in Case C-296/22, ECLI:EU:C:2023:743 (A.T.U. Auto-Teile-Unger GmbH & Co. KG and Carglass GmbH v. FCA Italy SpA).
[236] *Ibid.*
[237] These include relevant cybersecurity requirements found in European cybersecurity certification schemes, such as the European Common Criteria-based cybersecurity certification scheme (EUCC), based on Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cyber Security) (Cybersecurity Act). See also question 22a in the European Commission's FAQ.

- **Commonly used format**: the format should be widely accepted and common, at least within Europe. Examples of commonly used formats include JSON, XML and CSV. Common formats may vary depending on the industry or target group. Formats that are subject to licensing restrictions are not considered commonly used formats.[238]
- **Machine-readable format**: the format must be suitable for direct electronic processing of the data contained in the files.[239] This means that a data-processing program must be able to read the data in the file. This is not the case, for example, with PDF.

4.6.2 Specific requirements for direct access

122. If direct access to data is granted, such access should be provided **by default**. This means that the manufacturer must design the connected product or related service in such a way that the user can access the data without unreasonable effort on their part. It is up to the manufacturer to decide by what technical means access by default is provided.[240] The method of access should not be hidden behind multiple screens or settings, for example, nor should the user be discouraged or prevented from gaining access in other ways. In the example of a smart thermostat, the user has access to the data collected by the connected product through a mobile app or web portal by default.

4.6.3 Specific requirements for indirect access

123. If indirect access (access on demand) is granted, this access must be provided **immediately**, **continuously** and **in real time**. Moreover, the data holder should not make it **needlessly difficult** for the user to gain access, and the data provided **must be of the same quality**. This subsection explains these concepts in more detail.

124. Access to data should be provided **immediately**. This means that data must be made available quickly and without unnecessary delay. Solutions such as automation, streamlined request procedures and self-service portals should be used as much as possible to reduce delays and manual intervention.[241] While delays may be justified by security, technical or legal reasons, they must remain proportional to the request.[242]

125. In principle, access should be provided **continuously** and **in real time**. This means that the user does not have to request access every time they want to view the data, but that they have continuous access, without interruptions or undue delays. This requirement is included in the regulation for situations where there is a need to minimize delay ("latency"), for example in the case of certain IoT systems, connected mobility or industrial monitoring. The underlying philosophy of this requirement is that access should not be hindered by technical obstacles.[243] However, this form of access is only required when it is **relevant** and **technically feasible**.[244] For example, if the connected product collects data only incidentally, this may not be the case. Data holders should proactively implement solutions, such as APIs and "event architectures," to facilitate continuous and real-time access as much as possible.[245] If the data holder believes that continuous, real-time access is not technically feasible, it should consult with the user.

126. The data holder must not make it **needlessly difficult** for the user to exercise their choices or rights under the Data Act.[246] For example, it is not permitted to present choices in a non-neutral

[238] See also question 22a in the European Commission's FAQ.
[239] See also, in the context of machine-readable formats in vehicle data, recital 42 in the European Court of Justice's ruling of November 9, 2023, in Case C-319/22, ECLI:EU:C:2023:837 (Gesamtverband Autoteile-Handel eV v. Scania CV AB), and recital 28 in the European Court of Justice's ruling of October 27, 2022, in Case C-390/21, ECLI:EU:C:2022:837 (ADPA European Independent Automotive Data Publishers and Gesamtverband Autoteile-Handel e.V. v. Automobiles PEUGEOT SA and PSA Automobiles SA).
[240] Recital 22 of the Data Act.
[241] Recital 21 of the Data Act.
[242] See also question 22a in the European Commission's FAQ.
[243] Recital 35 of the Data Act. See also question 22a in the European Commission's FAQ. This is thus regulated differently than, for example, the right to data portability in Article 20 of the GDPR.
[244] See marginals 77 through 79 of these guidelines for explanations of these terms.
[245] See also question 22a in the European Commission's FAQ.
[246] This refers specifically to the rights set forth in Article 4(4) of the Data Act.

manner, or to undermine or interfere with the user's autonomy, decision-making or freedom of choice by modifying the structure, design, functionality or use of the digital user interface (or any part thereof). The use of "dark patterns" (misleading design choices that manipulate users into performing or avoiding certain actions) is therefore not allowed.[247]

127. Finally, the data shared by the data holder must be of **the same quality** as the data it has access to itself. This means that the data must be as accurate, complete, reliable, relevant and current as the data that is, or can be, accessed by the data holder itself based on the use of the connected product or related service.[248] This implies that the data that is shared with users must be of the same quality, and provided in the same format, as data shared with another subsidiary within the same group, or in a manner consistent with industry standards or practices within a specific industry.[249] This requirement also means that there may be no discrimination. In the context of the automotive industry, for example, discrimination might occur with respect to independent garages or service providers. The data holder must not make data accessible at a quality level lower than that at which the data is made available internally, or to subsidiaries, authorized partners, dealers and mechanics.[250]

4.7 Exceptional cases in which it is permissible to refuse data sharing due to security risks or trade secrets

128. The Data Act describes two situations in which it is permissible for users and data holders to restrict or deny data sharing: to avoid serious security risks (the "safety and security handbrake")[251] or due to trade secrets (the "trade secrets handbrake").[252] Neither of these grounds for exemption should be invoked lightly, which is why there are a number of conditions and safeguards. These are described in the next two subsections.

4.7.1 Security risks

129. The data holder or user may contractually restrict or prohibit access to data, or its use or further sharing. This can only be done in exceptional cases, when access to the data would compromise the security requirements of a connected product, resulting in serious risks to the health, safety or security of natural persons.[253] Relevant security requirements are set forth in national laws or European legislation, such as the Cyber Resilience Act,[254] the NIS2 Directive,[255] the Medical Device Regulation (MDR)[256] and the Toy Safety Regulation.[257]

[247] Article 6(1) and (2)(a) of the Data Act. See also recitals 37 and 38 of the Data Act. Recital 38 of the Data Act, the DSA Guidelines and ACM's Guidelines on the protection of the online consumer provide more information on dark patterns. For the DSA Guidelines, see ACM, *Guidelines on the Digital Services Act (DSA) for providers of online services*, available at https://www.acm.nl/en/publications/guidelines-digital-services-act-dsa-providers-online-services. For the Guidelines on the protection of the online consumer, see ACM, *Guidelines on the protection of the online consumer*, available at https://www.acm.nl/en/publications/guidelines-protection-online-consumer.
[248] Recital 30 of the Data Act. See also Section 41 of the European Commission's Vehicle Data Guidance.
[249] See also question 22a in the European Commission's FAQ and Section 41 of the European Commission's Vehicle Data Guidance.
[250] See also Section 42 of the European Commission's Vehicle Data Guidance.
[251] Article 4(2) of the Data Act. See also question 25 in the European Commission's FAQ.
[252] Articles 4(6) and (7) and 5(10) and (11) of the Data Act. See also question 23 in the European Commission's FAQ.
[253] Article 4(2) of the Data Act. See also question 25 in the European Commission's FAQ.
[254] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).
[255] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).
[256] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2027 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Medical Device Regulation).
[257] Regulation (EU) 2025/2509 of the European Parliament and of the Council of 26 November 2025 on the safety of toys and repealing Directive 2009/48/EC (Toy Safety Regulation).

