Meeting EU Data, Cybersecurity, and Artificial Intelligence Law Obligations: A Checklist for Swiss Life Sciences Companies

William RM Long, Eva von Mühlenen, and Lauren Cuyvers

For Swiss companies, the next six months are critical for preparing to meet new Digital Data Law obligations. In this briefing, we outline the key timelines, compliance requirements, and practical steps to align with EU requirements.

The Data Act: Ensuring Data Accessibility and Portability

The Data Act, which will apply gradually from September 2025, is mainly designed to empower users and third parties (e.g., competitors) with greater access to and use of data generated by connected devices (i.e., Internet-of-Things, IoT) to enhance data-driven innovation and competition. Connected products are everywhere, and with the rise of artificial intelligence (AI) are only expected to increase. These include not only medical devices but also other smart or connected products such as wearables, diagnostic tools, and robotics. The Data Act requires manufacturers of connected devices and other data holders to facilitate user access to product and service data generated by the device, and enables seamless transfers to third parties upon request. With just six months remaining until most of the sharing requirements under the Data Act apply, companies must act now.

Key obligations under the Data Act

- **User Data Access (B2C):**
    - **Direct-from-device:** Devices and related services (e.g., apps that allow remote control of a connected device) must be designed and manufactured so as to allow users to securely and *directly* access the data they generate from the device (e.g., direct download from the connected device by the user), and users must be given clear information on the data generation capabilities of the device. In practice, this may require redesign of connected devices, renegotiation with vendors, and implementation of data security measures to ensure secure data sharing (e.g. encryption). This obligation applies as of September 2027.
    - **Indirect:** If it is not possible to design the product so as to allow direct access from the device, the data holder (e.g. the device provider) will facilitate and act upon user data access requests through "electronic means" (e.g., by making

available an online form through which users can request access to data). This obligation applies as of September 2025.

- **Third-Party Data Access (B2B)**:
    - **Upon user request:** Users can request the data holder (including competitors) to transfer its data to third parties in a structured, machine-readable format, continuously, and in real time.
    - **Data access under other EU law:** The Data Act provides for certain mandatory commercial terms (e.g., compensation, dispute settlement, and technical data security terms) to be implemented where the Data Act or other EU law (e.g., the European Health Data Space Regulation) mandates data sharing.

To meet these requirements, companies across sectors—including medical device manufacturers—are actively assessing whether they fall in scope and if so, how they can meet the Data Act's obligations, starting by analyzing their data flows and implementing action plans for when data access requests are received (including by considering how these data-sharing requirements align with potentially competing interests such as their trade secret protection). This involves identifying what data is generated by their devices, how and where it is processed, and how it can be securely accessed or shared. These efforts are critical to anticipating and addressing future user or third-party data requests in compliance with the Data Act.

Impact of the Data Act for Swiss businesses

While the Data Act, as an EU regulation, does not *directly* apply in Switzerland, Swiss companies manufacturing, providing, and/or exporting connected devices or related services (e.g., apps) to the EU must comply irrespective of their place of establishment.

***NIS2 Directive*: Meeting Enhanced Cybersecurity Standards**

The NIS2 Directive, in effect since October 2024, introduces strict cybersecurity requirements for essential and important entities, including medical device manufacturers and healthcare providers. A key milestone is April 17, 2025, the deadline for companies within the scope of NIS2 to register with national authorities (depending on national law implementing NIS2).

Key obligations under NIS2

- **Risk Management Measures:** Companies must implement technical and organizational measures to manage cybersecurity risks including policies on IT security, incident handling, supply chain security, and multifactor authentication.
- **Incident Reporting:** Significant cybersecurity incidents must be reported to national authorities within 24 hours.
- **Senior Management Accountability:** Legal representatives and management bodies can be personally held responsible and liable for noncompliance and may face penalties including administrative fines.

Impact of NIS2 for Swiss businesses

Similar to the Data Act, NIS2 is an EU directive and as such does not apply directly in Switzerland. However, Swiss-based companies that provide in-scope services and carry out their activities in the EU must ensure they meet these requirements. Failing to register by the April 2025 deadline or not implementing sufficient cybersecurity measures could result in fines of a maximum of at least 2% of annual worldwide turnover, reputational damage, and loss of business opportunities.

The AI Act: Regulating High-Risk AI in Medical Devices

The EU AI Act (AIA), in effect since August 2024, introduces a horizontal comprehensive framework for regulating AI systems in line with a risk-based approach–with unacceptable risk AI systems being prohibited in the EU, high-risk AI systems being subject to regulatory requirements (see below), limited-risk AI systems being subject to transparency requirements and low-risk AI systems not being regulated under the AI Act (aside from being subject to the AI literacy principle).

Key obligations under AIA

AI systems that are themselves, or are used as safety components in, medical devices are, in most cases if not all, classified as "high risk" and subject to the following key requirements.

- **Conformity Assessments and CE Marking:** High-risk AI systems must undergo formal evaluation to ensure compliance with EU standards and bear CE marking.
- **Data Provenance and Cyber:** High-risk AI systems must be trained on the basis of high-quality training data that is free of errors and sufficiently representative to avoid bias, and shall adequately protect from attacks in particular those aimed at altering the system's output, use, or performance. AI systems must have the ability to log relevant events throughout the lifecycle of the product.

- **Transparency Requirements:** Users must be informed through instructions of use about the AI system's intended purpose, potential risks, and other relevant information that allow users to interpret the output.
- **Human Oversight:** Users shall implement, and providers and manufacturers shall design AI systems so as to facilitate, oversight by natural persons of the AI system to prevent or minimize risk.
- **AI Literacy Deadline:** By February 2, 2025, companies were required to ensure that relevant staff are trained to understand AI functionality, risks, and compliance obligations.

Impact of AIA for Swiss businesses

As an EU regulation, the AIA does not apply directly in Switzerland, but the AIA has extraterritorial effect, and Swiss-based companies must comply with the AIA if they provide or put into service AI systems in the EU or if they use AI output in the EU. Companies that fail to comply risk not only fines but also damage to their reputation and disruption of business operations.

Although Switzerland is not an EU Member State, its deep economic ties and reliance on the EU market make compliance with these regulations essential. Adapting to the Data Act, NIS2, and AIA is not only a legal obligation but also an opportunity for Swiss companies to demonstrate a commitment to data security, product safety, transparency, and ethical AI use to enhance customer trust and to facilitate access to the EU market by aligning with EU requirements.