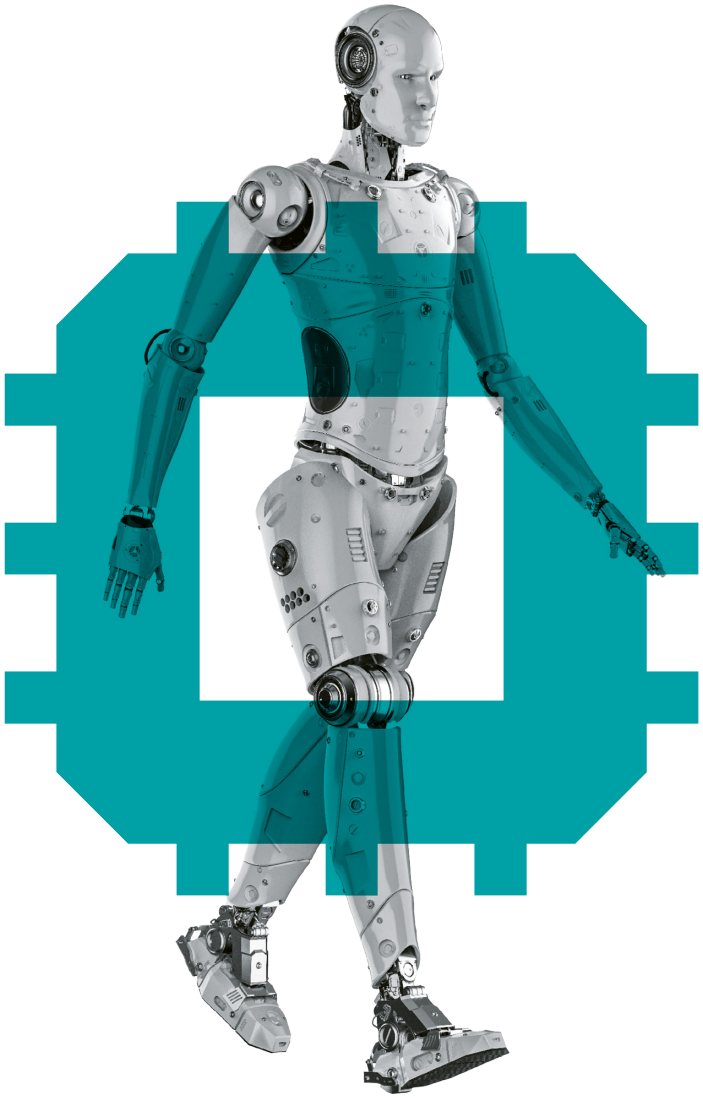
N

Monthly Newsletter March 2025

ICT

Schellenberg Wittmer



Relevance of EU regulations in the digital sector for Swiss companies

Roland Mathys, Jacqueline Brunner

Key Take-aways

1.
Swiss companies operating in the EU and offering products or services there often fall within the scope of various EU regulations in the digital sector, either directly or through their extraterritorial effect.

2.
The EU regulations introduce extensive rules of conduct aimed at ensuring greater security, transparency, and innovation, as well as improved data access.

3.
Non-compliance can result in significant sanctions, which is why Swiss companies should continuously assess their need for action.

1 Introduction

In recent times, numerous laws in the area of digital and data have been enacted in the European Union (**EU**). This newsletter provides a brief overview of selected regulations (without claiming to be exhaustive) in the digital sector and highlights their relevance for Swiss companies.

2 Data Act (DA), Digital Services Act (DSA) and Digital Markets Act (DMA)

The DA entered into force on 11 January 2024 and will be applicable across the EU after a 20-month transition period.

The DA aims to promote **free data access** and foster innovation. Key provisions of the DA include ensuring data access and availability of data, as well as ensuring interoperability and contractual compliance.

The DA applies to **personal and non-personal data** generated through the use of 'connected products' (items that collect, generate, or gather data about their use or environment and can transmit this data via wired or wireless connections) and 'connected services' (digital services that are linked to a connected product and support its functions).

The DA **addresses** in particular manufacturers of connected products and providers of connected services, as well as their users, data holders and public sector bodies. Micro and small enterprises (fewer than 10 or 50 employees and EUR 2 or 10 million turnover/balance sheet) are largely exempted from the obligations (e.g. disclosure of personal data). Due to its extraterritorial effect, the exact scope of which is still unclear, the DA can also affect **Swiss companies**, namely:

- manufacturers of connected products that are placed on the market in the EU and providers of related services to users in the EU;
- data holders who provide data to recipients in the EU; and
- data processing service providers who offer their services to customers in the EU.

Infringements of the DA will result in significant **sanctions**. The EU Member States adopt regulations on sanctions, with the DA requiring that the sanctions be effective, proportionate, and deterrent. Fines of up to EUR 20 million or 4% of worldwide annual turnover are possible.

The DMA (which regulates gatekeepers) and the DSA (which regulates digital service providers) contain extensive rules of conduct for the fair and secure use of digital platforms. Swiss companies may also be affected. You can find more information in our newsletter '[Digital Markets Act and Digital Services Act: Implications for Switzerland]'.

3 Artificial Intelligence (AI)

3.1 EU Artificial Intelligence Act (AI Act)

The AI Act entered into force on 1 August 2024, with implementation taking place in stages. The aim is to ensure the safety and transparency of AI systems in the EU and to uphold fundamental rights.

The AI Act distinguishes between **AI systems and AI models**: The term AI system refers to a machine-based system that can function independently and adapt to new situations, and that can learn from the input it receives and make predictions, content, recommendations or decisions that can influence physical or virtual environments (e.g. ChatGPT). AI models build elements of AI systems and refer to specific components within an AI system (e.g. large language models; LLM).

Numerous EU regulations also apply to Swiss companies.

The AI Act takes a **risk-based approach**: AI systems are allocated into four risk categories (unacceptable, high, limited or minimal risk) with decreasing level of regulation. While AI systems with unacceptable risk are generally prohibited, strict requirements apply to those with high risk (e.g. risk management, data governance and technical documentation). Less stringent obligations apply to AI systems with limited risk (e.g. the obligation to provide information about interaction with an AI system), and those with minimal risk are hardly regulated at all; so-called AI literacy must be ensured. The extensive catalogue of obligations is aimed primarily at providers. Deployers are responsible for the compliant use of the AI system (e.g. human supervision and monitoring of AI operation). Due to its extraterritorial effect, the exact scope of which is still unclear, the AI Act may also apply to **Swiss companies**, namely to:

- providers that place on the market or put into service AI systems or place on the market general-purpose AI models in the EU, whether these providers are established in the EU or in a third country;
- providers and deployers of AI systems established in or located in a third country if the output produced by the AI system is used in the EU.

Infringements of the AI Act can result in severe **sanctions**, with the AI Act providing for fines of up to EUR 35 million or – in the case of an undertaking – 7% of the worldwide annual turnover for the preceding financial year (whichever is higher).

3.2 Recent Development: AI Regulation in Switzerland

The Federal Council very recently published an overview of AI regulation **for Switzerland** (press release of 12 February 2025): According to this, the Council of Europe's AI Convention is to be incorporated into Swiss law, and any necessary legislative adjustments are to be made specifically for certain industry sectors. Therefore, no comprehensive and detailed regulation, as seen in the EU AI Act, is planned – except for key areas related to fundamental rights. Consequently, companies exclusively operating within Switzerland and not being subject to the AI Act will benefit from simplified regulations, in contrast to those companies that must additionally comply with the AI Act. This is because the upcoming Swiss AI regulation is not expected to implement the provisions of the AI Act, or only to a limited extent.

4 Cyber Resilience Act (CRA)

The CRA entered into force on 10 December 2024, and will be fully applicable from 11 December 2027, following a three-year implementation period. However, some provisions (such as the reporting requirement for IT vulnerabilities and security incidents) will become enforceable earlier.

The CRA aims to significantly improve the **cybersecurity** of connected products. The CRA sets out minimum requirements for cybersecurity and covers products with 'digital elements' that are placed on the EU market and can be connected to the internet, other devices or networks, such as hardware and software products, Internet of Things devices, smart home appliances, connected vehicles and industrial machines.

Affected companies can expect potentially high compliance efforts.

Important provisions of the CRA relate to ensuring cybersecurity throughout the entire lifecycle, compliance with reporting, documentation, and transparency obligations, conformity assessments, and the provision of security updates. The specific obligations arise from the role of the addressee and the product qualification. Manufacturers bear the main responsibility for product security and must, for example, create technical documentation and information material on cybersecurity. Importers and distributors must ensure that the products comply with the regulations (e.g. check CE marking/ declaration of conformity). The reporting obligations for security risks and vulnerabilities apply to all actors.