130. If the data holder refuses to share data with the user because of security risks, it must notify ACM.[258] This can be done using a dedicated form on ACM's website.[259]

131. Without prejudice to the user's right to go to court, in the event of a conflict with the data holder due to security risks, the user may file a complaint with ACM[260] or agree with the data holder to submit the dispute to a dispute resolution body.[261] The right to refer the matter to a dispute resolution body is further explained in Subsection 4.8 of these guidelines. Users can submit their complaints to ACM through a dedicated form on the ACM website.[262]

4.7.2 Trade secrets

132. The data holder may also deny or restrict access to data if data from a connected product or related service contains trade secrets.[263] In such cases, the Data Act seeks to balance two interests: the protection of the data holder's trade secrets versus the avoidance of unjustified refusals or restrictions on data sharing. The regulation therefore stipulates that trade secrets should only be shared if all necessary measures can be taken to ensure their confidentiality, especially with regard to third parties.[264] Trade secrets may only be shared with third parties if this is strictly necessary to achieve the purpose agreed upon between the user and the third party.[265]

133. The regulation outlines the following procedure for handling data containing trade secrets:
1. When the data holder receives a data sharing request, it identifies the data, including relevant metadata, to be protected as a trade secret.[266] Thus, the data holder determines what data qualifies as a trade secret.[267]
2. The data holder and the user or third party reach a joint agreement on the necessary measures to ensure the confidentiality of the trade secrets.[268] These measures must be established before the data is shared. Measures can be both technical and organizational in nature, such as the use of model contractual terms, confidentiality agreements, strict access protocols, technical standards and codes of conduct.[269]

134. In certain cases, using anonymization, pseudonymization or encryption techniques can reduce the risk of trade secret infringement (or GDPR violations). However, the use of these techniques does not relieve data holders of their obligations to make data available under the regulation. Users or third parties must also have been given a "reasonable opportunity" to copy the data before it is anonymized or encrypted.[270]

135. Data sharing may be stopped or suspended if:
1. no agreement is reached on the measures to be taken;
2. the agreements made and measures taken are not complied with; or
3. the confidentiality of trade secrets is undermined.

The data holder must communicate this in writing to the user or third party as soon as possible, including proper justification. In addition, the data holder must notify ACM. In doing so, it must explain

[258] Article 4(2) of the Data Act. See also question 25 in the European Commission's FAQ.
[259] ACM, *Geen data delen*, available at https://mijn.acm.nl/nl/geen-data-delen (Dutch only).
[260] Article 4(3)(a) of the Data Act. See also question 25 in the European Commission's FAQ.
[261] Article 4(3)(b) of the Data Act. See also question 25 in the European Commission's FAQ.
[262] ACM, *Uw melding over een online platform, clouddienst of data uit uw slimme apparaat*, available at https://www.acm.nl/nl/uw-melding-over-een-online-platform-clouddienst-data-uit-uw-slimme-apparaat (Dutch only).
[263] See also marginal 51 of these guidelines for a definition of the term "trade secrets."
[264] Articles 4(6) and 5(9) of the Data Act. See also question 23 in the European Commission's FAQ.
[265] Article 4(6). See also recital 31 of the Data Act.
[266] Articles 4(6) and 5(9) of the Data Act. The obligation applies to the data holder, or to the holder of a trade secret in cases where this is not the data holder.
[267] Articles 4(6) and 5(9) of the Data Act. See also question 23 in the European Commission's FAQ.
[268] Articles 4(6) and 5(9) of the Data Act. See also question 23 in the European Commission's FAQ.
[269] Articles 4(6) and 5(9) of the Data Act. See also recital 31 of the Data Act and questions 23 and 24 in the European Commission's FAQ.
[270] See also question 13a in the European Commission's FAQ.

which measures have not been agreed or complied with, and which trade secrets' confidentiality may have been undermined.[271] This can be done using a dedicated form on ACM's website.[272]

136. In exceptional cases, the data holder may deny a request to access specific data if the sharing of data containing trade secrets is highly likely to result in serious financial harm, despite all measures taken.[273] This harm must consist of serious and irreparable financial damages.[274] The data holder must demonstrate the existence of this risk and substantiate the evidence using objective elements, such as the enforceability of trade secret protection in third countries, the nature and level of confidentiality of the requested data, and the extent to which the connected product in question is new and unique.[275]

137. The data holder must provide the evidence in writing and as soon as possible to the user or third party. In addition, the data holder must notify ACM using the form on its website.[276]

138. The user may file a complaint with ACM in the event of a dispute over a decision by the data holder to refuse, stop or suspend data sharing citing the presence of trade secrets.[277] A third party with indirect access at the user's request also has this right.[278] Users and third parties can submit their complaints to ACM through a dedicated form on the ACM website.[279] If the complaint relates to the non-sharing of data due to trade secrets, ACM will decide without delay whether, and if so under what conditions, the data should be shared or the sharing of data should be resumed. ACM has a separate procedure for this purpose. As an alternative to filing a complaint, the user and third party may also agree with the data holder to submit the dispute to a dispute resolution body.[280] The right to refer the matter to a dispute resolution body is further explained in Subsection 4.8 of these guidelines. These options exist without prejudice to the user's right to seek redress in court.

4.8 Dispute resolution in cases of data access restriction

139. The user has several options to exercise their rights if the data holder restricts data sharing based on an exception and the user disagrees. If data is not shared, the user can submit a complaint to ACM.[281] ACM can then, for example in the case of multiple complaints, launch an investigation to examine whether the data holder is consistently violating the Data Act.[282] The parties may also refer the dispute to a dispute resolution body. This option is discussed in more detail in this subsection.

140. Dispute resolution by a dispute resolution body certified under the Data Act is only possible in a number of cases specified in the Data Act. Specifically for data sharing, dispute resolution is an option for disputes over reliance on the exceptions described in Subsection 4.7 of these guidelines, which pertain to restricting access due to security risks or security requirements.[283] Dispute resolution is also available for disputes over the terms and fees for making data available.[284]

[271] Articles 4(7) and 5(10) of the Data Act. See also question 23 in the European Commission's FAQ.
[272] ACM, *Geen data delen*, available at https://mijn.acm.nl/nl/geen-data-delen (Dutch only).
[273] Articles 4(8) and 5(11) of the Data Act.
[274] See also question 23 in the European Commission's FAQ.
[275] Articles 4(8) and 5(11) of the Data Act.
[276] ACM, *Geen data delen*, available at https://mijn.acm.nl/nl/geen-data-delen (Dutch only).
[277] Article 4(9)(a) of the Data Act.
[278] Article 5(12)(a) of the Data Act.
[279] ACM, *Uw melding over een online platform, clouddienst of data uit uw slimme apparaat*, available at https://www.acm.nl/nl/uw-melding-over-een-online-platform-clouddienst-data-uit-uw-slimme-apparaat (Dutch only).
[280] Article 10(1) of the Data Act.
[281] Article 38 of the Data Act.
[282] This is different for Articles 4(9)(a) and 5(12)(a) of the Data Act.
[283] Articles 4(9)(b) and 5(12)(b) of the Data Act. See also question 23 in the European Commission's FAQ.
[284] Article 10(1) of the Data Act.

