BÄR
& KARRER

BRIEFING DECEMBER 2023

THE EU‘S AI ACT. WHAT DOES IT MEAN FOR SWISS COMPANIES?

On 8 December 2023, the EU trilogues ended with a provisional agreement on the Artificial Intelligence Act, in short: the AI Act. The AI Act is the first law regulating AI systems comprehensively, focusing on ensuring safety, sustainability, respecting fundamental rights, democracy and the rule of law, and at the same time harnessing innovation. It is also expected to set a global standard, similar to the EU's General Data Protection Regulation (GDPR). Once it has been formally adopted, it is expected to be fully applicable after two years following adoption (with certain exceptions; see below).

Due to its extraterritorial effect, the AI Act may also apply to Swiss companies that make an AI system available in the EU market or if the output generated by their AI system is used in the EU.

Non-compliance with the AI Act can lead to substantial fines of up to EUR 35 million or 7% of global turnover, depending on the infringement and company size.

In this first briefing on AI regulation, we provide an overview of the AI Act, the risk-based approach it takes and also highlight important new obligations. In particular, we explain how the AI Act may affect Swiss companies.

RISK-BASED APPROACH

Under the AI Act, AI systems are regulated based on their potential risks to society and fundamental rights, with stricter rules applicable to so-called high-risk AI systems and foundation models – large systems capable of performing a wide range of distinctive tasks, such as generating video, text or images.

AI systems are categorised into **four risk categories**, each resulting in specific requirements and regulations for companies subject to the AI Act:

> **Unacceptable risk**: This category includes AI systems that pose a major threat to society or the safety and fundamental rights of individuals. The use of these systems is **prohibited** and will have to cease within six months of the AI Act entering into force. Examples of AI systems with unacceptable risks include social scoring systems used by governments, predictive policing, real-time biometric identification systems in public spaces (except for specific law enforcement purposes), untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases, emotion recognition in the workplace and educational institutions, children‘s toys using voice assistance that could lead to dangerous behaviour of children, AI systems that manipulate individuals‘ behaviour to circumvent their free will or that exploit the vulnerabilities of children or the disabled.

> **High risk**: These are AI systems that could pose significant risks to society, the environment or people‘s safety and fundamental rights. They are subject to **strict compliance and regulatory requirements** *(see below)*. Examples for such AI systems include AI systems used to screen job

candidates during the recruitment process, AI in critical infrastructures (e.g., transport, energy, gas), AI used for credit scoring or assessing creditworthiness of individuals, AI used in safety components of products (e.g., application of AI in robot-assisted surgery), biometric identification, categorisation, and emotion recognition systems (if not entirely banned) or AI systems used to influence elections.

- **Limited risk**: This category includes AI systems that entail limited risks, and specific **transparency obligations** must be met allowing users to make informed decisions. Examples of this risk category include chatbots and deepfakes that require clear information or labels for users to understand that they are interacting with an AI system, AI-enabled video games that adapt to player behaviour or AI systems used in virtual assistants. AI systems that use synthetic audio, video, text or images will, therefore, need to be designed in a way that allows their recognition as "artificially generated or manipulated".
- **Minimal or no risk**: These AI systems pose minimal or no risks to society or the rights or safety of individuals. They are **mostly free from regulatory constraints** under the AI Act. Most AI systems are expected to fall under this category. Examples of these AI systems include AI-driven spam filters or AI used for sorting documents in offices. However, persons developing or deploying such tools under the AI Act may still choose to voluntarily adhere to **codes of conducts** in developing and deploying such AI systems.

Specific rules apply to **general-purpose AI ("GPAI") models** which are also referred to as **foundation models**. They must comply with specific **transparency obligations** before they are placed on the market, e.g., to provide technical guidance to those who integrate GPAI model into their AI systems.

Foundation models that pose **"systemic risks"** (so-called **"high-impact" models**) – which are foundation models trained on large amounts of data using large quantities of computing power – such as GPT-4 which is the basis of OpenAI's widely known ChatGPT-4 or Dall-E 2 – are subject to a stricter regulatory regime. In particular, companies will have to **conduct model evaluations and adversarial testing, assess and mitigate systemic risks and report on serious incidents.** These obligations will apply sooner than other obligations provided under the AI Act; in fact, companies will have to comply with these obligations within twelve months of the AI Act entering into force.

STRICTER RULES FOR HIGH-RISK AI SYSTEMS

Under the AI Act, high-risk AI systems are subject to the most stringent rules. In particular, as agreed on 8 December 2023, providers of high-risk systems will need to carry out a **fundamental rights impact assessment ("FRIA")** to analyse the risks for individuals before releasing the AI system on the EU market.

