

## Introduction

The rapid growth of connected devices in the European market has led to an increase in data generation, offering significant potential for innovation and competitiveness in the EU. Responding to this, the European Commission (EC) came forward with its policy recommendation to harmonise rules on fair access to and use of data. The Data Act entered into force on 11 January 2024, after lengthy EU-level negotiations. The Data Act will become applicable on 12 September 2025, except for certain provisions that will be implemented at a later date.

The act aligns with the EU's [Digital Decade](#)'s goal of advancing digital transformation, and it is the second main legislative initiative of the [European Strategy For Data](#) of February 2020. The Data Act is closely interlinked with the [Data Governance Act](#). While the Data Governance Act creates the processes and structures to facilitate data sharing by companies, individuals and the public sector, the EU Data Act clarifies who can create value from data and under which conditions. Together, these acts will facilitate reliable and secure access to data, fostering its use in key economic sectors and areas of public interest.

Furthermore, the Data Act does not override the [General Data Protection Regulation](#) (GDPR) or the [ePrivacy Directive 2002/58](#), respecting the powers of supervisory authorities and the rights of data subjects. In case of conflict, the law on protection of personal data or privacy will prevail.

It is anticipated that the Data Act will significantly impact EU businesses, requiring thorough preparation. This client alert reviews and analyses the Data Act Regulation as adopted, emphasising its importance in future EU policy discussions. If the Data Act is of relevance for your organisation, please do not hesitate to reach out to us.

## The European Data Act

The Data Act aims to promote data access and data use while ensuring fair value distribution of data in the digital economy by specifying who can create value from data and under what conditions. The Data Act seeks to achieve those objectives through its broad scope and new, harmonised rules across the EU.

Regarding its scope, most of the provisions of the Data Act will apply to data holders, like manufacturers of connected products and service providers placing products or services on the EU market. It also encompasses data holders making data accessible to EU data recipients, regardless of their location. However, provisions on data sharing specifically pertain to users within the EU.

Regarding the new rules, the Data Act **provides users of connected products with access to the data generated by these devices**, fostering consumer control and boosting aftermarket services and innovation. **Public sector bodies will be able to access private sector data** for public emergency response and legal mandates. The act also **protects European businesses against unfair contractual terms**, enabling **small and medium-sized enterprises** (SMEs) to participate more actively in the data market. Additionally, it will allow **seamless switching between data processing service providers**, promoting competition and choice on the market while preventing vendor lock-in. The new act also includes **safeguards against unlawful requests** for access of nonpersonal data held in the EU, contributing to a reliable and secure data environment. Finally, the Data Act introduces measures to promote the development of **interoperability standards** for data-sharing and for data processing services, in line with the EU [Standardisation Strategy](#).

### 1. Users of Connected Devices Can Gain Access to Data Generated by Them

The Data Act sets out new rules that enable users of connected products to access the data generated by these devices and to share such data with third parties.

In particular, where the user cannot directly access data generated by the use of products, the data holder shall make such data available to the user. This should be done without undue delay, free of charge and, where applicable, continuously and in real time. For example, the owner of a connected car or the operator of a wind turbine will be able to request the manufacturer to share certain data generated using these connected products with a repair service of the owner's choice. The proposal considers trade secrets in this context, provided that they shall only be disclosed if all specific necessary measures are taken to preserve their confidentiality.

This measure will give more control to consumers and to other users of connected products, and it will boost aftermarket services and innovation.

### 2. Data Access for Public Sector Bodies and EU Institutions

The Data Act establishes rules enabling public sector bodies and EU institutions, agencies and bodies to access and use data held by the private sector in situations where there is an exceptional need for data. Such exceptional circumstances include public emergencies and when implementing a legal mandate, where the required data is not readily available through other means. According to the EC, data insights are often needed to respond quickly and securely, while minimising the burden on businesses.

### 3. Unfair Terms Related to Data Access and Use Between Enterprises

The Data Act protects European businesses from unfair contractual terms in data sharing contracts that one contracting party unilaterally imposes on the other. This will enable SMEs to participate more actively in the data market.

