The European Data Act

Antonia Herfurth, attorney at law, Munich/Hanover

April 2022

On February 23, 2022, the European Commission published the draft legislation for the Data Act. Together with the Data Governance Act, the Data Act forms a legislative package under the European Data Strategy. So far, only personal data has been in the focus of discussions, non-personal data is hardly regulated in the EU. The two new draft laws now regulate personal and non-personal data. Special about the Data Act is that it gives individuals and companies control over the non-personal data they generate.

Aim of the Data Act

Data are one of the most important economic goods of our time. In the absence of existing regulations for non-personal data, there is a lot of confusion about when data is generated, what data are generated and who holds the generated data. In addition, existing data are in the hands of a few powerful companies. Such concentration leads to a market imbalance that restricts competition and hinders data access and use by third parties.

The aim of the Data Act is to ensure a fair distribution of data value among the players in the data economy. To this end, it prescribes fair access and use of data, as well as data portability and interoperability between different service providers. In this way, data monopolies and lock-in effects are to be dissolved. Users should have more control over the data they generate, and the public sector should have access to data needed to address political and societal challenges, such as the Corona pandemic.

Data users and data holders

The Data Act defines a "user" as a natural or legal person who owns, rents or leases a product or uses 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 entitled or obliged to provide certain data, or in the case of non-personal data and through control of the technical design of the product and related services, is able to do so. Phrased simply: The data holder is the one who has de facto technical control over the data.

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

Data access and data use

For this reason, the draft law creates a right to data access and use 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, easily, securely and, where necessary and appropriate, directly. If the user does not have direct access, the data holder must grant him access on request without delay, free of charge and, if necessary, continuously and in real time.

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

- the nature and extent of the data generated by the product,
- whether data is generated continuously and in real time,
- how the user can access the data,
- whether the manufacturer or service provider intends to use the data itself or to allow a third party to do so, and if so, for what purposes,
- the 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. Data must be deleted when it is no longer needed for the agreed purpose. If the data holder is obliged to make data available to a data recipient, he must do so under fair, reasonable and non-discriminatory conditions and in a transparent manner. Any remuneration must be reasonable. If the data holder and the data recipient cannot agree on a fair data use contract, the Data Act provides for dispute resolution bodies.

The right to data access shall not be enforced against small and micro enterprises.

Prohibition of unfair contractual terms

The Data Act stipulates that unfair terms in data use agreements that are unilaterally imposed on a medium, small or micro enterprise are not binding on them. Such clauses are usually not the result of balanced contractual negotiations, but the consequence of take-it-or-leave-it situations. In Article 13 of the Data Act, the EU has introduced an *unfairness test*. According to this, a contractual term is unfair if it deviates grossly from good commercial practice and is thus contrary to good faith and morality. This general rule is supplemented by a list of terms which are always unfair and a list of terms which are presumed to be unfair, i.e. which are deemed to be unfair. In addition, the European Commission is to develop non-binding model contract clauses which the parties can use, similar to the standard contractual clauses under the General Data Protection Regulation.

Data portability

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

The rights of the customer must be specified in a written contract. As a minimum, the contract must state that the customer has the right to change provider within 30 days. The provider must support the customer in switching and continue to provide unrestricted services. The provider must also provide a full specification of all data that will be exported during the switching process. This includes all data imported by the customer at the beginning of the service contract and all data generated by the customer and by the use of the service during the contract period. This includes, in particular, security settings, access rights and access logs to the service. If the service provider

states that a change within 30 days is technically not possible, he must inform the customer within seven days. The provider bears the burden of proof. The switch must be completed within six months of the customer's request at the latest.
The service provider may not charge the user for the change. This applies after a transitional period of three years after the Data Act comes into force.

Interoperability

In addition, the Data Act lays down basic interoperability requirements for operators of data rooms and providers of data processing services. Here, the draft law refers in particular to cloud computing and edge computing providers. Uniform standards will enable data to be exchanged more effectively and mechanisms for data sharing 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 use conditions are adhered to.
For cloud and edge computing providers, the rules of data portability also apply; in particular, a change of service provider must be possible within 30 days and must not be artificially impeded by legacy providers.

Data access due to exceptional circumstances

Data holders must make data available to the public sector due to exceptional circumstances. Exceptional circumstances are, for example, public emergencies or if the lack of data prevents a public institution from fulfilling a task in the public interest and the data cannot be obtained in any other way. If the data holder has incurred technical or organisational costs as a result of the provision of the data, these costs shall be reimbursable.
The public institution may use the data only for the purpose stated 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 fulfilment of the purpose. In the case of trade secrets, the public institution should only request them as a last resort and only to a limited extent. In doing so, it must take reasonable measures to ensure the confidentiality of the trade secret.
The right to access data should not be asserted against data holders who are small or micro enterprises.

Safeguards for non-personal data in international contexts

Data processing services shall not disclose or provide access to non-personal data to third countries if this would create a conflict with Union law or the national law of the Member State concerned. If the request is based on the decision of a court or an authority and on an international treaty, the decision shall be recognised and enforced. If it is not based on an international treaty, the request should only be complied with in exceptional cases, for example 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 the context of rights in data, there have been discussions about the introduction of data ownership, which the EU has not followed up on in the Data Act. Rather, a shift towards data sharing seems to be taking place, i.e. the EU is more concerned with data sovereignty.
It remains to be seen how the Data Act will develop and establish itself in practice. For example, there are no rules on how to deal with overlapping rights to use data. It is conceivable that everyone should be able to use the data they need to fulfil their services, for example, a garage should be able to use the data it needs to repair a vehicle.

The Data Act will presumably not come into force before 2023.

+ + +

alliuris

ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

Alliuris Publications

Please find more information about the legal framework for technology under

www.alliuris.law
www.alliuris.org/profile/publications

among others:

- Artificial Intelligence and Law
- Artificial Intelligence in Europe
- Data Protection in the USA
- Data Protection in Brazil
- Data Protection in China
- IT Security Management
- IT Security under ISO 27001
- IT Security Basic Protection BSI

The Alliuris Group

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

Contact	Alisha Daley-Stehr, Alliuris Communication
Web	www.alliuris.law
Mail	info@alliuris.org
Fon	++-(0) 511-307 56-20
Fax	++-(0) 511-307 56-21

Alliuris in Germany

Firm	Herfurth & Partner Luisenstraße 5 DE-30159 Hanover
Web	www.herfurth.de
Fon	++-(0) 511-307 56-0
Fax	++-(0) 511-307 56-10
Mob	++-
Contact	Ulrich Herfurth, Managing Partner
Language	German, English
Mail	herfurth@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