Countdown to the Data Act: 15 Key Points on the Regulation on Harmonized Rules on Fair Access to and Use of Data

October 10, 2024

The Regulation (EU) 2023/2854 on harmonized rules for fair access to and use of data, the so-called Data Act (available here), is an important part of the EU's digital strategy, aiming to establish the foundation for a data-driven future in the EU. The purpose of the Data Act is to create clear rules for access to and use of data. At its core, it seeks to promote free flow of data within the internal market, support innovative business models, and ensure privacy and data security. The impact of the Data Act is far-reaching, affecting numerous sectors. Given the complexity and novelty of the Data Act, a clear understanding of its various aspects is crucial. This Q&A will answer key questions surrounding the Data Act.

1. **As of which date the Data Act must be complied with?**

   The Data Act entered into force on 11 January 2024. According to Art. 50 (2) Data Act, most of its provisions are applicable as of **12 September 2025**.

2. **What are the main regulatory areas of the Data Act?**

   The Data Act is characterised by the following distinct and partially non-interconnected regulatory areas:

   - Data access rights
   - Unfair contractual terms between businesses
   - Switching between data processing services/ providers
   - Minimum requirements for data interoperability

3. **To which companies does the Data Act apply to?**

   The different regulatory areas of the Data Act apply to the following businesses:

   a) The Data Act requires **manufacturers** of **connected products** and **providers** of **related services** to make data available.

   A **connected product** is an item that obtains, generates, or collects data about its use or environment and can transmit that data. This includes, for example, IoT devices such as smart cars, wearables, smartphones, virtual voice assistants, intelligent security systems, or navigation systems.

   A **related service** is a digital service connected to the product in such a way that the connected product could not perform one or more of its functions without it, or that is subsequently connected to the product by the manufacturer or a third party to add to,

update, or adapt the functions of the connected product. Such related services can include auxiliary consulting, analytics or financial services, or regular repair and maintenance services.

b) The Data Act also applies to **data holders** (regardless of where they are established), who provide data to data recipients within the EU.

A data holder is defined as a natural or legal person entitled or obliged under the Data Act, applicable EU law, or national legislation adopted in accordance with EU law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service.

c) Additionally, companies that conclude data access agreements with other companies, as well as providers of data processing services and participants in European data spaces, fall within the scope of the Data Act.

4. Does the Data Act apply to companies based outside the EU?

The scope of the Data Act is broad and follows the “market location principle”. The decisive factor is therefore the location where the connected product is placed on the market. Accordingly, the Data Act may also apply to companies that are not established within the EU. These include companies that manufacture connected products that are placed on the market in the EU, as well as companies that offer connected services in the EU.

5. Does the Data Act also apply to small and medium-sized enterprises (SMEs)?

The Data Act also applies to small and medium-sized enterprises (SMEs) but contains certain exemptions for micro and small enterprises, i.e., companies with fewer than 50 employees and a maximum annual turnover of EUR 10 million. These exemptions include:

- The obligation to provide product data or related service data to users or third parties does not apply if the connected product was manufactured or designed by a micro or small enterprise, or if such a company provides the related services. This exemption, set out in Art. 7 (1) Data Act, does not apply if the micro or small enterprise has a partner enterprise or linked enterprise that is not a micro or small enterprise or if the micro or small enterprise is subcontracted to manufacture or design a connected product or provide the related service.
- For medium-sized enterprises (fewer than 250 employees and max. EUR 50 million annual turnover), the obligation to provide data applies without

exception, but not until one year after (i) the connected product is placed on the market or (ii) a company exceeds the thresholds of a medium-sized enterprise.

- Micro and small enterprises also benefit from privileges concerning the obligation to provide data to public sector bodies in cases of exceptional need. If they are supposed to make data available, stricter requirements for the exceptional need are to be applied based on Art. 15 (2) Data Act. Additionally, Art. 20 (1) Data Act grants them the right to financial compensation for providing data, even in cases where larger companies are required to provide the data free of charge.

6. What data access rights do users have under the Data Act?

The Data Act regulates access to data from connected products or related services. The basic premise is that users should be granted access to all data that they have contributed to generating. Users should be able to see how their data is used by the data holder and also to decide whether to share this data with third parties. Three different – legally enforceable – access rights can be distinguished:

First scenario: Art. 3 Data Act requires data holders to design and manufacture connected products in such a manner that users have direct access to product data and related service data. Where direct access is not possible, data holders are required by Art. 4 (1) Data Act to provide the data immediately, free of charge, in a machine-readable format, continuously and in real time.

Second scenario: Furthermore, Art. 5 (1) Data Act obliges data holders, upon the user's request, to provide data to a third party. Data may also be provided to a competitor of the data holder. However, if the competitor is designated as a gatekeeper under Art. 3 Digital Markets Act (DMA), the data does not need be provided.

Third scenario: A third access right is regulated in Art. 14 Data Act. Data holders are obliged to provide data to public sector bodies if they can demonstrate that there is an exceptional need for these data in order to fulfil their legal tasks in the public interest. This access right is particularly relevant in cases where the requested data are required to address a public emergency and cannot be obtained in a timely and effective manner by other means.