The CRA is aimed at manufacturers, importers, and distributors in the EU. Due to its **extraterritorial effect**, the exact scope of which is still unclear, it also applies to Swiss manufacturers, importers and distributors who make such products available to recipients in the EU.

Infringements of the CRA can result in severe **sanctions**, namely in fines of up to EUR 15 million or – in the case of an undertaking – 2.5% of the worldwide turnover (whichever is higher). In addition, market surveillance measures – such as mandatory product recalls – are possible.

Infringements may result in significant sanctions.

5 Digital Operational Resilience Act (DORA)

The DORA entered into force on 17 January 2025. It **focuses** on risks from information and communication technology (ICT) and aims to strengthen the digital operational resilience of the European financial sector.

The DORA contains **requirements for ICT risk management** and for contracts with ICT service providers. This obliges the addressees to implement robust cybersecurity measures, conduct security assessments, and ensure business continuity. Key areas include: ICT risk management, ICT third-party management, ICT incident management, testing, and information sharing.

The DORA is aimed at EU **financial entities** (e.g. credit institutions, investment firms, and insurance undertakings) and ICT providers that deliver services to these financial entities. Swiss companies operating as **ICT service providers** for EU financial entities or forming part of an EU financial group are also affected by the DORA and must comply with its provisions.

The DORA does not provide for immediate monetary fines or criminal **sanctions**. Instead, it is at the discretion of the EU Member States to impose sanctions for infringements in their national laws. Competent authorities can also impose administrative sanctions and corrective measures, and publish the administrative penalties imposed, as well as the affected company, on their website.

6 NIS 2 Directive (NIS2)

The NIS2 (successor to the NIS1) entered into force on 16 January 2023, and had to be transposed into national law by EU Member States by 17 October 2024. The NIS2 aims to strengthen cybersecurity across the EU by setting higher standards for **critical infrastructure** and extending its scope to other sectors and types of organizations.

The key **provisions** of the NIS2 concern: governance, cybersecurity risk management measures, security risk assessments of critical supply chains in the EU, reporting obligations, representation in the EU and registration of operators of critical infrastructures.

The **scope of application** of the NIS2 includes essential and important entities, with different obligations tied to their respective qualifications. The NIS2 applies to public and private entities classified as medium or large enterprises (at least 50 employees and EUR 10 million in turnover/balance sheet total or 250 employees and EUR 50 million in turnover or EUR 43 million in balance sheet total). Certain entities (e.g., communication networks) are included in the scope regardless of these thresholds. **Swiss companies** may also be affected by the NIS2 if they provide their services in the EU or carry out their activities there.

Infringements of the NIS2 can be subject to **sanctions**: The competent authorities may take various supervisory and enforcement measures, such as on-site inspections. Infringements are subject to fines, in the case of essential entities up to EUR 10 million or 2% of worldwide annual turnover (whichever is higher).

7 Conclusion

The aforementioned (and other) EU regulations in the digital sector do not stop at the EU (or EEA) external borders – in fact, Swiss companies can also be affected and required to comply. Therefore, it is important to review these regulations in a timely manner and take targeted action!

Roland Mathys
Partner
roland.mathys@swlegal.ch

Lorenza Ferrari Hofer
Partner
lorenza.ferrari@swlegal.ch

Stéphanie Chuffart-Finsterwald
Partner
stéphanie.chuffart@swlegal.ch

Grégoire Tribolet
Partner
gregoire.tribolet@swlegal.ch

Schellenberg Wittmer Ltd is your leading Swiss business law firm with more than 150 lawyers in Zurich and Geneva, and an office in Singapore. We take care of all your legal needs – transactions, advisory, disputes.

Schellenberg Wittmer Ltd
Attorneys at Law

Zurich
Löwenstrasse 19
P.O. Box 2201
8021 Zurich / Switzerland
T +41 44 215 5252
www.swlegal.com

Geneva
15bis, rue des Alpes
P.O. Box 2088
1211 Geneva 1 / Switzerland
T +41 22 707 8000
www.swlegal.com

Singapore
Schellenberg Wittmer Pte Ltd
50 Raffles Place, #40-05
Singapore Land Tower
Singapore 048623
www.swlegal.sg