SQUIRE PATTON BOGGS

Understanding the EU Data Act

The European FAQ-tastic Guide to Keep Your Data (Ducks) in a Row

The digital economy has transformed the way businesses operate, with data becoming one of the most valuable assets. In response, the EU introduced the Data Act in 2023.

The Data Act is a pivotal regulation aimed at creating a more equitable and transparent data economy. For businesses, manufacturers, service providers and individual users, the Data Act imposes new requirements on data rights, responsibilities and access. Less lobbied than some of the other new digital package frameworks (EU AI Act, eID, etc.), its broad scope and some drafting errancies led to some cacophony in its actual implementation.

In an effort to help organizations, the European Commission published in September 2024 "Frequently Asked Questions (FAQs) on the Data Act". The 40-page long document has many useful questions (and answers). Below, is a summary of what you think are some relevant ones (also in the format of a FAQ) for a Data Act 101.

What is the Purpose of the Data Act?

The Data Act aims to foster a fair, competitive and transparent data economy. It regulates data access, usage and sharing to ensure that no one entity can monopolize the data generated by devices or services. For businesses and individuals, this means more control over the data they generate

Which Kinds of Data Are in Scope?

- **Product Data** – Data obtained, generated or collected by a connected product (e.g., smartphone, industrial machinery or medical devices) and which related to its performance, use or environment. Purely descriptive data is not product data.
- **Related Service Data** – Data representing user action, inaction and events related to the connected product during the provision of a related service (e.g., apps that regulates the temperature of the fridge, or that adjust the brightness of lights).

For the data related to the connected product to fall under the scope of the Data Act, the product needs to have been placed on the Union market. Afterwards, despite the product being used outside the EU, the data generated by it both inside and outside the EU is in scope.

The level of enrichment of both types of data cannot be very high, therefore, only raw data and pre-processed data, accompanied by the necessary metadata to make it understandable and usable are in scope. Highly enriched data, meaning inferred or derived data that result from additional investments, or content that is often covered by intellectual property rights (e.g. textual or audio content) are out of scope.

Finally, it must be noted that the Data Act only covers non-personal data, so even if users are entitled to access all data generated by the connected product or related service, to access personal data the user will have to rely on GDPR provisions.

Who Does the Data Act Apply To?

The Data Act has broad applicability. It covers manufacturers of connected devices, service providers (particularly cloud services), businesses that hold data and individual users, who generate or rely on digital data. Whether you're a small business using cloud software or a manufacturer of connected devices, the Data Act has implications for your data handling practices.

In that sense, there are three different roles you might take in relation to the data:

- **User** – A natural or legal person established in the EU who owns the connected product, or whom temporary rights to use that connected product have been contractually transferred or that receives a related service. There might be more than one user for a connected product/related service.
- **Data Holder** – Usually, it will be either the manufacturer of the connected product or the company that provides the related service. However, it is also possible for an entity to outsource the role of data holder. They control access to the readily available data, and do not need to be established in the EU (only the product needs to be placed in the EU market).
- **Third party** – Those who receive the data generated from a user or a data holder for the purposes agreed with the user (usually in the context of providing a service to the user). There are some limitations as per the types of action a third party can do (e.g. develop a competing product).

What Rights Do Users Have Over Data Generated by Their Devices?

One of the key pillars of the Data Act is the user's right to access and control the data generated by their devices. Users, whether individuals or businesses, can access this data and share it with third parties of their choice. For instance, if you own a smart home device or an IoT-enabled business system, you have the legal right to the data it generates, empowering you to make decisions on how it's used.

How Does the Data Act Promote Data Sharing Between Businesses and Third Parties?

The Data Act creates a framework for sharing data between businesses and third parties under fair, reasonable and non-discriminatory terms. It ensures that data holders, like platform providers, cannot block access to valuable data that could be used by third-party developers or service providers to improve their offerings.

Can Public Authorities Access Private Data Under the Data Act?

Yes, but only under specific conditions. Public authorities can request access to data held by businesses or individuals in cases of public interest, such as during national emergencies or for public safety reasons. However, the Data Act sets clear limitations on such access, ensuring that sensitive data is protected and that access is only granted when necessary and legally justified.

What Provisions Does the Data Act have for Cloud Service Portability?

One of the major innovations in the Data Act is its focus on cloud service portability. Users should be able to switch between cloud service providers without being locked in by restrictive contracts or technical barriers. This entails revisiting the service conditions to ensure that they are fair and compliant. From January 11, 2024, switching charges should be limited to the costs the providers incur and from January 12, 2027, onwards they should no longer exist.

Moreover, the Data Act provides for a notice (two months) and a transition (30 calendar days) period for the switching to be completed. These timelines can be extended freely by the user but only on a case-by-case basis by the provider, with a maximum extension of seven months.

What Are the Responsibilities of Data Holders Regarding Security and Liability?

Data holders — whether they're businesses storing data for clients or cloud providers — are required to ensure the security of the data they hold. The Data Act places the burden on these entities to protect against data breaches and unauthorized access. In the event of a breach, they are liable for any damage caused, reinforcing the importance of strong cybersecurity measures.

Which Will be the Competent Authority to Handle Disputes or Conflicts Over Data Access?

Disputes regarding data access and usage are inevitable, especially in a competitive landscape. Each member state is required to designate at least one competent authority to deal with the enforcement of the Data Act. Natural and legal persons should lodge complaints with the relevant competent authority in the member state of their habitual residence, place of work or establishment, including with respect to cross-border matters.

Next Steps and Future Actions

Among the next steps identified are:

- The European Data Innovation Board to publish guidance on reasonable compensation for making data available after the Act becomes applicable.
- The European Commission will cover some requirements related to interoperability in data spaces within the "European Trusted Data Framework". The request is expected to be formally adopted by the end of 2024.
- An Expert Group managed by the European Commission is currently developing model contractual terms for data sharing and standard contractual clauses for cloud computing contracts. The European Commission is expected to adopt them before September 12, 2025.

Key Takeaway: Start Navigating the Data Act

The EU Data Act invests the complex world of data governance, ensuring that users, businesses and service providers operate on a level playing field. As we move deeper into the digital age, understanding how this regulation affects your business or personal digital footprint is critical.

In this rapidly evolving data-driven world, the Data Act is more than just a legal requirement—it's an opportunity to assert control over your data and foster a more innovative, competitive future. Whether you are revisiting contracts with cloud providers, rethinking your data-sharing practices or safeguarding against potential disputes, you will need to meet the new regulatory standards.

When it looks like a Data law, it surely is a Data law. So have your ducks in a row.

Contacts

Charles Helleputte
Head of EU Data and Digital, Brussels/Paris
T +32 2 627 1100/+33 1 5383 7400
E charles.helleputte@squirepb.com

Claire Murphy
Associate, Madrid
T +34 91 520 0771
E claire.murphy@squirepb.com

Andrea Otaola
Associate, Brussels
T +32 2 627 1113
E andrea.otaola@squirepb.com

66507/10/24