141. A dispute resolution request must be submitted jointly by the user and data holder (and/or third party) involved in the dispute. This means that the parties involved must agree to submit the dispute to the dispute resolution body.[285]

142. Dispute resolution does not preclude the possibility of taking the issue to court. This means that the parties may at any time, even after dispute resolution as described here, apply to the competent judicial authority.

143. Dispute resolution requests can only be submitted to a dispute resolution body that is certified in the manner described in the Data Act.[286] ACM is authorized to certify dispute resolution bodies based in the Netherlands.[287] The European Commission publishes a list of certified dispute resolution bodies in the European Union on its website.[288] ACM keeps the European Commission informed about the certification of dispute resolution bodies in the Netherlands.[289]

144. ACM only certifies dispute resolution bodies upon request. To apply for certification, dispute resolution bodies must use the dedicated form on ACM's website. In their application, organizations must demonstrate that they meet all the certification requirements set forth in the Data Act.[290] ACM may revoke certification if the body in question no longer meets these requirements.[291]

[285] Articles 4(3) and (9) and 5(12) of the Data Act.
[286] Article 10(5) of the Data Act.
[287] Article 10(5) of the Data Act and Article 2(1) of the Data Act Implementation Act.
[288] At the time of writing, the link to this page is not yet available. Once it does become available, ACM will refer to the European Commission's list on its website.
[289] Article 10(6) of the Data Act.
[290] These requirements are laid down in Article 10(5) of the Data Act.
[291] Article 2(3) of the Data Act Implementation Act.

5 Data sharing requirements, conditions and agreements

5.1 Introduction

145. In addition to pre-contractual disclosure obligations,[292] the Data Act also provides rules for the contractual relationship between the data holder and the data recipient. The regulation sets rules for data holders, as well as users and third parties, on what they may and may not do with the collected or obtained data, and on what parties may agree with each other regarding the use of this data.

146. Subsection 5.2 begins by explaining the rules governing the use of data by the data holder and the safeguards it must provide. Next, Subsection 5.3 discusses the conditions for and restrictions on the use of acquired data by users and third parties. Following that, Section 5.4 examines the sharing of data by the data holder with a data recipient, paying particular attention to the standard that data sharing agreements must be "fair, reasonable, non-discriminatory and transparent." Subsection 5.5 then discusses the compensation data holders may demand for data access. Finally, Subsection 5.6 discusses standard contracts that can be used to establish mutual rights and obligations.

5.2 Requirements for data holders

147. The GDPR is fully applicable to all processing of personal data within the scope of the Data Act.[293] This means that when a user requests personal data on someone other than themselves, or wants to share this data with a third party,[294] the data holder may only grant the request if there is a valid legal basis for processing.[295] This is regulated by the DPA.

148. The data holder may use non-personal, readily available data only if this has been agreed upon in advance (contractually) with the user.[296] The data holder may make non-personal product data available to third parties, but only to the extent specified in the agreement with the user. It is also the responsibility of the data holder to contractually prohibit third parties to whom it makes this data available from sharing it further.[297]

149. Stricter rules apply to the use of readily available data in certain circumstances. This is the case if the data holder may thereby gain insight into the financial situation, assets, production methods, products or services of the user or of a third party in the market in which it operates, and if such insight could affect the commercial position of the user or third party.

1. Such use of data is not permitted when the data in question is the user's own data. Thus, this may also not be contractually agreed upon.[298]
2. In principle, such use of data is also not permitted when the data in question is a third party's data. This is only permitted if the third party has given explicit consent *and* can easily withdraw this consent at any time.[299]

[292] As outlined in Section 3 of these guidelines.
[293] Article 1(5) of the Data Act. See also Subsection 2.6 of these guidelines.
[294] Article 5(7) of the Data Act. See also recital 35 of the Data Act.
[295] Article 4(12) of the Data Act. See also recital 34 of the Data Act. The legal grounds for processing are listed in Article 6 of the GDPR. In addition, Article 4(12) of the Data Act refers to Article 9 of the GDPR and Article 5(3) of the Directive on privacy and electronic communications.
[296] Article 4(13) of the Data Act. This applies to connected products placed on the EU market before and after September 12, 2025. Data holders able to identify users of their connected products placed on the market before September 12, 2025, must therefore: (1) enter into a contract that secures the user's consent to use the data, if they did so without a contractual basis; or (2) check whether an existing agreement (e.g. a sales contract, a contract for the provision of related services, or another agreement) needs to be modified to include the user's consent to use the data. For more information, see also question 34a in the European Commission's FAQ.
[297] Article 4(14) of the Data Act.
[298] Article 4(13) of the Data Act.
[299] Article 5(6) of the Data Act.

Example: smart inventory management

Example: smart inventory management

Stricter rules may apply to readily available data when using RFID-based smart inventory management systems in a B2B relationship. Smart RFID shelves in warehouses can collect real-time data on inventory levels, sales trends and product sales. While this data may appear simple, it can offer deep insights into a user's commercial position, such as which products are selling well and how efficiently inventory is being managed.

150. The data holder may implement technical safeguards, such as smart contracts and encryption for authentication and authorization purposes, to prevent unauthorized access to data and metadata, and to ensure that all parties comply with their legal obligations under the Data Act and the contractual terms they agreed to.[300]

151. These safeguards must be proportionate and non-discriminatory: the data holder may not distinguish between different data recipients or interfere with users' fundamental rights.[301] This means that users must still be able to access, copy and use their data unimpeded. They must also still be able to share it with third parties, in accordance with legal requirements. The rights of third parties under European legislation and national legislation adopted in accordance with European law must also be fully respected.[302]

5.3 Requirements for users and third parties

5.3.1 Requirements for users and third parties

152. The user or third party granted access to data in accordance with the Data Act may not use this data to develop a connected product that would compete with the connected product from which the data originated,[303] nor are they permitted to share data with another third party for this purpose. A competing connected product is a product that falls within the same market as the connected product from which the data originated.[304]

153. Note that this prohibition expressly does not apply to developing a related service that may compete with that of the data holder. Stimulating innovation in aftermarkets is an explicit objective of the Data Act.[305] The Data Act also states that the use of data for reverse engineering is permitted, as long as this is done in accordance with the regulation and European or national legislation. This can be done for repair purposes, to extend the life of a connected product, or to provide aftermarket services, for example.[306]

154. The user and third party are not permitted to use the data to gain insight into the financial situation, assets, production methods, or their use by the manufacturer or data holder.[307]

[300] Article 11(1) of the Data Act. See also recital 57 of the Data Act.
[301] See also Section 42 of the European Commission's Vehicle Data Guidance.
[302] Article 11(1) of the Data Act. See also recital 57 of the Data Act.
[303] Articles 4(10) and 6(2)(e) of the Data Act.
[304] Recital 32 of the Data Act. The relevant market should be defined according to the established principles of EU competition law.
[305] Recital 32 of the Data Act. See also question 26 in the European Commission's FAQ.
[306] Recital 25 of the Data Act.
[307] Article 4(10) of the Data Act.

