Bird & Bird

EU Data Act

& the Life Sciences Sector

2025

What is the Data Act?

During the operation of a connected medical device, a large amount of data is generated. This data is used, for example, to provide individualised nutrition and training plans, deliver monitoring services related to vital parameters and/or drug administration, support research and development, and facilitate processes such as device repair, maintenance and operational improvements.

The Data Act is a new cross-sectoral horizontal EU Regulation designed to enhance the EU's data economy and foster a competitive data market. It aims to make data generated by the Internet of Things (IoT) more accessible and usable, increase data availability and encourage data-driven innovation, including in the life science sector.

The Data Act seeks to address the dominant position of manufacturers and service providers by putting the owners, renters and lessors in control of their data. It also facilitates data access for users, repair and maintenance services and other service providers, enabling new business opportunities. For example, it promotes competition in B2B relationships within the life science industry. The Data Act explicitly includes provisions for data sharing with competing aftermarket services. However, it also introduces new obligations.

To which products and services do the data sharing obligations apply?

- **Broad application to connected products**: The Data Act applies to any connected or IoT product that generates or collects data. It expressly states that health and lifestyle equipment, and medical and health devices, are in scope. Examples of connected products to which it applies include continuous glucose monitors and smart insulin pens, smart blood pressure monitors, pacemakers, diagnostic devices, fitness trackers and other wellness wearables, ingestible sensors, and MRI and X-ray scanners.
- **Related services:** The Data Act also sets out rules for digital services (such as user interfaces, applications or other software) which are necessary for the operation of the connected product's functions.
- **Data sharing obligations**: Any data generated using a connected medical or health device, or wearable falls under the Data Act. This means manufacturers of software medical devices, wearable health devices, and any related services they offer must comply with the Act when placing their products or services on the market.

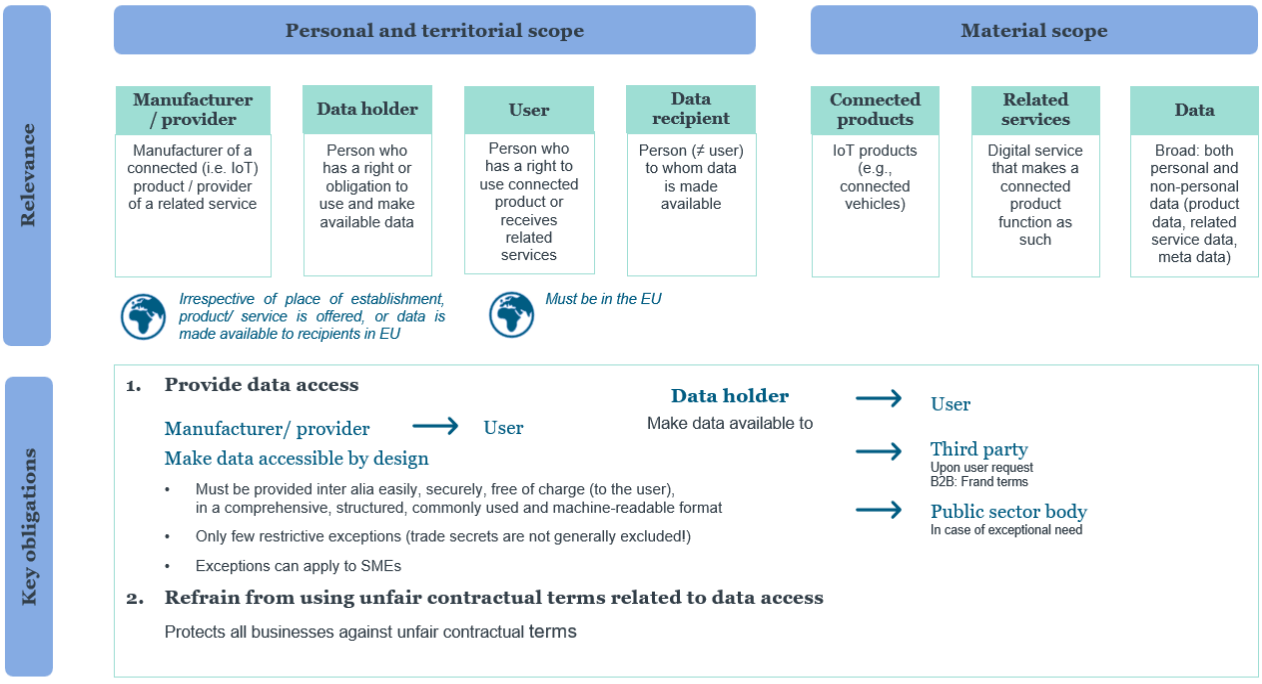
Some will see the Data Act as an opportunity. They will enhance their innovation and collaboration capabilities through improved data access. For users of relevant technologies, such as patients, they will be empowered to control and benefit from their own data. Others will recognise the challenges associated with compliance with the Data Act including the interoperability and data access requirements, managing data access contracts and determining user rights to data.

Who is subject to the Data Act's data sharing obligations?

The Data Act generally applies to manufacturers, suppliers of data-generating components, providers of related services, holders of product data as well as sellers, renters, and lessors of products placed on the EU market, regardless of their place of establishment. This means that most medical and health device manufacturers, as well as many software suppliers in the life sciences sector, fall within its scope. In contrast, beneficiaries - namely users (owners, lessees, and renters of devices) and third-party recipients appointed by users, such as specialised healthcare providers or third-party repair and maintenance providers - must be established in the EU.