7. What data is covered by the access rights under the Data Act?

Users can request the provision of all product data or related service data that are readily available. According to Art. 1 (2) Data Act, both personal and non-personal data within the meaning of the General Data Protection Regulation (GDPR) are covered by its scope. The right also includes data consciously recorded by the users, data generated in connection with the use of the connected product, but also data that is generated without the user's intervention or when the product is switched off.

8. Can the data holder request compensation for providing data?

The right to compensation depends on the data recipient:

- The provision of data **to users** must always be free of charge.
- The provision of data **to a third party** who is not a user of the connected product or related service is governed by Art. 9 Data Act. Compensation may be requested in B2B-relations. Such compensation must be non-discriminatory and reasonable and may include a margin, provided the data recipient is not a small or medium-sized enterprise. The compensation should take into account the costs incurred in providing the data and investments in data collection and generation. If the third party is not a business, it remains unclear whether compensation can be requested, as the Data Act does not explicitly address this situation.

9. What obligations do data recipients have?

A data recipient, as defined in Art. 2 (14) Data Act, is a third party to whom product data or related service data is provided at the user's request. Art. 6 Data Act regulates specific obligations for data recipients:

- Data recipients may only use the data provided for the purposes and under the conditions agreed with the users. Generally, the data must be deleted once it is no longer required for the agreed purpose. If personal data is involved, the provisions of the GDPR must also be complied with.
- Data recipients may not share the data provided to them with a third party without the user's consent.
- Data recipients may not use the provided data to develop a product that competes with the connected product from which the data originate or share the data for this purpose.
- Data recipients may not prevent users who are consumers from making the received data available to another party.

10. Can data holders provide personal data to users?

With regard to personal data, the fields of application of the Data Act and the GDPR do overlap. The GDPR contains a ban with reservation of permission: the processing of personal data is prohibited unless it is based on a legal ground under Art. 6 (1) GDPR or Art. 9 (2) GDPR. Providing personal data to users or a third party constitutes data processing under the GDPR and is thus only permissible if covered by a legal ground. Whether such a legal basis exists in a particular case depends primarily on whether the users are also data subjects within the meaning of Art. 4 (1) GDPR:

- **Users are also data subjects within the meaning of the GDPR**: In this first scenario, the requested personal data are the users' "own" data. In this case, the data access request under Art. 4 (1) Data Act or Art. 5 (1) Data Act can also be seen as consent to data processing under data protection law.
- **Users are not simultaneously data subjects within the meaning of the GDPR**: More problematic is the scenario in which the users are not also data subjects within the meaning of the GDPR. This may be the case, for example, when a vehicle is used by several people – for example in car sharing. In such cases, the provision of personal data is only possible if all data subjects have given their consent to the disclosure under data protection law, if there is a contractual necessity for the disclosure or if there is a necessity to protect legitimate interests.

11. Must data also be provided if trade secrets are disclosed through the provision of data?

In principle, all data must be disclosed — including those containing trade secrets. However, the data holder may agree with the users on technical and organisational measures to protect the confidentiality of the trade secrets, particularly with regard to third parties. Such measures may include, for example, the use of model contractual terms, confidentiality agreements, and strict access protocols. In exceptional cases, the provision of data may be refused if no agreement on the necessary measures for the protection of trade secrets is reached between the data holder and the users or if the users fail to implement these measures. Furthermore, the provision of data may be refused if the data holder is likely to suffer significant economic damage from the disclosure, despite the technical and organisational measures taken. In both cases, the data holder must justify the decision, inform the users promptly in writing, and notify the competent supervisory authority.

12. Can users' data access rights be contractually waived?

No. Based on section 7 (2) Data Act, any contractual clauses that restrict or exclude data access claims – beyond the limits set out in the Data Act – to the detriment of users are not binding. Thus, a case-by-case examination of existing contracts is

required to determine whether a claim for access can be rejected, for example, on the grounds of the need to protect trade secrets.

13. Two companies enter into a contract for data access and use. What requirements must be taken into account when drafting the contract?

If a data holder is obliged to provide data to another company, the following aspects must be considered when drafting the data provision agreement:

- For B2B-contracts that include data and are unilaterally imposed, an abuse control is required, see Chapter IV Data Act.
- Additionally, certain data-sharing agreements must comply with the FRAND-principles under Art. 8 (1) Data Act. These principles ensure that the provision of data is done under fair, reasonable, non-discriminatory conditions and in a transparent manner to prevent contractual imbalances.

14. What provisions does the Data Act contain regarding switching between data processing services?

The conditions for switching between data processing services must pursuant to Art. 25 (1) Data Act be set out in writing and provided in a storable and reproducible format before the contract is signed. Furthermore, several specific requirements for switching conditions must be fulfilled. For example, the termination period must not exceed two months. Additionally, any fees for switching between services must be gradually eliminated.

15. What sanctions does the Data Act provide for in response to violations?

Art. 40 Data Act obliges the Member States to establish rules on sanctions to be imposed in case of violations of the Data Act and to take all necessary measures to ensure the enforcement of these sanctions. The sanctions must be effective, proportionate, and dissuasive and are essentially aligned with the fines of the GDPR of up to 4% of the worldwide annual turnover.