155. Moreover, a user or third party may not use coercive means or exploit weaknesses in the technology used by the data holder to secure data in order to gain access to that data.[308]

156. The data holder may implement technical safeguards to prevent unauthorized access to data and metadata and ensure that all parties comply with the obligations of the Data Act and the agreed contract terms. This is discussed in Subsection 4.7.2 of these guidelines. The user, third party or other data recipient may not modify or remove these technical safeguards without the explicit consent of the data holder.[309]

5.3.2 Specific requirements for third parties

157. A third party may only use the received data for the purpose authorized by the user and within the conditions agreed with the user.[310] In doing so, the third party must also comply with European and national data protection laws, for example as prescribed in the GDPR. The data must be deleted as soon as it is no longer needed for the agreed purpose, unless otherwise agreed for non-personal data.[311]

158. It should be as easy for the user to deny or terminate third party access to the data as it is for them to grant access.[312] The third party should not make it needlessly difficult for the user to exercise their choices or rights under the Data Act.[313] For example, a third party is not permitted to present choices in a non-neutral manner, or to undermine or interfere with the user's autonomy, decision-making or freedom of choice by modifying the structure, design, functionality or use of the digital user interface (or any part thereof). The use of "dark patterns" (misleading design choices that manipulate users into performing or avoiding certain actions) is therefore not allowed.[314]

159. The third party may not use the data received to profile individuals. Profiling refers to any form of automated processing of personal data in which certain personal aspects of a natural person are evaluated on the basis of personal data.[315] Profiling is allowed, however, if such processing activities are strictly necessary to provide the service requested by the user. This may be the case in the context of automated decision-making, for example.[316] The DPA oversees these regulations.

160. The third party may not share the data received with another third party, unless the user has agreed to this. If data is shared with another third party, it must take all necessary measures to protect the confidentiality of trade secrets, as agreed by the data holder and the third party.[317]

161. The third party may not share the data received with companies designated as gatekeepers as referred to in the DMA.[318]

162. A third party may not use the data received in a way that would negatively impact the security of a connected product or related service. It is not permitted, for instance, to manipulate software updates

[308] Articles 4(11) and 5(5) of the Data Act.
[309] Article 11(1) of the Data Act. See also recital 57 of the Data Act. This provision thus ensures a balance between the security needs of data holders and the access rights of users and third parties, stimulating technical innovation without undermining the objectives of the Data Act.
[310] Article 6(1) of the Data Act. See also question 35 in the European Commission's FAQ.
[311] Article 6(1) of the Data Act. See also recitals 38 and 39 of the Data Act. The obligation to delete data as soon as it is no longer needed for the purpose agreed with the user – unless something else has been agreed for non-personal data – is in addition to the data subject's right to have their data deleted under Article 17 of the GDPR.
[312] Recital 38 of the Data Act.
[313] This refers specifically to the rights set forth in Articles 5 and 6 of the Data Act.
[314] Article 6(1) and (2)(a) of the Data Act. See also recitals 37 and 38 of the Data Act. Recital 38 of the Data Act, the DSA Guidelines and ACM's Guidelines on the protection of the online consumer provide more information on dark patterns. For the DSA Guidelines, see ACM, *Guidelines on the Digital Services Act (DSA) for providers of online services*, available at https://www.acm.nl/en/publications/guidelines-digital-services-act-dsa-providers-online-services. For the Guidelines on the protection of the online consumer, see ACM, *Guidelines on the protection of the online consumer*, available at https://www.acm.nl/en/publications/guidelines-protection-online-consumer.
[315] Article 2(20) of the Data Act. See also Article 4(4) of the GDPR.
[316] Article 6(2)(b) of the Data Act. See also recital 39 of the Data Act and Article 2(2)(a) and (c) of the GDPR.
[317] Article 6(2)(c) of the Data Act.
[318] Article 6(2)(d) of the Data Act. See also marginal 101 of these guidelines.

for a smart thermostat in a way that could cause overheating, or to disrupt communications between a connected car and its sensors, as this could lead to accidents.[319]

163. The third party is expected to comply with the specific measures agreed with the data holder or trade secret holder. Moreover, the third party is explicitly prohibited from compromising the confidentiality of trade secrets.[320]

164. The third party receiving data may not hinder a user who is a consumer, through contract terms or otherwise, from sharing the data with another party.[321]

5.3.3 Remedies

165. The Data Act offers far-reaching remedies in the event that a third party or data recipient breaches its obligations under the regulation. The situations where there is such a breach are also listed in the regulation, which states that a breach occurs if a third party or data recipient:
1. has sought to obtain data by providing false information to the data holder, employing deceptive means, using coercive means or exploiting weaknesses in technology used by the data holder to protect the data;[322]
2. has used the data made available for unauthorized purposes, such as developing a competing connected product;[323]
3. has unlawfully shared data with another party;[324]
4. has failed to comply with the technical and organizational security requirements agreed with the data holder or trade secret holder;[325]
5. has removed or modified the technical safeguards implemented by the data holder without the data holder's consent.[326]

166. If one of the situations described above occurs, the data holder, user or trade secret holder may request certain remedies from the third party or data recipient. The third party or data recipient must comply with such requests as soon as possible. The data holder, user or trade secret holder may request that the third party or data recipient:
1. delete the data made available by the data holder and copies thereof;[327]
2. inform the user of the unauthorized use or disclosure of the data, as well as the measures taken to stop such use or disclosure;[328]
3. indemnify the party that has suffered damages due to the misuse or disclosure of the unlawfully accessed or used data.[329]

167. The data holder, user or trade secret holder may also, under certain conditions, request that the third party or data recipient:[330]
    1. stop producing, offering, bringing to market or using goods or derived data or services created using the data received; or
    2. stop storing infringing goods for these purposes or importing or exporting infringing goods (or that they destroy the infringing goods).

[319] Article 6(2)(f) of the Data Act.
[320] Article 6(2)(g) of the Data Act. See also marginal 135 of these guidelines.
[321] Article 6(2)(h) of the Data Act.
[322] Article 11(3)(a) of the Data Act. This prohibition is imposed on third parties in Article 5(5) of the Data Act and further elaborated in marginal 155 of these guidelines.
[323] This prohibition is stipulated in Article 6(2)(e) of the Data Act. It is further elaborated in marginal 104 of these guidelines.
[324] Article 11(3)(c) of the Data Act.
[325] This requirement is laid down in Article 5(9) of the Data Act. It is further elaborated in marginals 132 and 133 of these guidelines.
[326] This requirement is laid down in Article 11(1) of the Data Act. It is further elaborated in marginal 156 of these guidelines.
[327] Article 11(2)(a) of the Data Act.
[328] Article 11(2)(c) of the Data Act.
[329] Article 11(2)(d) of the Data Act.
[330] Article 11(2)(b) of the Data Act.

168. The data holder, user or trade secret holder may request these actions if:[331]
1. in case of infringement, there is a serious risk that unauthorized use of the data will cause serious harm to the data holder, user or trade secret holder; or
2. implementing the requested measure would not be disproportionate in view of the interests of the data holder, user or trade secret holder.

169. These remedial provisions also apply:[332]
1. when the user has changed or removed the data holder's technical safeguards to protect trade secrets; or
2. when the user has failed to comply with the technical and organizational security requirements agreed with the data holder or trade secret holder.

170. The remedial provisions also apply to any other party that has received data from a user as a result of a breach of the Data Act.[333]

171. Finally, certain third party requirements with respect to the user also apply to the data recipient. A data recipient should not make it needlessly difficult for the user to exercise their choices or rights under the Data Act. In addition, a data recipient may not, in principle, use received data for profiling. These prohibitions and their exceptions are further described in marginals 158 and 159 of these guidelines. If a data recipient violates the requirements described herein, a user may demand the remedies described in this section from the data recipient.[334]

5.4 Requirements for data sharing by the data holder

172. The data holder may be required by the Data Act or other national or European legislation to share data with a data recipient, usually a third party. The Data Act requires the data holder and third party to establish data sharing arrangements in an agreement.[335] In line with the principle of freedom of contract, the parties involved are free to negotiate the exact terms under which data is made available.[336] However, these arrangements must be fair, reasonable, non-discriminatory and transparent.[337]

173. The terms "fair," "reasonable," "non-discriminatory" and "transparent" are broad, open standards, often referred to as the FRAND standards. These standards are common in regulating access, for example to telecommunications networks, but they are also used in the context of technologies and industry standards.[338] Since these are open standards, their precise interpretation will vary from case to case, and it is up to the relevant parties to determine their appropriate application. This interpretation may be reviewed by the regulator, dispute resolution bodies or the courts. General explanations of each term are provided below.
- **Fair**: Contractual terms that deviate significantly from common business practices and violate the principles of good faith and fair treatment are considered unfair.
- **Reasonable**: Contractual provisions should be balanced. The party that drafted the provisions must be able to demonstrate that these were not unilaterally imposed and are not unreasonable. This is especially important for preventing unfair commercial practices and ensuring a fair distribution of data value within the European data economy.

[331] *Ibid.*
[332] Article 11(4) of the Data Act.
[333] Article 11(4) of the Data Act.
[334] Article 11(5) of the Data Act.
[335] Article 8(1) of the Data Act.
[336] Recital 43 of the Data Act.
[337] Article 8(1) of the Data Act.
[338] See, for example, in the context of standard essential patents, the European Court of Justice's ruling of July 16, 2015, in Case C-170/13, ECLI:EU:C:2015:477 (Huawei Technologies Co. Ltd v. ZTE Corp. and ZTE Deutschland GmbH). See also Sections 7 and 8 of the European Commission's Draft Guidelines for Reasonable Compensation.

- **Non-discriminatory**: Businesses and users should be treated equally when it comes to data access and use. This includes preventing unfair contractual terms imposed by large or strong parties on small or weak parties, which can lead to discrimination.

174. The regulation gives additional substance to the term **non-discriminatory** and stipulates that the data holder may not discriminate between similar categories of data recipients when sharing data, regardless of their size.[339] Whether a data recipient falls into a similar category will vary from case to case, and determining this will require specific analysis.[340] There is no unlawful discrimination when the use of different contract terms for data sharing is justified for objective reasons.[341] If a data recipient believes that the conditions for making data available are discriminatory, they may submit a substantiated request to the data holder. The data holder must then provide information that shows that there is no discrimination as soon as possible.[342]

175. Regarding the requirement of **fairness**, the regulation introduces a system[343] for assessing whether a unilaterally imposed[344] contractual term *is considered* unfair[345] or *presumed to be* unfair.[346] The difference is that terms that are presumed to be unfair will only be considered unfair if the data holder fails to provide convincing evidence to the contrary. The system described here is similar to the gray and black lists of unfair contractual terms in consumer law.[347]

176. An example of a provision that is always considered unfair is one in which the party unilaterally imposing the clause excludes or restricts its liability in the event of an intentional act or gross negligence.[348] An example of a provision that is presumed to be unfair is one in which the party on whom the clause is imposed is prevented from terminating the contract within a reasonable time frame.[349]

177. Terms that are considered to be unfair are non-binding. This means that the party on whom they are imposed cannot be held to them. The methodology for assessing the fairness of unilaterally imposed contractual terms applies specifically to contractual terms on access to and use of data, or on liability for data-related obligations.[350] Parts of the contract that do not involve data do not fall within the scope of these rules.[351] Sometimes agreements also contain general provisions that apply to all contractual obligations. Such provisions are subject to these rules only insofar as they relate to data access and use or data-related obligations. Thus, provisions governing other contractual aspects, such as the terms of a bank loan, are not included.[352]

178. Contractual terms that limit the user's rights under Chapter II of the Data Act, to the user's detriment, are always non-binding, whether unilaterally imposed or not.[353]

[339] Article 8(3) of the Data Act.
[340] See also question 38 in the European Commission's FAQ.
[341] Recital 45 of the Data Act.
[342] Article 8(3) of the Data Act.
[343] Article 50 of the Data Act makes it clear that this system is only applicable to: (1) contracts entered into after September 12, 2025; or (2) from September 12, 2027, to contracts entered into on or before September 12, 2025, provided these contracts are indefinite or will expire at least 10 years after January 11, 2024. For more information, see also question 42b in the European Commission's FAQ.
[344] In essence, a contractual term is considered unilaterally imposed when one party proposes a particular contractual term and the other is unable to influence its content, despite attempting to negotiate it. See also recital 59 of the Data Act.
[345] Article 13(4) of the Data Act lists contractual terms that are considered to be unfair.
[346] Article 13(5) of the Data Act lists contractual terms that are presumed to be unfair.
[347] For more on the methodology of Article 13 of the Data Act, see also recitals 58 through 62 of the Data Act and questions 41 and 42 in the European Commission's FAQ.
[348] Article 13(4)(a) of the Data Act.
[349] Article 13(5)(d) of the Data Act.
[350] Article 13(1) of the Data Act.
[351] Recital 60 of the Data Act. See also question 42a in the European Commission's FAQ.
[352] See also question 42a in the European Commission's FAQ.
[353] Article 8(2) of the Data Act.

179. The data holder may share data with a data recipient only if this is requested by the user under the regulation. This also applies to sharing data with the data recipient on an exclusive basis.[354]

180. Neither the data holder nor the data recipient is required to provide information beyond what is necessary to demonstrate compliance with the agreed upon conditions for making data available, or with other obligations under the Data Act or other European or national law.[355]

5.5 Compensation for data sharing

181. The data holder and data recipient may mutually agree on a fee for data sharing.[356] This is permitted only in business-to-business relationships; it is not permitted in relationships between data holders and consumers.[357] To clarify, the data recipient in this situation is a third party, not the user. User access to data must always be provided free of charge, regardless of the form of access.[358] In addition, if the user shares the data with a third party independently, that is, without the data holder's intervention, the data holder cannot seek compensation from the user or the third party. However, the user in this case would be allowed to charge a fee to the third party.[359] The Data Act emphasizes that this fee should not be construed as payment for the data itself.[360]

182. Although the regulation sets several general conditions for allowable data sharing fees, it only elaborates on these conditions to a limited extent. To provide as much explanation as possible, ACM has used a draft version of the guidelines that the European Commission will publish in 2026, the Draft Guidelines for Reasonable Compensation Under Article 9 of the Data Act.[361] It is important to note that this is a consultation version, and that the information below will be updated later this year based on the European Commission's final publication.