The rules explicitly define unfair terms in the context of data exchange. A contractual term is deemed unfair if its object or effect is to:

- Exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence
- Exclude the remedies available to the party upon whom the term has been unilaterally imposed in case of non-performance of contractual obligations, or the liability of the party that unilaterally imposed the term in case of breach of those obligations
- Give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied is in conformity with the contract, or to interpret any term of the contract

This provision does not apply to contract subject matter or price adequacy regarding the data supplied in exchange, and parties cannot exclude, derogate or vary the effects of these rules in covered contracts.

### 4. Switching Between Data Processing Services

The Data Act will allow customers to switch seamlessly (and eventually free of charge) between different data processing services.<sup>1</sup> Providers of a data processing service will be obliged to ensure that customers of their service can switch to another data processing service, covering the same service type, which is provided by a different service provider.

Additionally, providers of data processing services are gradually prohibited from imposing switching charges on customers. After 12 January 2027, they will be prohibited from imposing switching charges. Until that date, they may impose reduced charges, provided they are transparently disclosed to customers.

These measures will promote competition and choice on the market while preventing vendor lock-in. For instance, any European enterprise could combine data services from different providers and benefit from the vast opportunities in the EU data market. It will also drastically reduce costs for businesses and administrations when they move their data and applications to a different data processing service provider.

### 5. Safeguards Against Unlawful International Governmental Access and Transfer of Nonpersonal Data

The Data Act includes safeguards against unlawful requests by third-country authorities to transfer or access nonpersonal data held in the EU, ensuring a more reliable and secure data processing environment.

In particular, providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to nonpersonal data held in the EU where such transfer or access would create a conflict with EU law or national law. Any judicial decision from a third-country authority requiring access to such data will be enforceable only if based on an international agreement.

In case of absence of such an international agreement, a transfer to a third country would be possible provided that the following conditions apply:

- The third-country system requires the reasons and proportionality of the decision or judgment to be set out, and it requires such decision or judgment to be specific in character; for instance, by establishing a sufficient link to certain suspected persons or infringements.
- The reasoned objection of the addressee is subject to a review by a competent court or tribunal in the third country.
- The competent court or tribunal issuing the decision or judgment, or reviewing the decision of an administrative authority, is empowered under the law of that country to take duly into account the relevant legal interests of the provider of the data protected by EU law or national law of the relevant member state.

If the conditions are met, the provider shall provide the minimum amount of data necessary based on a reasonable interpretation of the request. Providers must also inform customers about third-country requests for data access before complying with that request, except in cases where it serves law enforcement purposes.

### 6. Measures To Promote the Development of Interoperability Standards

Finally, the Data Act introduces measures to promote the development of interoperability standards for data sharing and for data processing services, in line with the EU [standardisation strategy](#). The act outlines essential requirements for interoperability concerning data, data sharing mechanisms, and services within data spaces. These requirements include descriptions of datasets, data structures, technical access means, and provisions for interoperability of tools like smart contracts. It also emphasises the use of harmonised standards, and the role of the EC to request standardisation organisations to draft these standards and adopt common specifications through implementing acts. These measures will ensure interoperability, portability and security while allowing for innovation and technical advances.

<sup>1</sup> In other words, cloud services.

## Implementation and Enforcement

The Data Act will become applicable on 12 September 2025, with certain provisions coming into effect later. Connected products and related services must ensure default data accessibility by 12 September 2026, while rules on unfair contractual terms apply from 12 September 2027, to contracts concluded on or before 12 September 2025.

The EC is tasked with adopting implementing acts to establish common specifications for data interoperability; sharing mechanisms; and common European data spaces, data processing services and smart contracts.

The EC will also adopt delegated acts to establish a monitoring mechanism for data processing services' switching charges. For B2B data sharing, the EC will adopt guidelines on the calculation of reasonable compensation, taking into account the advice of the European Data Innovation Board (EDIB).