Cloud Services

Many life sciences and healthcare businesses make use of cloud services and host significant amounts of data critical to their business interests in the cloud. The Data Act mandates that cloud service providers must facilitate, and remove friction from, the process of switching of data between different cloud services without imposing excessive costs or technical barriers. Those purchasing cloud services within the European Union should adjust their procurement processes to take account of these new rules, which give greater rights and protections to customers.



What are the main implications of the data sharing obligations?

Connected medical and health devices, as well as related services, must be designed and manufactured or provided in such a manner that relevant data is by default, available to EU user(s). If the data cannot be directly accessed, data holders must ensure that the data is made readily accessible without undue delay.

Users are granted the right to access a wide range of data generated by their use of IoT products and related services and can even request that this data be made available to third parties of their choice. This may also require the **disclosure of data** considered **trade secrets**. The EU Commission will publish non-binding model

contractual terms to support these requirements. Manufacturers and data holders must provide such access under fair, reasonable and non-discriminatory terms (FRAND). Additionally, data holders are only permitted to share data with non-EU public sector bodies under certain conditions.

The Data Act also stipulates that third parties (other than users) may only use non-personal data based on a contract with the user. As a result, corresponding rights of use must be explicitly granted, triggering the **need to conclude data sharing agreements** with users and third parties (including competitors). For manufacturers/related service providers and data holders, these new obligations pose significant technical and commercial challenges, requiring adjustments on the technical, contractual and operational levels.

The high number of stakeholders involved in the operation of medical and health devices introduces additional challenges, particularly with respect to implementing security measures for data and operational processes within a tight timeframe. Furthermore, the interplay with sector specific legislation, such as the Medical Device Regulation (MDR) requires attention. For example, medical device manufacturers may be obliged under the MDR to conduct post-market clinical follow-ups, where the collection and analysis of health data could be highly relevant.

However, the Data Act also presents opportunities, such as the ability to obtain data from third-party products and related services, either as a user or through users. Although the Data Act prohibits the use of product and related service data to develop competing products, it does allow such data to be used for the development of novel (competing) services. For instance, this could include the provision of aftermarket services, such as auxiliary consulting, analytics, financial services, or routine repair and maintenance services.

How we can support your business

To ensure compliance with the Data Act, we can support you in:

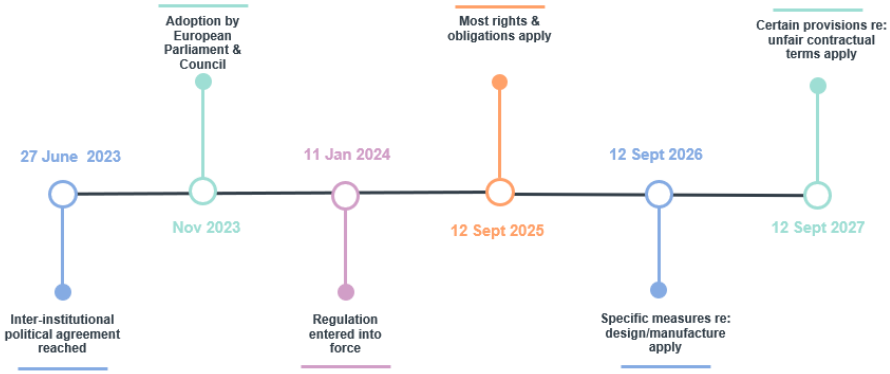
- **Getting an overview** about the existing legal landscape, upcoming legislation, developments (for example connected to the European Health Data Space) and the market practice
- **Undertaking a scoping exercise** to determine the applicability of the Data Act to your products and data
- **Conducting an impact analysis** to identify which (new) rules apply to your organisation and what it means for your business
- **Implementing the Data Act** including:
  - Advising **on changes to product design, manufacturing and information requirements** to comply with data access obligations and how to **protect against unlawful use or disclosure of data**
  - Advising on **compliance with existing obligations** (esp. GDPR, MDR etc.) when implementing the Data Act
  - **Designing processes and procedures** for handling data access requests from users including:
    - Analysing which data to share with others
    - Balancing the requests against the protection of trade secrets, IP and personal data
    - Managing requests from public sector bodies in cases of exceptional need
  - **Drafting and revising your contracts** and additional documentation such as:
    - Data sharing agreements
    - Coud computing contracts
    - Confidentiality, non-disclosure agreements (NDAs)

  - Notices providing users with transparent information

- **Developing template agreements** for making data available to third-party businesses, ensuring the data is made available under FRAND terms
- Adopting **a pricing policy** on how third-party businesses compensate for accessing in-scope data
- Advising on potential FRAND disputes regarding **data access & licensing agreements**
- Advising on **the potential benefits of the Data Act** (e.g. access to third-party data)

What is most urgent?

The Data Act has been in force since **11 January 2024**. Most rights and obligations applied from **12 September 2025**, while certain measures regarding design & manufacturing will only apply from **12 September 2026.** A staggered approach is provided for legacy contracts.



Enforcement

Member States are required to designate the competent authorities and establish effective, proportionate and dissuasive penalties in their local law. If personal data is involved, such fines may align with Regulation (EU) 2016/679 (GDPR) up to **20,000,000 EUR** or **4 % of the total worldwide annual turnover** of the preceding financial year, whichever is higher. It is currently unclear how the competence of the authorities and the number of fines will be defined in detail.

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Lyon • Madrid • Milan • Munich • Paris • Prague • Riyadh • Rome • San Francisco • Shanghai • Shenzhen • Singapore • Stockholm • Sydney • Tokyo • Warsaw