5.5.1 Conditions for calculating compensation

183. When negotiating fees, principal considerations should be:
1. the technical costs of making data available, including the costs of **data formatting**, **electronic dissemination** and **storage**;[362] and
2. the investment in data **collection** and **production**, including the extent to which other parties contributed to obtaining, generating or collecting the data.[363]

184. Compensation must be **non-discriminatory** and **reasonable**.[364] In addition, the fee must generally be **incremental**, **objective**, **measurable** and **proportionate**.[365] The fee may include a margin.[366] The Data Act does not stipulate a minimum or maximum fee.[367] In general, fees will depend

[354] Article 8(4) of the Data Act. The original intent of the provision was to preclude situations where data would be shared exclusively with one data recipient. During the legislative process, the provision was modified slightly to emphasize that the data transfer between the data holder and a data recipient may occur only at the request of the user. The article is thus in line with what follows from Article 5 of the Data Act.
[355] Article 8(5) of the Data Act.
[356] Recital 48 of the Data Act emphasizes that intervention is not necessary in the case of data sharing between large enterprises, or when a small or medium-sized enterprise is the data holder and a large enterprise is the data recipient, since these parties are assumed to be able to negotiate reasonable and non-discriminatory fees.
[357] Article 9(1) of the Data Act.
[358] See marginal 120 of these guidelines.
[359] Recital 26 of the Data Act.
[360] Recital 46 of the Data Act.
[361] European Commission, *Draft Guidelines for Reasonable Compensation Under Article 9 of the Data Act*, available at https://digital-strategy.ec.europa.eu/en/consultations/data-act-commission-seeks-feedback-draft-guidelines-reasonable-compensation.
[362] Article 9(2)(a) of the Data Act.
[363] Article 9(2)(b) of the Data Act. See also Section 21 of the European Commission's Draft Guidelines for Reasonable Compensation.
[364] Article 9(1) of the Data Act. See also recital 48 of the Data Act.
[365] See also Section 32 of the European Commission's Draft Guidelines for Reasonable Compensation.
[366] *Ibid.*
[367] See also question 39 in the European Commission's FAQ.

on the size, format and nature of the data, and thus may vary from case to case.[368]

184. The requirement that the fee be **non-discriminatory** is not explained in detail in the regulation, but the European Commission does provide some clarification on this. The aim of the requirement is to ensure that data recipients are treated equally. Only if justified by objective criteria may a distinction be made between data recipients.[369] Thus, unwarranted differentiation, such as denying access or imposing higher fees simply because a recipient is a current or potential competitor, is not permitted.[370] However, differentiation may be justified when it is related to objective requirements, such as additional costs:[371]

1. that are necessary to ensure that security, compliance or confidentiality standards are met;
2. arising from measures to protect or safeguard the confidentiality of sensitive data, including security-critical data, personal data and trade secrets; or
3. related to objective technical constraints, such as data format, volume, frequency, real-time versus delayed access, or the effort required to prepare certain data sets.

In any case, any distinction must be proportionate and aimed at legitimate interests, such as protecting innovations and trade secrets and ensuring a level playing field.[372]

185. The requirement that the fee be **reasonable** aims to ensure that the amount of the fee is not financially prohibitive and does not deter potential data recipients from using data.[373]

186. **Incremental** refers to the additional costs incurred by the data holder as a result of a request to provide data access to a data recipient, falling outside the data holder's existing normal business activities.

187. **Proportionate** means that the fee must be proportional to the purpose of making the data available. The data holder is expected to define the various cost categories in a comparable and verifiable manner.[374]

188. The costs of making data available will vary depending on the volume of the data and the agreements made to make it available. In most cases, these are one-time costs, such as those associated with onboarding or negotiating contracts.[375] For regular or repeated transactions in a business relationship, costs can be reduced by making long-term arrangements, for instance by spreading them using a subscription model or smart contracts. Costs not incurred for a single specific request should not be charged to a single data recipient.[376]

189. In addition to the eligible cost and investment items, the data holder and data recipient must also agree on how the fee will be paid. Payment can be made on a per-transaction basis, via a subscription model or through a hybrid model combining a base rate and variable charges.[377] For example, the base rate could cover integration and onboarding costs, while data usage could be priced based on volume, such as per API call, data set, user or device.[378] Reasonable compensation can also take a non-monetary form, such as access to services or mutual data sharing. The use of

[368] Article 9(3) of the Data Act. See also question 38 in the European Commission's FAQ. Furthermore, Article 9(6) of the Data Act explains that the Data Act does not prevent other European law, or national law adopted in accordance with European law, from prohibiting fees for data sharing or from stipulating lower fees.
[369] See also Section 12 of the European Commission's Draft Guidelines for Reasonable Compensation.
[370] See also Section 13 of the European Commission's Draft Guidelines for Reasonable Compensation.
[371] See also Section 14 of the European Commission's Draft Guidelines for Reasonable Compensation.
[372] See also Section 15 of the European Commission's Draft Guidelines for Reasonable Compensation.
[373] See also Section 16 of the European Commission's Draft Guidelines for Reasonable Compensation.
[374] *Ibid.*
[375] See also Section 36 of the European Commission's Draft Guidelines for Reasonable Compensation.
[376] Recital 47 of the Data Act. See also Sections 21 and 36 of the European Commission's Draft Guidelines for Reasonable Compensation.
[377] See also Sections 49 and 50 of the European Commission's Draft Guidelines for Reasonable Compensation.
[378] *Ibid.*

such forms of compensation should take into account that compensation must be non-discriminatory.[379]

5.5.2 Technical costs of making data available

184. First, it is worth noting that the costs associated with data sharing must be linked to a specific request to make data available, or shared with other requests.[380]

185. When making data available, the cost of **formatting** the data may be included in the compensation calculation. According to the regulation, data must be made available in a structured, commonly used and machine-readable format.[381] If the data holder stores data in an unusual format and converts it to another format to meet the obligations of the regulation, the cost of doing so should not be included in the calculation of the fee.[382] However, if the data recipient themselves requests a specific format that differs from the legal requirements, the cost of reformatting may be included.[383] Similarly, if the data recipient wishes to receive only a specific subset of the data that cannot be shared automatically via an API, the cost of selecting this subset may be included in the fee calculation.[384]

186. Costs arising from adjustments to protect data subjects, such as when anonymizing personal data, may be included in the fee calculation, provided that these costs are directly related to the specific request.[385]

187. **Electronic dissemination** costs include the costs incurred when sending data to the data recipient,[386] such as the cost of operating licensing or access tools (e.g. a secure web portal or API) or the personnel costs associated with requesting data access.[387] Onboarding costs, such as those associated with creating a user account for the data recipient or verification costs, may be included as well.[388]

