Congenius

Data Act Regulation (EU) 2023/2854

Updated - February 2026
By Jörg Dogwiler

Overview

The EU Data Act aims to harmonise fair data access, data use, and data control within the EU, enhance the EU's data economy, and encourage data-driven innovation.

Having entered into force from **11 January 2024**, the majority of rights and obligations in the Data Act applied from **12 September 2025**. Product design obligations will apply from **12 September this year,** and certain unfair contract provisions from 2027.

Some context...
In 2018 the EU Commission introduced the data economy strategy to promote the growth and competitiveness of the EU's digital economy, creating a single market for data and ensuring its ethical and responsible use. Complementing the Data Governance Act, the Data Act represents the second pillar and cornerstone of the framework for the European single market for data.

Whilst the Data Governance Act regulates processes and structures that facilitate voluntary data sharing, the Data Act clarifies who can use what data and under which conditions - establishing a framework for citizen-generated data sharing in the EU which will impact both individuals and organisations.

What are the benefits of the Data Act?

More data

The Data Act makes **more data available** for the benefit of companies, citizens, and public administrations through establishing **clear rules on the permissible use of data** and the associated conditions.

Improved accessibility

The act **facilitates and regulates data requests** from public sector bodies to private sector businesses when there's a public interest – e.g., during a public emergency.

Greater control

The Data Act gives users of connected **products greater control over the data** they generate while **maintaining incentives for those who invest in data technologies**. General conditions are also stipulated for when one business has a legal obligation to share data with another business.

Enhanced safeguarding

It also introduces safeguards **to avoid the accessing of non-personal data** by third country government bodies where it's against EU or national law.

What are the benefits of the Data Act?

Increased fairness and competition

Measures are included in the Data Act that increase fairness and competition regarding data-sharing agreements - especially between businesses - such as rules that **protect enterprises from unjust contractual terms** imposed by parties holding a stronger market position, or that enable customers to switch between different providers of data-processing services.

The Data Act mandates that contractual terms related to data access and use must be **fair, reasonable, and non-discriminatory (FRAND),** certain **unfair terms are prohibited outright** (e.g., clauses that overly restrict liability or unilaterally allow modification), and the **EU Commission must publish "model contractual clauses"** to support companies in drafting Data Act-compliant agreements.

These model clauses will serve as standard templates or safe-harbour formulations that ensure compliance and reduce legal uncertainty for businesses - especially SMEs. **The EU Commission has not yet published these model contractual clauses however.**

Seamless and confidential interoperability

The Data Act defines **essential requirements regarding interoperability** to ensure seamless and confidential data flow between sectors, Member States, and data processing service providers.

What are the transition periods?

November 2023

Data Act adopted by the European Parliament and Council

22 December 2023

Data Act published

11 January 2024

Data Act entered force

12 September 2025

Majority of rights and obligations in the Data Act applied

12 September 2026

Specific provisions concerning changes to the design and manufacture of products will apply

12 September 2027

Particular provisions related to certain unfair contractual terms will apply

How is the Data Act enforced?

Each EU Member State must designate at least one competent authority to oversee and enforce the Data Act, which may or may not be the existing data protection authority. These authorities **coordinate with sector-specific regulators**, and where personal data is at stake, the **GDPR supervisory authorities** (and the EDPS for EU institutions) remain responsible for enforcement.

Member States must notify the EU Commission of their enforcement rules and designated authorities, and the **Commission will maintain a public register of these arrangements**. This structure is intended to ensure consistent and cross-sectoral enforcement while leaving institutional design to national law.

The Data Act relies on national supervisory authorities to enforce its rules, with **Member States setting concrete penalties** that must be **"effective, proportionate and dissuasive",** and GDPR-level fines applying where personal data is involved.

Enforcement can combine administrative measures (e.g., orders, injunctions, periodic penalty payments) with **significant monetary fines** that may reach up to 20 million euros or 4% of global annual turnover in cases falling under the GDPR regime.

How are medical device manufacturers impacted?

What type of medical device data is covered in the Data Act?

The Data Act and its data-sharing obligations and rights cover any connected physical product that obtains, generates, or collects data concerning its use or environment, which includes medical devices such as, for example, pacemakers, digital diabetes control devices like continuous glucose monitors and smart insulin pens, fitness trackers and wellness wearables, ingestible sensors, and MRI or X-ray scanners.

Personal and non-personal data are covered, as well as the data generated when the user is inactive, for example the data on battery life when a device is on standby or switched off. Cloud or data processing services are also explicitly included.

Data Act sharing provisions relate to:	Data Act sharing provisions do not relate to:
Data that hasn't been substantially modified - specifically raw data and data that has been pre-processed to make it understandable and usable (e.g., heart rate, glucose level). Also, metadata, such as basic context and timestamps.	Any derived information that's the outcome of additional investments into assigning values or insights from the data (e.g., diagnoses, tests, medical treatments, correlations between certain lifestyle factors and diseases, actions to be taken based on data collected).

