# The European Data Act: Update 2024

*Antonia Herfurth, LL.M. (Göttingen), attorney at law in Munich and Hanover*

*February 2024*

The Data Act came into force on 22 December 2023. It will be directly applicable throughout the EU from 12 September 2025. Compared to the draft legislation from February 2022 (HP Compact "The European Data Act", April 2022), the final version also contains important changes for small and medium-sized enterprises. This Compact provides an updated overview of the new provisions of the Data Act.

**Aim of the Data Act**

The aim of the Data Act is to distribute the value of data fairly among the players in the data economy. To this end, it stipulates fair access and fair use of data as well as data portability and interoperability between different service providers. This is intended to prevent the concentration of data in the hands of a few companies with market power and to promote competition. Users should be given more control over the data they generate and the public sector should have access to data that is necessary to overcome political and social challenges, such as the Covid pandemic.

**Data users and data owners**

The Data Act defines a "user" as a natural or legal person who owns, rents or leases a networked product or utilises a service. The status of "data user" is linked to the contractual relationship with the device.

"Data holder" is the legal or natural person who is legally authorised or obliged to provide certain data or, in the case of non-personal data, is able to do so by controlling the technical design of the product and the associated services. In simple terms: The data holder is the person who has de facto technical control over the data.

The Data Act therefore assumes that data is not in the hands of the user, i.e. in the hands of the data producer, but in the hands of the company processing the data.

**Data access and use**

For this reason, the draft law creates a right to access and to use data in favour of data-generating users.

Products and services should be designed in such a way that users have access to the data they generate, simply, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, directly. If the user does not have direct access, the data holder must grant him access upon request without undue delay, free of charge and, where

appropriate, continuously and in real time. If the networked product is subject to statutory security requirements that are impaired by the disclosure of data, access, use and the re-disclosure of data may be contractually restricted.

In addition, the Data Act stipulates information obligations towards the user before the user purchases, rents or leases the data-generating product or service. For example, he must be informed about:

- nature and scope of the data generated by the product,
- whether data is generated continuously and in real time,
- access options of the user to the data,
- whether the manufacturer or service provider intends to use the data itself or authorise a third party to do so, and if so, for what purposes,
- identity and contact details of the data holder.

At the request of the data user, the data holder must share his data with third parties. These so-called data recipients may only process the data for the purposes and under the conditions agreed with the user. If the data holder is obliged to make data accessible to a data recipient, he must do so under fair, reasonable and non-discriminatory conditions and in a transparent manner. Any remuneration must be appropriate.

If the data holder and data recipient cannot agree on a fair data usage agreement, the Data Act provides for dispute resolution bodies. Data holders may not provide non-personal product data to third parties for any commercial or non-commercial purposes other than to fulfil their contract with the user. Where applicable, third parties are contractually obliged by data holders not to disclose the data received from them again.

The right to data access should not be asserted against small and micro-enterprises.

**Prohibition of unfair contract clauses**

The Data Act stipulates that unfair clauses in data usage agreements that are unilaterally imposed on a company are not binding on it. Unlike in the old draft of the Data Act, this regulation applies not only to small and medium-sized companies, but also regardless of the size of the company. In Article 13 of the Data Act, the EU has introduced a so-called *unfairness test.* This states that a contractual clause is unfair if it grossly deviates from good commercial practice or is contrary to good faith. This general rule is supplemented by a list of clauses that are considered unfair in particular and an exhaustive list of clauses that are considered unfair. In addition, the European Commission is to develop non-binding standard contractual clauses that the parties can use, similar to the Standard Contractual Clauses in data protection law.

**Data portability**

It is common for providers of data processing services to prevent customers from switching to a competing service provider by, for example, imposing long cancellation periods or making data portability more difficult. By making the switch as cumbersome as possible, customers are tied to the existing provider, the so-called lock-in effect. The Data Act provides that customers can switch from one data processing service to another data processing service that includes the same type of service without being hindered by commercial, technical, contractual and organisational measures.

The customer's rights must be set out in a written contract. As a minimum, the contract must stipulate that the customer has the right to switch providers within 30 days. The provider must support the customer during the change and continue to provide its services without restriction. During the switch, the provider must ensure a high level of data security, especially during the transfer and subsequent retrieval period. In addition, the provider must list all categories of data and digital assets that can be transferred during the switching process, including at least all exportable data. This includes, in particular, security settings, access rights and access logs to the service. If the service provider states that it is technically impossible to carry out a switch within 30 days, it must inform the customer of this within 14 days. The provider bears the burden of proof. The switch must be completed within seven months of the customer's request at the latest.