188. **Storage** costs are costs incurred by the data holder for storing data in a dedicated IT system or cloud environment for the purpose of making it available to users or data recipients.[389] Only costs directly related to making data available to data recipients may be included in the fee.[390]

189. It is worth noting that the data holder does not always have to use the cheapest solution,[391] but is expected to consider the reasonable options available. While smart contracts or APIs may reduce costs, they are not always appropriate for all data holders or data recipients. Sometimes manual processes are required, resulting in higher costs. The data holder must therefore carefully assess what costs are necessary and what improvements to the cost structure are possible in order to keep the costs reasonable.[392]

190. When it comes to sharing data that contains trade secrets, the regulation strikes a balance between the basic obligations of the data holder and the additional measures resulting from the obligation to make the data available.[393] As explained in marginal 133, the data holder must identify what data is classified as a trade secret and make agreements about this with the data recipient. In

[379] See also Section 51 of the European Commission's Draft Guidelines for Reasonable Compensation.
[380] Recital 47 of the Data Act. See also Section 32 of the European Commission's Draft Guidelines for Reasonable Compensation.
[381] Articles 4(1) and 5(1) of the Data Act. See also Subsection 4.6 of these guidelines.
[382] See also Section 23 of the European Commission's Draft Guidelines for Reasonable Compensation.
[383] *Ibid.*
[384] See also Section 24 of the European Commission's Draft Guidelines for Reasonable Compensation.
[385] See also Section 25 of the European Commission's Draft Guidelines for Reasonable Compensation.
[386] See also Section 29 of the European Commission's Draft Guidelines for Reasonable Compensation.
[387] *Ibid.*
[388] See also Section 30 of the European Commission's Draft Guidelines for Reasonable Compensation.
[389] See also Section 31 of the European Commission's Draft Guidelines for Reasonable Compensation.
[390] *Ibid.*
[391] See also Section 35 of the European Commission's Draft Guidelines for Reasonable Compensation.
[392] *Ibid.*
[393] See also Section 27 of the European Commission's Draft Guidelines for Reasonable Compensation.

principle, the data holder may not include the costs of identifying and protecting trade secrets in the fee calculation.[394] In the event that data containing trade secrets is shared, the compensation for this may only cover measures that ensure the confidentiality of this data. The primary purpose of such measures is to ensure that data sharing does not result in the loss of trade secrets.[395]

191. If additional costs are incurred specifically as a result of providing individual access to data containing trade secrets, these costs may be included in the fee calculation.[396] This may include the costs of:[397]
1. negotiating a contract for access to data containing trade secrets;
2. drafting an individual liability or confidentiality agreement specific to the request for trade secret data;
3. audits to verify the data recipient's compliance with protective measures for trade secrets;
4. implementing recipient-specific measures to protect trade secrets, such as access controls and encryption; and
5. engaging a neutral, trusted intermediary to manage data containing trade secrets.

5.5.3 Investments in data collection and production

192. In calculating the fee, the data holder may take into account the investments made to **collect** existing data. This includes investments to obtain, compile or look up existing data, such as:[398]
1. moving data from its original source to the data holder's IT system;
2. developing and deploying the IT systems needed to receive and organize the data;
3. the equipment or services hosting the data, such as servers, including operational costs such as electricity, security and maintenance;
4. tools that automate data collection.

It does not include investments aimed at creating new data or curating, preparing or making data available to others.[399]

193. Investments made in order to **produce** the original data may also be included in the fee calculation. This includes investments for:[400]
1. deploying and operating physical instruments, such as cameras, sensors and meters;
2. the use of virtual technologies for data generation, such as web forms, surveys, simulations and digital twins;
3. the infrastructure or environments needed to create or record new data, such as new sensors or storage systems.

Activities aimed at preparing or making data available to others, such as cleansing or anonymizing data, or setting up APIs or access controls,[401] are not included.

194. For all non-recurring cost and investment items (start-up and overhead costs), it is necessary to calculate the reasonable share for each individual data recipient.[402] The European Commission states that several strategies are conceivable for this. For example, data holders can:[403]

1. define reasonable depreciation cycles, linked, for instance, to the useful life of technical equipment;

[394] See also Section 26 of the European Commission's Draft Guidelines for Reasonable Compensation.
[395] *Ibid.*
[396] See also Section 27 of the European Commission's Draft Guidelines for Reasonable Compensation.
[397] *Ibid.*
[398] See also Section 38 of the European Commission's Draft Guidelines for Reasonable Compensation.
[399] *Ibid.*
[400] See also Section 39 of the European Commission's Draft Guidelines for Reasonable Compensation.
[401] *Ibid.*
[402] See also Section 47 of the European Commission's Draft Guidelines for Reasonable Compensation.
[403] See also Section 48 of the European Commission's Draft Guidelines for Reasonable Compensation.

2. calculate the pro-rata share based on a conservative estimate of the number of potential data recipients. If start-up and overhead costs are amortized earlier than expected, this must affect the future calculation of compensation;
3. periodically adjust fees (e.g. on an annual basis) in a way that ensures clear pro-rata cost allocation and avoids discriminatory pricing over time.[404]

5.5.4 Including a margin

195. The fee may also include a margin.[405] This margin may vary depending on factors such as the volume, format or nature of the data.[406] The margin can also be based on the investments made to facilitate data collection.[407] If the data holder has been able to collect the data as a result of significant investments, including for the purpose of its own operations, a higher margin may be justified.[408] If such investments were more modest, this should be reflected in a lower margin.[409] In some cases, the margin may be limited or even excluded entirely, such as when the data recipient's use of the data does not affect the data holder's own activities.[410] The data holder should carefully consider the above when setting its margins.[411]

196. To calculate the margin, the data holder may only request information about the data recipient's intended use of the data to assess whether its own activities are affected.[412] For example, the data holder may ask the data recipient to explain whether the use will compete with, substitute for, or interfere with its own activities. This allows the data holder to determine whether a margin is justified, or if it should be reduced or eliminated. The regulation also explains, perhaps superfluously, that information that is not relevant to the margin calculation, such as the data recipient's commercial plans or profit expectations, may not be requested to justify a higher margin.[413]

197. Investments in data collection and production should generally be taken into account when calculating a reasonable margin, including investments made by the data holder for its own purposes.[414] However, there are situations in which investments may not be taken into account (in whole or in part), such as when:[415]
    1. the investments are amortized or already covered by another source of revenue, such as the purchase price of a related product or service;
    2. the data holder collects the data for its own purposes and uses it itself. If this is the case, the margin must be reduced. However, in situations where the data holder does not use the data itself and invests solely to enable additional data collection and production functionalities, these investments may be included in the margin.