How are medical device manufacturers impacted?

Who is affected by the Data Act's rights and obligations?

The rights and obligations of the Data Act rest mainly on the **connected medical device users**, and on **those who hold the data** from a connected medical device.

Connected medical device users

"Users" are the natural or legal persons who either own the connected medical device or have a temporary right to use the connected medical device.

Users encompass patients, healthy consumers, hospitals, healthcare providers or healthcare research facilities.

Connected medical device data holders

A **"data holder"** is any natural or legal person who has the right or obligation under EU or national law to use data or make data available.

In many relevant cases, the medical device manufacturer holds this role.

How are medical device manufacturers impacted?

What are the implications for device design and data access?

The Data Act requires certain **data access** and **sharing obligations**, meaning that companies should design and manufacture their connected medical devices and related digital services to ensure that data generated from the use of the device are:

- Directly accessible to the user by default (where relevant and feasible)
- Free of charge
- Delivered in a format that's comprehensive, structured, commonly used, and machine-readable

What if the data isn't made directly accessible by default?

The user may require that the data holder provides indirect access to the data without undue delay and, where applicable, continuously and in real-time. The user also has the right to share and transfer such data to a third party for their own specified purposes (within what's permissible under the Act). Third parties may, however, be charged reasonable cost recovery.

What issues could direct data access cause?

Manufacturers of connected medical devices should consider the extra cybersecurity risks posed, as well as the potential functionality challenges that accompany the increased processing power needed for direct data access.

What do data holders need to consider?

As well as being required to share and allow access to data, data holders' own use of data is also regulated. Non-personal data cannot be used unless a contract is agreed with the medical device user that specifies the purposes for which the data holder will use the data.

Note: These requirements only apply to products and related services placed on the market **after 12 September 2026**. Those that have been marketed before this date will not require modifications to enable this direct data access.

How are medical device manufacturers impacted?

How does the Data Act interact with the MDR & IVDR?

The sharing of connected medical device data is also covered in the:

- ✓ General Data Protection Regulation (GDPR)
- ✓ Data Governance Act (DGA)
- ✓ Artificial Intelligence Act
- ✓ European Health Data Space proposal (EHDS)
- ✓ NIS 2 Directive
- ✓ **EU MDR & EU IVDR**

There is, however, a lack of alignment on interpretation of certain concepts as well as some conflicting obligations for manufacturers – particularly between the Data Act and the MDR / IVDR on the topic of data access.

Notably, the principal objective of the MDR and IVDR is to guarantee the safety and effectiveness of medical devices and in vitro diagnostics. In parallel, the Data Act requires manufacturers to design and develop their medical devices to allow users direct access to user-generated data. As mentioned on the previous page, this requirement for direct access may pose additional cybersecurity risks, and in turn, from a regulatory perspective, undermine the manufacturer's obligations under the MDR / IVDR.

Furthermore, the obligation under the Data Act to make additional data points available to the user or authorised third parties may seriously impact device function, potentially leading to design modifications. If such design modifications are considered "substantial changes" under the MDR / IVDR, the product may be subject to a new conformity assessment and certification.

To avoid considerable additional costs and delays, manufacturers should, as early as possible in their device development, scope the potential cybersecurity threats and design modifications that may arise from Data Act compliance.

How are medical device manufacturers impacted?

How can you facilitate Data Act compliance?

Assess whether your medical devices and digital services fall within the scope of the Data Act

Determine any necessary product modifications to comply with the data access and sharing obligations, and any resulting new conformity assessments and certifications required

Update your user documentation, and prepare documentation for third party data sharing

Establish processes and procedures for sharing data with users and other data recipients

Assess whether controls are needed to protect your intellectual property and trade secrets

What does this mean for Swiss legislation?

Currently, there is no comparable legal act planned in Switzerland. However, the Data Act's extraterritorial application extends to many Swiss companies.

Swiss manufacturers of connected medical devices that are marketed within the EU, Swiss data holders sharing data with recipients within the EU, and Swiss providers offering data processing services to customers in the EU all fall within the scope of the legislation – despite their place of establishment.

Swiss companies will be impacted by the Data Act, and as such, should take proactive steps (as outlined on the previous page) towards compliance. On a final, positive note - the new requirements laid down in the Data Act bring increased potential for data-driven innovation. As such, Swiss companies should evaluate and harness this potential to further their business growth.

Congenius

Should you have a data challenge related to medical devices, get in touch with our team of experts today.

Congenius AG
Riedstrasse 1
CH - 8953 Dietikon

E: info@congenius.ch
T: +41 44 741 04 04

congenius.ch

Revision 2 – February 2026