Furthermore, high-risk AI systems must have a robust **risk management** system, ensure the **quality and integrity of the data** they use, keep thorough **documentation** (including on programming and training methodologies, data sets used, and measures taken for oversight and control), comply with **storage and transparency** requirements, ensure **human oversight** to prevent autonomous operation that could risk safety or rights, ensure **accuracy, robustness** and **security** so that the AI system functions as intended, undergo **conformity assessment** procedures before being released and **register the AI system in a public database** maintained by the EU Commission. In sectors where conformity assessments already have to be carried out today (e.g., for medical devices), compliance with the requirements of the AI Act will be assessed in the conformity assessment of the sector specific regulation.

Individuals will have a right to launch **complaints** about AI systems individually or collectively if they believe that the AI system has violated their rights as stated in the AI Act.

Distributors of high-risk AI systems will also have to ensure that the AI system bears the required CE conformity marking, that it is accompanied by the required documentation and instruction of use, and that the provider and the importer of the AI system have complied with the AI Act before the AI system hits the market. Distributors will thus play a crucial role in the implementation of the AI Act.

HOW WILL THE AI ACT AFFECT SWISS COMPANIES?

The AI Act imposes obligations in connection with AI systems that are "placed on the market, put into service or used in the EU". This means that in addition to developers and distributors in the EU, it also applies to companies outside of the EU selling or otherwise making their system or its output available to users in the EU.

Therefore, like the GDPR, the AI Act will apply to Swiss companies as it has an **extraterritorial reach**. It will not only be applicable to a Swiss company that **makes an AI system available in the EU market** but will even apply if only the **output generated by the AI system of a Swiss company is used in the EU**.

This means that Swiss companies may have to comply with the rules set out under the AI Act and, if they fail to do so, they may face investigations by European AI regulators and be subject to fines under the AI Act.

WHAT SHOULD SWISS COMPANIES DO?

Swiss companies developing or deploying an AI system should closely monitor when the AI Act will enter into force and prepare accordingly. As a first step, Swiss companies should assess: (i) whether the AI Act applies because they offer their AI system in the EU, their AI system is deployed, imported or used in the EU or the output of their AI system is used in the EU and, if so, (ii) within which risk category their AI system falls.

Unless the AI system bears unacceptable risks (in which case it needs to be stopped within six months of the AI Act entering into force), Swiss companies will need to ensure that they comply with the transparency obligations (in case of a limited risk AI system) or the specific additional obligations (in case of a high-risk AI system or high-impact foundation model) by the time the AI Act enters into force.

When dealing with **high-risk AI systems**, Swiss companies will have to check or implement in particular the following:

> AI governance within the company (assign responsibilities and resources and establish reporting lines);
> Information notices or disclosures to ensure compliance with the transparency obligations;
> Process to ensure data quality and governance when training AI systems;
> Risk management system (existing systems should be extended as needed);
> Cyber security measures (existing measures should be reviewed and updated as needed);
> Process for conformity assessments (existing (sector-specific) compliance processes should be extended as needed);
> Process to carry out a fundamental rights impact assessment (this can be built on past experiences of data protection impact assessment);
> Process to ensure human oversight;
> Technical documentation (showing among others compliance with the AI Act); and
> Register the AI system with the competent authorities.

In situations where the AI system is banned under the AI Act, Swiss companies may need to make a strategic shift in their business.

WHAT COMES NEXT IN THE EU?

The AI Act still has to be formally adopted to become law and is expected to enter into force next year. It will then **become applicable two years after its entry into force**. However, the **prohibition of AI systems with unacceptable risks will already apply after six months** and the r**ules on GPAI will apply after twelve months** following the entry into force of the AI Act.

Until the AI Act is fully applicable, the EU Commission intends to launch an **"AI Pact"** which will group AI developers from Europe and around the world who voluntarily commit to implement key obligations of the AI Act ahead of the actual legal deadlines for doing so.

WHAT IS HAPPENING IN SWITZERLAND?

On 22 November 2023, the Swiss Federal Council decided to evaluate the regulation of AI in Switzerland to ensure that the potential of AI can be harnessed while minimising inherent risks such as discrimination, misinformation or copyright infringements. The Federal Council mandated the Federal Department of Environment, Transport, Energy and Communications to identify possible approaches to regulate AI in Switzerland by the end of 2024. The analysis aims to identify possible regulatory approaches that are compatible with other regulations, such as the AI Act.

AUTHORS

Jennifer Winkler
Junior Asssociate
T: +41 58 261 53 05
jennifer.winkler@baerkarrer.ch

Dr. Rehana Harasgama
Senior Associate
T: +41 58 261 54 51
rehana.harasgama@baerkarrer.ch

Dr. Christian Kunz
Partner
T: +41 58 261 52 66
christian.kunz@baerkarrer.ch

FURTHER CONTRIBUTORS

Gadi Winter
Senior Associate
T: +41 58 261 53 59
gadi.winter@baerkarrer.ch

Dr. Djamila Batache
Associate
T: +41 58 261 50 66
djamila.batache@baerkarrer.ch

Michele Bernasconi
Partner
T: +41 58 261 54 10
michele.bernasconi@baerkarrer.ch