    In addition, if a connected product is operated by the user, the operational costs are not considered investments in data collection or generation, as these costs are borne by the user.[416]

[404] It should be noted here that periodic adjustments may result in a "first-mover disadvantage" if early data recipients are charged disproportionately higher amounts than later data recipients. This would violate the non-discrimination principle. Data holders must therefore ensure that any adjustments are applied consistently and transparently. See also Section 48 of the European Commission's Draft Guidelines for Reasonable Compensation.
[405] Article 9(1) of the Data Act. See also Sections 10 and 11 of the European Commission's Draft Guidelines for Reasonable Compensation.
[406] Recital 47 of the Data Act.
[407] *Ibid.*
[408] Recital 47 of the Data Act. See also Sections 41 and 43 of the European Commission's Draft Guidelines for Reasonable Compensation.
[409] *Ibid.*
[410] Recital 47 of the Data Act. See also Section 41 of the European Commission's Draft Guidelines for Reasonable Compensation.
[411] Recital 47 of the Data Act.
[412] See also Section 42 of the European Commission's Draft Guidelines for Reasonable Compensation.
[413] *Ibid.*
[414] See also Section 43 of the European Commission's Draft Guidelines for Reasonable Compensation.
[415] *Ibid.*
[416] Recital 68 of the Data Act. See also Section 43 of the European Commission's Draft Guidelines for Reasonable Compensation.

198. For micro and small enterprises[417] or non-profit research organizations, only the costs described in marginal 183(1) may be included in the fee calculation.[418] This means that the fees they can receive as data recipients are lower. These fees may not include a margin and should only cover costs directly related to individual requests, with the understanding that the data holder will need to set up the necessary technical interfaces, associated software and connectivity, and that these must remain in place permanently.[419] This exception does not apply to data recipients with partner enterprises or affiliated enterprises that do not qualify as micro or small enterprises.[420]

5.5.5 Transparency requirements

199. The data holder must be able to provide the data recipient with sufficiently detailed information on how the fee was calculated, allowing the data recipient to assess whether the fee is reasonable.[421] Unlike the disclosure obligations discussed in Section 3 of these guidelines, this is not a general transparency requirement; therefore, the information only needs to be provided upon the data recipient's request.[422]

200. Confidential information, such as cost items that are protected by non-disclosure agreements or those that qualify as trade secrets, does not need to be fully shared with the data recipient.[423] The data holder must strike a balance between transparency and protecting sensitive information. Possible solutions include the use of summaries, standard templates with sample calculations or additional confidentiality statements.[424]

201. The European Commission recommends that data holders publicly disclose cost categories early before discussing them in more detail during pre-contractual negotiations.[425] To comply with the transparency requirement, the data holder is expected to document relevant choices and decisions related to cost calculation, both for general situations and individual requests.[426]

202. If the data recipient is a micro or small enterprise, or a non-profit research organization, the information provided must clearly show that the fee does not exceed the costs directly associated with making the data available to that recipient and attributable to the individual request.[427]

5.6 Standard contracts

190. The European Commission has developed and recommended model contractual terms (MCTs) to assist relevant parties in implementing the above requirements.[428] For now, only an English-language draft version of this document is available. This means that it still needs to be adopted by the European Parliament before it becomes final. The European Commission has indicated that it will

[417] Footnote 31 explains when a company qualifies as a micro or small enterprise.
[418] Article 9(4) of the Data Act. See also recital 49 of the Data Act, question 39 in the European Commission's FAQ and Section 9 of the European Commission's Draft Guidelines for Reasonable Compensation.
[419] Recital 49 of the Data Act. See also Section 45 of the European Commission's Draft Guidelines for Reasonable Compensation.
[420] Article 9(4) of the Data Act. See also Section 44 of the European Commission's Draft Guidelines for Reasonable Compensation.
[421] Article 9(7) of the Data Act. See also recital 51 of the Data Act.
[422] See also Section 52 of the European Commission's Draft Guidelines for Reasonable Compensation. Please note that if the data holder and the data recipient are potential or actual competitors, the Dutch Competition Act must be taken into account when the data holder provides cost data. For more information, see also Section 56 of the European Commission's Draft Guidelines for Reasonable Compensation.
[423] See also Section 55 of the European Commission's Draft Guidelines for Reasonable Compensation.
[424] *Ibid.*
[425] See also Section 53 of the European Commission's Draft Guidelines for Reasonable Compensation.
[426] See also Section 54 of the European Commission's Draft Guidelines for Reasonable Compensation.
[427] Article 9(7) of the Data Act. See also recital 49 and 51 of the Data Act and Section 46 of the European Commission's Draft Guidelines for Reasonable Compensation.
[428] Article 41 of the Data Act. See also European Commission, *Draft Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts*, available at https://digital-strategy.ec.europa.eu/en/library/draft-recommendation-non-binding-model-contractual-terms-data-access-and-use-and-non-binding. Please note that this is a draft version, which has yet to be adopted by the European Parliament.

publish the MCTs in all official EU languages following adoption. The MCTs are intended as a tool, and their use is not mandatory under the Data Act.[429]

191. The MCTs provide templates and guidelines and are designed to ensure fair, reasonable and non-discriminatory contractual rights and obligations, including the protection of trade secrets. Parties may use the MCTs in mutual consultation to align an agreement for the purchase, rental or lease of a connected product, or for the provision of a related service, with the Data Act.[430]

192. The MCTs may be used by the manufacturer of a connected product and related service to draft contracts for business users, but they may also be applicable in contractual relationships with users who are consumers. In the latter case, the MCTs must be amended to align with consumer protection regulations.

193. The MCTs are modular, meaning that parties can choose to use either the entire set or only certain components. Parties may choose to use the MCTs as the sole basis for their agreements, or to insert them into the pre-established contractual frameworks that they normally use. In addition to the provisions, the European Commission has also provided instructions and explanations regarding which MCTs require attention when modifying them and integrating them into contracts. The European Commission has developed multiple versions of certain provisions to ensure their applicability in different types of commercial relationships.

194. There will be four different sets of MCTs, which can be applied in different types of commercial relationships:

- *Set 1: data holder – user*
  This set of MCTs is designed for contracts between the data holder and a user of a connected product or related service, where the data holder wants to use data generated through the use of the product or service.

- *Set 2: user – data recipient*
  This set of MCTs is designed for contracts between a user of a connected product or related service and a data recipient, where the user requests that the data holder make data available to the data recipient under Article 5 of the Data Act.

- *Set 3: data holder – data recipient*
  This set of MCTs is designed for contracts between the data holder and a data recipient, where the Data Act requires the data holder to make data available to a data recipient when requested by a user of a connected product or related service.[431] The same set can be used, with certain modifications, if data sharing is required by other European or national legislation.

- *Set 4: "voluntary" data sharing between a data sharer and a company*
  This set of MCTs is designed for contracts between data sharers and data recipients, where the data sharer, voluntarily and independently of any request from a user or similar party, makes data available to a data recipients. In this context, "voluntary" means that the contractual relationship is not established through a user request, but rather based on a commercial interest between the data sharer and data recipient. For this set of MCTs, the European Commission has chosen to deviate from the definitions of parties used in the Data Act, opting instead to use the term "data sharer" to cover all possible scenarios.

[429] Annexes I through IV of the "Final Report of the Expert Group on B2B data sharing and cloud computing contracts" (April 2, 2025).
[430] In addition to the MCTs, the European Commission has also developed standard contractual clauses (SCCs) that can serve as a framework for contractual relationships between business customers and providers of data processing services (cloud services). Because the SCCs are not focused on sharing data from connected products or related services, they are beyond the scope of these guidelines.
[431] These are requests as described in Article 5 of the Data Act.