Member States are mandated to designate one or more competent authorities and a data coordinator to facilitate cooperation in case more authorities are designated. The authority will be tasked to promote awareness of the rights and obligations under the Data Act, to conduct investigations on the application of the Data Act, and to impose fines when violations are found.

EDIB will facilitate cooperation between competent authorities and advise the EC on implementation strategies of the Data Act.

## How We Can Help

The Data Act establishes an ambitious and far-reaching framework for the use of industrial and other nonpersonal data within the EU economy. It seeks to find a balance between the significance of data as a source of innovation and competitiveness as the EU's digital market develops, and the risks of market distortions and barriers to market entry that could arise if data becomes too concentrated in a small number of powerful economic actors.

The act will undoubtedly bring forward changes to the cross-sectoral governance framework for data access and use, with the potential to radically change the data-driven business environment in the EU. While the rules will apply in parallel to the GDPR, it will be critical for businesses to consider the wide definition of data, which can entail a broader range of obligations.

Similarly, the infringements for not complying with the rules would be "effective, proportionate and dissuasive" and left at the discretion of national competent authorities, which can bring significant fines for companies. The new rules align with the administrative fines of the GDPR, meaning they can reach up to €20 million or 4% of total worldwide annual turnover, whichever is higher.

As such, a compliance assessment, reviewing your existing data practices to ascertain alignment with the requirements stipulated by the Data Act, would be advised.

With us as your trusted advisers by your side, you will be able to spot, assess and understand the risk and opportunities for your organisation from the EU Data Act. We can support you with any legal or policy request you may have. Please do not hesitate to reach out to us for a discussion.

## About Us

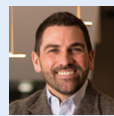
As a full-service global law firm, we provide insight at the point where law, business and government meet, giving our clients a voice, supporting their ambitions and achieving successful outcomes. Our multidisciplinary team of more than 1,500 lawyers and public policy experts in over 40 offices across 4 continents provides unrivalled access to expertise and invaluable connections on the ground. It is a seamless service that operates on any scale – locally or globally. It encompasses virtually every matter, jurisdiction and market – and we place our clients at the centre.

We combine sound legal counsel with a deep knowledge of our clients' businesses to resolve their legal, public policy and political challenges. We care about the quality of our services, the success of our clients and the relationships that are forged through those successes. Our client base spans every type of business, both private and public, worldwide. We advise a diverse mix of clients, from Fortune 100 and FTSE 100 corporations to emerging companies, and from individuals to local and national governments. Leveraging local connections, while exerting global influence, we are commercial, connected and committed.

Our Public Policy Practice Group works with clients to make sure they are heard, at the right time, by the right people, with the right message, in Washington DC, Brussels, London and other major capitals around the world.

Visit our [European Public Policy](#) and [International Policy](#) webpages for more information on our team and capabilities.

## Contacts



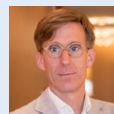
### Wolfgang Maschek

Partner and Chair, European Public Policy Practice, Brussels  
T +322 627 1104  
E [wolfgang.maschek@sqirepb.com](mailto:wolfgang.maschek@sqirepb.com)



### Francesco Liberatore

Partner, London  
T +44 20 7655 1505  
E [francesco.liberatore@sqirepb.com](mailto:francesco.liberatore@sqirepb.com)



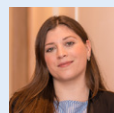
### Charles Helleputte

Partner and Head, EU Data Privacy, Cybersecurity & Digital Assets, Brussels  
T +322 627 1107  
E [charles.helleputte@sqirepb.com](mailto:charles.helleputte@sqirepb.com)



### Matthew Kirk

International Affairs Advisor, London  
T +44 20 7655 1389  
E [matthew.kirk@sqirepb.com](mailto:matthew.kirk@sqirepb.com)



### Christina Economides

Public Policy Advisor, Brussels  
T +322 627 1105  
E [christina.economides@sqirepb.com](mailto:christina.economides@sqirepb.com)