New AI, Data, and Cyber Laws — State of Play

Francesca Blythe, William Long, Eva von Mühlenen and Matthias Bruynseraede

As part of the EU Digital Transformation Strategy, the EU has proposed several new AI, data, and cyber laws — many of which will apply to companies in the life sciences industry, including those operating in Switzerland. In this article, we explore the state of play of some of these proposed laws and their application for life sciences companies.

Artificial Intelligence Act (AI Act)

The proposal for the AI Act regulates the use, placing on the market, and putting into service of "AI systems" in the EU. It takes a risk-based approach whereby the regulatory obligations that are imposed increase as the presumed level of risk posed by the AI system increases. In turn, providers of AI systems that are considered "high risk" (which would, as currently drafted, include most AI-enabled medical devices) would be subject to the most onerous requirements under the AI Act. These requirements include, for example, implementation of conformity assessments, the use of high-quality data sets for training purposes, mandatory reporting obligations for serious incidents, and measures to ensure appropriate human oversight.

The AI Act has a broad, extraterritorial scope and would also apply in certain instances to providers and users of AI systems located outside of the EU, for instance, in Switzerland where the output of an AI system (i.e., an AI prediction, recommendation, or decision) is used in the EU.

The proposal for the AI Act was published by the European Commission in April 2021. Since then, the Council has adopted its negotiation position, and we understand that the European Parliament will adopt its text in the coming weeks. Following this, discussions between the Member States, the Parliament, and the Commission (the so-called "trilogue") are expected to commence. If this timeline is met, the final AI Act should be adopted by the end of 2023 and will formally apply from the end of 2025.

However, the time to act is now as there already exists a large amount of guidance on the development and deployment of AI systems from both national Data Protection Authorities (e.g., in the UK and France) and health regulators (e.g., the UK's Medicines and Healthcare Products Regulatory Agency). Standards have also been published including, for example, the ISO framework for AI systems using machine learning and the U.S. National Institute of Standards and Technology AI risk-management framework which companies may consider leveraging for compliance purposes.

For further details, please read our Sidley Update on the AI Act.

European Health Data Space (EHDS)

Of particular interest to the life sciences sector is the proposal for the EHDS Regulation, which (among other things) requires so-called "data holders" processing electronic health data (EHD) to make this data available to so-called "data users" for prescribed secondary-use purposes (including scientific research). As drafted, the categories of EHD that a data holder may need to disclose include a very broad set of data, that is, both personal and nonpersonal data, from a wide variety of sources (e.g., from clinical trials, electronic health record systems, connected devices). Access by the data user is typically subject to the data user's having applied for and having received a permit from a national health data access body to access the EHD.

However, there is at present a lack of clarity, in particular, as it relates to the scope of the EHDS Regulation. For example, the definition of who constitutes a data holder is still open for interpretation, and the extraterritorial scope (in particular, as it relates to data holders) is uncertain. This is, in turn, something that companies in the life sciences industry (including those based in Switzerland) should monitor closely as it is expected that the final text will be agreed on in 2024.

Data Act

The proposal for the Data Act seeks to (among other things) regulate the use of, and access to, data generated through connected (or Internet-of-Things) devices. The Data Act has not yet been formally adopted, but it is expected that the final text will be agreed on in the coming months and will therefore likely apply in 2024.

The material scope of the Data Act is broad, and it places obligations on a wide range of actors including, for example, (i) manufacturers of connected devices and providers of related services — who are required to facilitate access to the data generated, (ii) data holders — who must provide the data generated to a user or a third-party data recipient (upon request by a user), and (iii) data recipients – who are subject to various conditions regarding the use of the data received by them.

Importantly, Digital Europe has recently expressed concern that the Data Act in its current form is a "huge leap into the unknown" for businesses already overwhelmed with new upcoming regulations. In particular, Digital Europe has asked the European Commission to reconsider the proposals in light of the potential risks presented from the perspectives of cybersecurity, trade secrets, and competition. It will be interesting to see how these concerns are addressed — including, potentially more broadly in the EHDS Regulation, which has a similar objective as it relates to data sharing.

Network and Information Security Directive 2 (NISD2)

On the cybersecurity side, the NISD2, which aims to establish a harmonized minimum level of cybersecurity across the EU, entered into force on January 17, 2023, and, as an EU directive, must be implemented into national EU Member State legislation by October 17, 2024.

At a high level, NISD2 applies to entities that provide their services or carry out their activities in the EU and that qualify as either an "essential" or an "important" entity. Examples of such entities include healthcare providers, entities carrying out research and development of medicinal products, and entities manufacturing pharmaceutical products. Providers of information and communication technology (or ICT) management services also fall within scope where they offer services in the EU, irrespective of their location.

The minimum set of cybersecurity requirements to be implemented are prescribed in NISD2 and include policies and procedures to assess the effectiveness of cybersecurity risk-management measures and supply-chain security measures and the use of multifactor authentication. Companies are also required to notify the competent authority within 24 hours of becoming aware of a cyber incident that has a significant impact.

Importantly, and in addition to any administrative fines that may be imposed on the company for noncompliance, NISD2 introduces personal liability for senior management where they fail to adequately implement the cybersecurity risk management measures in line with NISD2.

Next Steps

As a next step, Swiss life sciences companies should determine which of these new AI, data, and cyber laws they are subject to and, if so, what the impact of these laws will be.

For more information on Sidley's Digital Transformation Strategy, click here.