In the interests of a fair business relationship, the new legal text obliges all parties to act in good faith.

The service provider may not charge the user any costs for the change. This will be the case after a transition period of three years from the date of entry into force of the Data Act.

**Interoperability**

The Data Act sets out basic interoperability requirements for operators of data rooms and providers of data processing services. The draft legislation relates in particular to cloud computing. Uniform standards allow data to be exchanged more easily and mechanisms for sharing data to work better together. The Data Act also sets out basic requirements for *smart contracts.* These help the contracting parties to guarantee that the agreed data usage conditions are adhered to. The rules of data portability also apply to cloud computing and edge computing providers; in particular, a change of service provider must be possible within 30 days and must not be made artificially difficult by the old providers.

**Data access due to exceptional circumstances**

Data owners must make data available to the public sector due to exceptional circumstances. Exceptional circumstances include, for example, public emergencies or where the lack of data prevents a public body from carrying out a task in the public interest and the data cannot be obtained in any other way. The new version of the Data Act contains an important innovation in this respect: the right to data provision now also applies to data holders who are small or micro-enterprises. If the data holder has incurred technical or organisational costs as a result of the provision, these are eligible for reimbursement. However, this does not apply to the provision of data by medium-sized and large companies in the event of a public emergency.

The public sector body may only use the data for the purpose specified by it. If the data is personal data, it must take technical and organisational measures to protect the data subject and destroy the data as soon as it is no longer necessary for the purpose for which it was collected. In the case of business secrets, the public sector body should only request them as a last resort and only to the minimum extent. In doing so, it must take appropriate measures to ensure the confidentiality of the business secret. Access to data may be refused in individual cases if the disclosure of a trade secret would very likely lead to serious economic damage despite the protective measures provided.

**International protection of non-personal data**

Data processing services should not disclose or grant access to non-personal data to third countries if this would result in a conflict with EU law or the national law of the Member State concerned. If the request is based on the decision of a court or authority and on an international treaty, the decision should be recognised and enforced. If it is not based on an international treaty, the request should only be honoured in exceptional cases, e.g. for the purposes of criminal prosecution.

**Conclusion**

With the Data Act, the European legislator has introduced a further measure that weakens the de facto control of monopolistic data holders and strengthens the position of data-generating users. The regulatory measures of recent years show that the EU wants to break up the current one-sided structures of the data market and thus create opportunities for innovation and competition in the data economy. In connection with data rights, there have been discussions about the introduction of data ownership, which the EU has not honoured in the Data Act. Instead, there appears to be a shift towards *data sharing*, meaning that the EU is more concerned with data sovereignty.

It remains to be seen how the Data Act will establish itself in practice. For example, there are no rules on how to deal with overlapping rights to use data. It is quite conceivable that everyone should be able to use the data they need to provide their services, for

example, a car repair shop should have access to the data it needs to repair a car.

+ + +

## The Alliuris Group

The Alliuris Group consists of 20 law firms and 400 business lawyers within Europe, Asia and America.

| | |
|---|---|
| *Contact* | Alisha Daley-Stehr<br>Alliuris Communication |
| *Web* | www.alliuris.law |
| *Mail* | info@alliuris.org |
| *Fon* | +49-511-307 56-20 |
| *Fax* | +49-511-307 56-21 |

## Alliuris in Germany

| | |
|---|---|
| *Firm* | Herfurth & Partner<br>Luisentraße 5, D-30159 Hanover |
| *Web* | www.herfurth.de |
| *Fon* | + 49 511 30756 0 |
| *Fax* | + 49 511 30756 10 |
| *Mob* | |
| *Contact* | Ulrich Herfurth, Partner |
| *Language* | German, English, French, Spanish, Portuguese, Russian, Mandarin, Czech, Polish |
| *Mail* | info@herfurth.de |

IMPRINT

EDITORS: ALLIURIS A.S.B.L. ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS | BRUSSELS

MANAGEMENT: Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-20, Fax +49-511-307 56-21

BRUSSELS · PARIS · LONDON · AMERSFOORT · UTRECHT · KNOKKE · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · SALZBURG · MOSCOW MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI · GUANGZHOU NEW DELHI · MUMBAY · NEW YORK · MEXICO CITY SAO PAULO · RIO DE JANEIRO · BRASILIA · BUENOS AIRES · LIMA

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt