White paper

AI regulation and Governance

swisscom

Enable, drive and protect your business.

Introduction

In today's increasingly digitalised world, artificial intelligence (AI) is far more than just a trend – it is transformative technology with the potential to fundamentally change our working world and business landscape. AI is becoming a decisive building block for the future viability of companies and is opening up major opportunities for innovation and efficiency improvements. However, along with these opportunities come new challenges, especially with regard to legal and ethical issues. The use and development of AI systems require not only technological expertise but also compliance with applicable regulations.

When introducing an AI system, as with other software solutions, the first step always lies in clarifying which legal requirements apply. For Swiss companies, these can include – especially when processing personal data – the Swiss Federal Act on Data Protection (FADP) and in some cases cantonal regulations, the European Union (EU) General Data Protection Regulation (GDPR) and even confidentiality regulations. Industry regulations can also play a role. Now, there are also specific AI regulations, such as the EU Regulation on Artificial Intelligence (also known as the AI Act), which are becoming increasingly important. As a result, companies are finding themselves not only facing existing legal requirements but also having to look closely at the new regulations being created and developed due to the rapid development of AI technology. Switzerland, too, is proposing new regulations for AI technology.

In view of the new legal framework conditions (especially the EU AI Act), companies and public authorities are faced with the task of expanding their existing compliance and Governance models to include targeted AI Governance. It is important to bear in mind that clear rules for data handling need to be established before the requirements set out in AI regulations can be based on them.

This white paper explains the current situation of AI regulation in Switzerland and the EU. With regard to the EU, it provides an insight into the EU AI Act and outlines why this can also be of relevance to Swiss companies. We also use the example of Swisscom to show how AI Governance can be designed, why the topic is of importance for competitiveness and why organisations should tackle the topic of AI Governance at an early stage.

The EU AI Act and its relevance for companies in Switzerland

The AI Act[1] entered into force in the EU on 1 August 2024 within the scope of a broader package of digital policy measures and as the world's first comprehensive legal framework for AI. Its aim is to promote trustworthy AI systems and general-purpose AI models (GPAI models) in the EU.

AI system
A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

Known AI systems
ChatGPT from OpenAI, Copilot from Microsoft, Perplexity from Perplexity AI

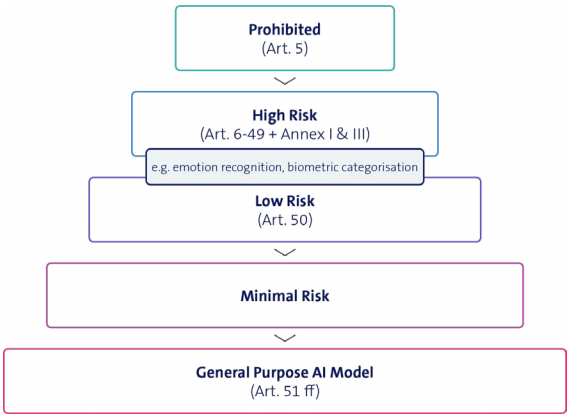
General-purpose AI Model
An AI model that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications.

Known GPAI models
GPT from OpenAI, Claude from Anthropic, LLaMA from Meta

[1] Regulation 2024/1689 laying down harmonised rules on artificial intelligence.

Risk-based approach

Although most AI systems do not present any significant risks, certain AI applications can pose challenges that the EU aims to address with its legislation. The AI Act follows a risk-based approach: the greater the risk, the stricter the legal requirements. AI systems are accordingly divided into four risk levels:



Prohibited AI systems

The AI Act (Art. 5) prohibits specific AI practices. These include the development and deployment of AI systems that manipulate human decisions or specifically exploit vulnerabilities, as well as AI systems that evaluate or classify people based on their social behaviour or personal characteristics (social scoring). AI systems that predict whether a person is likely to commit a criminal offence are also prohibited. The Act furthermore prohibits the use of AI systems that scrape facial images from the Internet or surveillance cameras and that use biometric data (e.g. voice or facial geometry) to analyse emotions in the workplace or educational institutions, or that categorise people accordingly. Exceptions are, however, possible in certain cases, such as for law enforcement, when searching for missing persons or for the prevention of terrorism.

Practical example

A company uses an AI system that employs voice recognition to analyse the emotions of its employees while working. Specifically, the AI system evaluates the employees' biometric data to identify feelings such as joy, anger or sadness and creates reports about the moods that prevail in different departments or teams. The management uses these analyses to identify supposedly unmotivated or emotionally stressed employees and take action accordingly.

This kind of AI system is prohibited under the AI Act, as it analyses emotions on the basis of biometric data and draws conclusions about employees' behaviour or work performance. The only exception would be if the system were used for medical or safety reasons; for example, to prevent accidents by detecting exhaustion in machine operators.

High-risk AI systems

The second risk level relates to 'high-risk AI systems' (Art. 6; Annex I, Annex III), the development and deployment of which pose a high risk to the health, safety or fundamental rights of EU citizens. High-risk AI systems can be divided into two subcategories, which are set out in Annex I and Annex III:

Firstly, these include AI systems that operate as safety components of regulated products (e.g. medical devices, toys, radio equipment, recreational craft, aircraft, vehicles, the rail system or lifts). The failure of these could endanger the health or safety of people or property.[2]

[2] AI Act: Annex I

Secondly, this category includes applications in the fields of biometrics, critical infrastructure, education and vocational training, employment, essential services, law enforcement, migration and justice. However, exceptions apply to certain AI applications, such as those used for the purpose of biometric identity verification, financial fraud detection or the organisation of political campaigns.[3] It is estimated that only five to ten percent of all AI systems are classed as high risk. The AI Act establishes several requirements for high-risk AI systems, including extensive Governance structures and appropriate documentation.

Practical example
A medtech company uses an AI system to improve medical imaging and support the diagnosis of medical conditions. The AI-based system analyses X-ray, MRT or CT images and automatically detects anomalies such as tumours, lung abnormalities or heart disease. The system highlights these areas for the attending doctor and provides additional information to facilitate a sound diagnosis. As such systems directly influence the health and safety of patients, they are categorised as high-risk AI systems under the AI Act.

AI systems with limited risk and special transparency obligations

Pursuant to Art. 50 AI Act, AI systems with limited risk are subject to special transparency obligations. This category includes the development of AI systems intended to interact directly with people (where it is not necessarily obvious that people are interacting with an AI system due to the context of use) and the development of AI systems that generate or manipulate synthetic audio, image, video or text content, where the average person would consider the content to be real. The Article therefore addresses companies that develop and offer such AI systems.

Practical example
A company commissions the development of an AI chatbot to automatically answer customer enquiries on its own website. As the chatbot interacts directly with website visitors who will not necessarily realise that it is an AI system, the company must ensure that this is clearly communicated in order for the AI system to be used; for example, by the chatbot introducing itself as an AI system at the start of the conversation.

In specific cases, high-risk AI systems can also be affected by the requirements established by Art. 50 AI Act. This particularly applies to the deployers of AI systems that can (1) process the biometric data of natural persons (e.g. voice, facial expressions etc.) to infer their emotions or intentions (emotion recognition) or (2) assign the biometric data to certain categories (e.g. aspects such as sex, age, eye colour, tattoos, personality traits etc.).

Art. 50 AI Act also covers the deployment of AI systems used to generate or manipulate image, audio or video content that appreciably resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful. In this case, certain transparency obligations are imposed on companies that assume the role of a deployer of such AI systems.

[3] AI Act: Annex III

Practical example
An agency deploys an AI system that generates synthetic video and image content for ad campaigns. The system uses deep-fake technology to create realistic-looking videos in which people (who have not actually taken part in the ad) advocate the advertised product. This synthetic content is so convincing that the average consumer could think the recordings are real. Although the company does not use any actual people in the videos, it ensures that the synthetic content is clearly labelled with a notice. Text appears at the start of the video explaining that the scenes shown were artificially generated and that no real people were involved. To ensure transparency, the notice is also visibly displayed on the company's website and on social media. As this synthetic content looks realistic but has clearly been labelled as synthetic, the company ensures that consumers are in no way misled.

If, on the other hand, an AI system has simply corrected the colours in a video to make them look bolder or has controlled the focus of the camera to make the video as sharp as possible, these videos are not classed as synthetic as defined by Art. 50 AI Act.

Texts are classed as synthetic if, for example, they have been created by a generative AI system on the basis of specific prompts. If, on the other hand, AI is simply used to perform a grammar check, this does not significantly alter the text and it is therefore not classed as synthetic.

AI systems with minimal risk

These include all other AI systems that do not fall into any of the three aforementioned categories for AI systems and that do not, therefore, pose any risk to the health, fundamental rights or safety of natural persons. Accordingly, they are not subject to any special mandatory requirements under the AI Act.

Practical example
A company uses an AI-based spam filter to automatically filter out undesired e-mails from users' inboxes. The AI system differentiates spam from legitimate messages by analysing patterns in the e-mails, such as sender addresses, keywords and suspicious links. The AI Act does not establish any special requirements for this AI system.

General-purpose AI model

In addition to AI systems, there is also a separate category for GPAI models (Art. 51 et seq. AI Act). GPAI models are designed for general results and have a wide range of potential uses. In other words, they can perform multiple different tasks rather than having been developed for a specific, limited purpose. They provide a general basis that developers can build on to create AI systems. As such, GPAI models always form part of an AI system from a legal perspective. GPAI models can be brought to market in various ways; for example, via an application programming interface (API) as a Model as a Service. GPAI models can also be modified or developed into new models. GPAI models differ from AI systems and are separately regulated in the AI Act.

Roles under the AI Act

The AI Act applies to a broad range of actors. For companies and public authorities in Switzerland, the roles of 'provider' and 'deployer' are of particular relevance.

Provider
A natural or legal person, public authority or agency that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name.

- *Placing on the market* means the first making available of an AI system or a general-purpose AI model on the Union market;
- *Putting into service* means the supply of an AI system for first use directly to the deployer or for own use in the Union;
- As an exception, anyone who essentially assumes the role of provider (especially in connection with high-risk AI systems) is also classed as a provider.

Practical example
A medium-sized company commissions an external service provider to develop a chatbot for it. This chatbot is not only intended to alleviate the workload of the company's support team but also to respond to customer queries on the website. The chatbot is put into service under the name of the company, which is therefore considered to be the AI system's **provider**. As the AI system is also used internally, the company is also a **deployer**. In this situation, the external service provider that helped the company to develop the AI system is not assigned a role in accordance with the AI Act.

Deployer
A natural or legal person, public authority or agency using an AI system under its authority.

- Use of an AI system under its authority – this distinguishes the mere enjoyment of an AI system from the use of an AI system as a proprietary tool;
- If the company uses an AI system (e.g. in the field of HR, in relation to customers etc.) to make a certain task simpler, more efficient etc., an AI system is deployed;
- People who use an AI system solely for personal, non-professional purposes are NOT deployers.

Practical example
A Swiss company provides its employees with user rights for ChatGPT or Copilot. These are used to generate images and create e-mails, presentations, blog posts, summaries, translations and other texts in a work context. The AI-generated content is not only aimed at people in Switzerland, but also at people in the EU; for example, in the form of e-mails or website texts. The company is a **deployer** of the AI system.

Various implementation deadlines

Although the AI Act already entered into force on 1 August 2024, various deadlines for implementation have been established. According to these, the standards will only fully enter into force 24 months after this date. The provisions will become applicable in a phased manner, with some having to be implemented sooner than others. For example, compliance with the provisions on prohibited AI systems has already been mandatory since 2 February 2025.

Extraterritorial effect

Particular attention should be paid to the AI Act's 'extraterritorial effect', especially in relation to Switzerland. In spite of Switzerland not being an EU member state, the AI Act can still be directly applicable to companies based in Switzerland, even if they have neither their registered office nor a branch office in the EU. This is the case in the following situations:

- The company is a provider of an AI system that is placed on the market or put into service in the EU.
- The company is a provider of a GPAI model that is placed on the market in the EU.
- The company is a provider or deployer of an AI system that generates output (e.g. a forecast, recommendation or decision) that is used in the EU. This rule aims to prevent EU companies from outsourcing high-risk systems, which ultimately affect people in the EU, to providers in third countries.
- Finally, the AI Act also applies to product manufacturers that place an AI system on the market or put it into service in the EU together with their product and under their own name.

The AI Act could also indirectly affect companies in Switzerland, due to customers who operate within the EU demanding compliance with it. This could force companies based in Switzerland to adapt to EU regulations in order to remain competitive on the European market. The AI Act can therefore indirectly affect companies in Switzerland via these market mechanisms.

Companies that are directly or indirectly affected by the AI Act therefore place great focus on the provisions established within it. In particular, companies that use AI systems provided by other companies assess the AI systems and then analyse their role in accordance with the AI Act together with their associated obligations.

AI law in Switzerland

At present, there is no overarching, horizontal AI legislation in Switzerland. However, developments in the EU also influence Swiss policy and with that the country's regulatory landscape. On 22 November 2023, the Federal Council instructed the Federal Department of Environment, Transport, Energy and Communications (DETEC) and the Federal Department of Foreign Affairs (FDFA) to prepare an overview of potential regulatory approaches in the field of AI. This overview (consisting of three reports) was presented on 12 February 2025 as an answer to the future legal framework conditions for the deployment and development of AI in Switzerland. Based on the reports from the Federal Office of Justice (FOJ) and the Federal Office of Communications (OFCOM), the Federal Council decided to sign the Council of Europe Framework Convention on Artificial Intelligence and transpose the principles of this into national law. In contrast to the EU AI Act, the AI Convention does not stipulate any specific measures but instead allows contract parties a great deal of discretion when implementing the principles.

Many of the principles of the AI Convention are already being fulfilled at federal level. However, Swiss law also contains provisions that do not go far enough in comparison to the obligations established in the Convention. In this regard, the Federal Government sees a particular need for action in the fields of transparency and supervision, safe innovation, legal remedies and procedural guarantees. The key principle of transparency, in particular, makes it possible to improve the effectiveness of the existing legal framework (e.g. with regard to equality and non-discrimination as well as data protection). Existing laws in Switzerland do not yet provide for any provisions in relation to the other principles established by the Convention. This particularly applies to the topics of 'risk and impact management' and 'effective oversight mechanisms'.

Transparency means...

- that people must be able to tell that they are interacting with a machine rather than a natural person, or that content has been generated by an AI system ('recognisability');
- that people can understand how an AI system came to a certain prediction, recommendation or decision, or how the AI system created certain content ('traceability').

Where legislative amendments are needed, these should be as sector-specific and principle-based as possible; cross-sectoral regulations should only be adopted in central areas that are of relevance to fundamental rights, such as data protection law. The Federal Council rejects the creation of an overarching AI law such as that in the EU, partly because many existing laws are already applicable to the use and development of AI technology. In addition to legislative amendments, there are plans to introduce several non-legally binding measures for the implementation of the AI Convention (e.g. self-declaration agreements and industry solutions). By combining legislative amendments and additions with the non-legally binding accompanying measures, the Federal Council is consciously using less strict regulation to ensure that Swiss companies can remain competitive on the global market. Whereas large companies have to comply with EU regulations when operating there anyway, start-ups in Switzerland benefit from less bureaucracy. They can therefore place greater focus on developing new AI technologies, which can offer them a competitive advantage.

AI Governance using Swisscom as an example

Even if no new legal provisions are expected to enter into force until 2028, it is still worth monitoring the legislative process and implementing new requirements internally at an early stage. AI Governance can help companies meet both current and future legal requirements. It makes it possible to avoid potential legal pitfalls and gives companies confidence in their legally compliant use of AI technology.

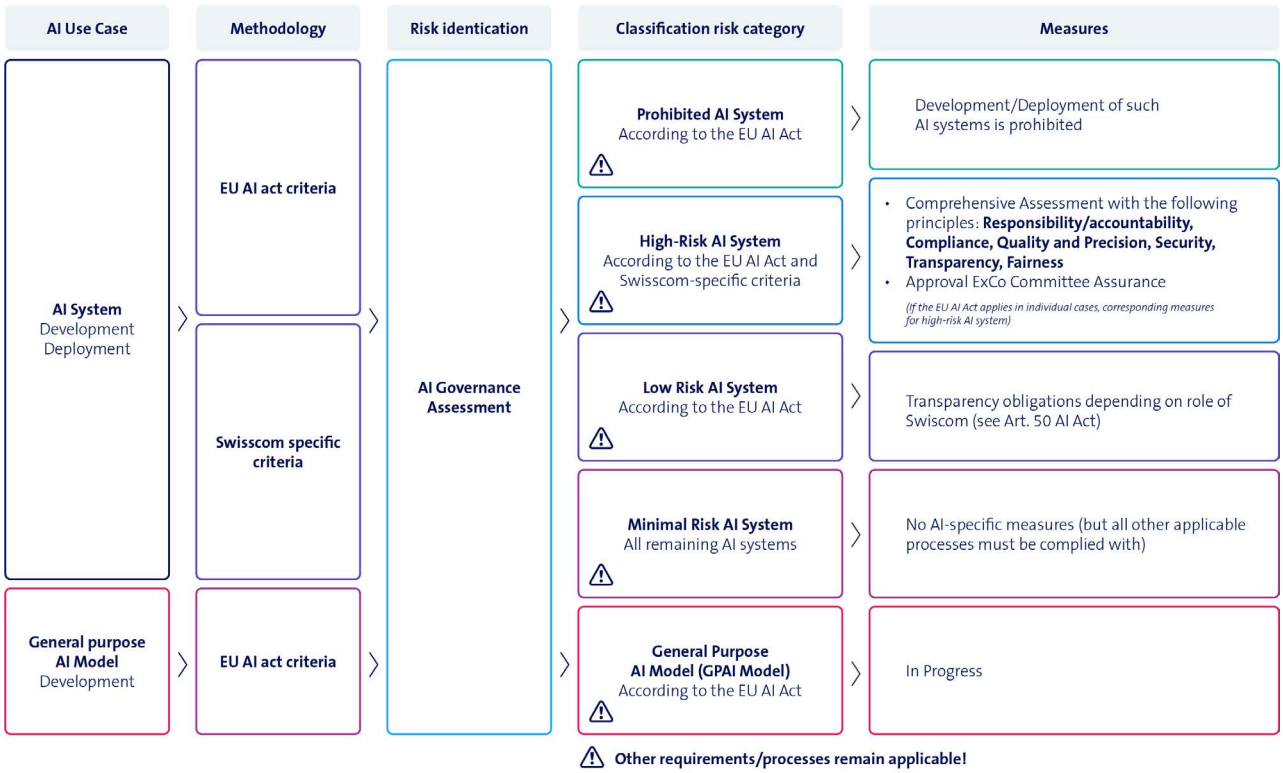
AI Governance ensures that companies use AI responsibly, ethically, legally and efficiently. It comprises a system of rules, processes, organisational measures and controls, which manages the development and deployment of AI systems as well as the development of GPAI models.

Solid AI Governance is essential for companies for several reasons. Firstly, it enables compliance with regulatory requirements, as the legal environment surrounding AI is becoming increasingly complex – for example, due to the extensive scope of the EU AI Act. Secondly, it helps to create trust by not only considering legal requirements but also ethical and social ones. This strengthens the trust of customers, partners and other stakeholders. Furthermore, clear AI Governance offers a competitive advantage, as it signalises transparency and responsible actions while also promoting innovation within safe framework conditions. Companies that implement sophisticated AI Governance at an early stage not only protect themselves from a legal standpoint but can also position themselves more successfully and in a more future-proof manner over the long term.

Swisscom's AI Governance follows a risk-based approach and establishes clear requirements for dealing with AI projects. These apply to the development and deployment of AI systems as well as the (further) development of GPAI models. To ensure that all requirements are met, Swisscom has developed an 'AI Governance Assessment' and has closely integrated this into existing Governance structures.

The assessment starts by determining the role played by Swisscom and whether the use case is an AI system or a GPAI model. Swisscom bases these determinations on the definitions established in the AI Act. In the next step, the AI project is categorised into one of five risk levels on the basis of the criteria established in the AI Act and additional, internal Swisscom criteria:

1. Prohibited AI systems
2. High-risk AI systems
3. Low-risk AI systems
4. Minimal-risk AI systems
5. GPAI models



Depending on the category, it is not only necessary to comply with different requirements but also to perform different review steps. For example, when categorising AI systems as high risk, certain basic principles are examined comprehensively and in detail: accountability, compliance, transparency, quality and precision, safety and fairness. A comprehensive review is particularly important in these cases, as these AI systems pose a high risk to people's fundamental rights and safety, meaning that they can also be critical to Swisscom's reputation. The Swisscom ethics board is involved with regard to the basic principle of fairness. High-risk AI systems then always require final approval from the ExCo Committee Assurance.

Experience gained to date has shown that most AI systems reviewed in the next few years will fall into the 'low risk' and 'minimal risk' categories. If an AI system is categorised as a 'minimal-risk AI system', no AI-specific requirements need to be complied with. However, it is important to bear in mind that additional requirements from other internal processes must always be observed.

Recommendations

In order to make informed decisions, it is essential to have a sound understanding of the basic legal principles. We have summarised the most important points as follows:

Most legal requirements for IT projects are based on existing laws that apply independently of AI technologies, such as the Swiss Federal Act on Data Protection. These requirements have to be met in both 'classic' and AI-based projects.

There are also new, specific AI regulations that companies should keep an eye on. The EU AI Act not only affects companies within the EU, but can also be of relevance to companies in Switzerland, as its effects can extend beyond EU borders (directly or indirectly via market mechanisms). Furthermore, the Federal Council is planning its own Swiss regulations on the use of AI technology, which will add further specifics to national legislation with regard to AI systems and GPAI models.

With regard to the EU AI Act, companies should pay particular attention to the following points:

- **Use of AI technology in the company:** Analyse where and how AI technology is already in use within the company and what future usage is planned.
- **Review of the definition of an AI system:** Check whether the AI technology planned for development or deployment falls under the definition of an 'AI system'.
- **Assessment of the GPAI model:** Where relevant, check whether a GPAI model acts as a basis for an AI system, as well as whether it meets the requirements established by the AI Act and is 'recognised' in the EU.
- **Determination of the company's role:** Companies should assess whether they are an AI system provider or deployer.
- **Risk classification:** Determining the risk level at an early stage helps to avoid unnecessary regulatory burdens and focus on the key requirements.

Based on this list, we have derived three recommendations:

1. Start strategically and with a clear plan
When implementing AI projects, the focus should lie on a clear business case instead of getting carried away by hype. Ask yourself what specific added value the use of AI in your company offers. Should it reduce costs, improve customer satisfaction or generate new revenue sources?

Choose the appropriate project category based on your risk appetite and the specific goals you want to achieve. If you want to start from a clear, manageable point, you should focus on AI products or functions within your existing product suites. This enables simple implementation that builds on established systems. If you are willing to take a little more risk, you can develop user-defined processes based on large language models. This offers you greater flexibility with regard to automation and analysis. For companies with greater AI expertise and extensive data resources, the next step can be to create your own machine learning or deep learning models. This approach enables more in-depth personalisation and greater control of the systems developed but also requires careful planning and the right skills.

A gradual approach enables controlled implementation and reduces potential risks.

2. Use AI Governance and AI as a competitive advantage

AI offers enormous opportunities for companies – from optimisation of processes through to cost savings and new business models. Do not be deterred by legal requirements. Most stipulations can be successfully implemented through intelligent AI Governance. Those who create a solid basis for reviewing the requirements at an early stage promote creativity and AI innovation within a safe remit and can thus minimise the risk of startling (legal) mistakes. Companies that want to realise multiple AI projects should establish company-wide AI Governance at an early stage. This not only creates a uniform basis for future developments but also helps to make use of synergies between different projects.

Please bear in mind that AI Governance does not have to be perfect from the outset. The initial version can be kept lean and pragmatic as long as it is tailored to the company's specific requirements. The following best practices have proved successful:

- **Risk-based approach:** AI systems should be categorised on the basis of their risk potential. Not all AI applications are subject to strict regulatory requirements. Companies should divide their projects into different risk levels and define suitable measures for each level.
- **Iterative process:** AI Governance is not a static set of rules, but an ongoing process. Companies should regularly assess whether existing structures are still in line with technological and regulatory developments.
- **Internal communication and training:** AI Governance can only be successful if there is a company-wide awareness and understanding of it. It is therefore essential to actively involve and continually train employees.
- **Interdisciplinary working group:** AI projects do not only affect the IT department. Successful implementation requires expertise from different areas and departments (e.g. including legal, security, the ethics board and other specialist departments).
- **Management integration:** Management support is critical for the success of AI Governance. To increase acceptance, the company management should be actively involved in the development and implementation.
- **Adaptation to suit company size:** Simple AI Governance with a few guidelines and control mechanisms may suffice for smaller companies; for larger companies with more complex structures, on the other hand, more extensive and detailed regulations are often required. It is important to strike a good balance between the scope of the AI Governance and the practical benefits for the company.

Ultimately, AI Governance is a strategic necessity. It helps to minimise risks, meet regulatory requirements and increase trust in AI technologies.

3. Involve the right stakeholders from an early stage

For AI projects to be implemented in a smooth and legally compliant manner, all relevant internal and external stakeholders should be involved from an early stage. This includes in particular:

- experienced service providers that offer technical expertise and can professionally support the implementation;
- the person or department responsible for AI Governance or – if AI Governance has not yet been implemented – the internal legal department, data protection officer and other internal stakeholders (e.g. from the security or purchasing departments);
- in some cases: specialised law firms to ensure that all regulatory requirements are fulfilled and legal risks are minimised.

FAQ

1. A company based in Switzerland develops an AI system. Under what conditions is the EU AI Act applicable?

The AI Act is not only applicable to companies in the EU but can also be of relevance to companies with their registered office in Switzerland. If the Swiss company in question develops an AI system that is placed on the market in the EU or deployed by an EU-based company, it is affected by the AI Act. The AI Act is also of relevance to the company if the developed AI system is used in a second step (by the company itself or by a different company) and the output from the AI system (e.g. a forecast, recommendation or decision) is used in the EU.

2. What classes as 'development' with regard to GPAI models and AI systems?

'Development' in the context of a GPAI model usually refers to an action that goes beyond mere parameterising, prompting or delivering input. The differentiation depends on whether the underlying structure or training knowledge of the GPAI model is changed. Fine-tuning a GPAI model, whereby it is further trained with additional data or special adjustments, leads to a change in the GPAI model's training knowledge and thus its programming. This kind of action would be regarded as development, as it actively modifies the original functions of the model and adapts them to suit the company's specific requirements. In contrast, the use of retrieval-augmented generation (RAG) relates to the modification of the input entered in the system without changing the internal model structure or training. This process merely involves modifying the input to achieve certain results, which is not regarded as development in the traditional sense.

Development in the context of an AI system means that the entire AI system is developed – i.e. the software itself as well as the user interface – to make the AI system suitable for use for a particular purpose. The development of an AI system does not depend on whether the AI model on which it is based has been (further) developed or the AI system is built on an unmodified model.

3. What happens if a company (co-)develops an AI system for a customer but places it on the market or puts it into service under the name of another company or trademark rather than its own? (E.g. through secondment of personnel, support with expertise etc. but without final responsibility)

To be classed as a provider, a company must place an AI system on the market or put an AI system into service under its own name or trademark. It does not matter who has developed the AI system, as the 'putting into service'/'placing on the market' under its own name or trademark is the decisive factor.

From a legal perspective, this means that a company cannot be a provider in the said case, as it does not fulfil a mandatory criterion of the legal definition of a provider.

If a company (co-)develops an AI system (e.g. through expertise, secondment of personnel etc.) and permissibly affixes the name or trademark of the customer to it, the company has acted solely on behalf of the customer, who is in turn regarded as the provider. Displaying the customer's name or affixing its trademark – or permitting a third party to do so – can be regarded as a declaration that the company is taking on the role of the AI system's provider and therefore the associated responsibilities.

4. A company operates in Switzerland in a sector that is already highly regulated. Does the AI Act change anything about the existing regulations?

The provisions established in the EU AI Act do not change the existing national rules of law in Switzerland or other non-EU countries. AI systems that are used as safety components for one of the following products or that are themselves one of the following products are classed as high-risk AI systems under the AI Act: radio equipment, machinery and associated products, toys, lifts, recreational craft and personal watercraft, other vehicles, cableway installations, personal protective equipment, medical devices (extract from Annex I of the AI Act). These are sectors that are already strictly regulated – both in the EU and in Switzerland. If the company in Switzerland falls directly within the scope of the AI Act, it must comply with the additional, strict rules for high-risk AI systems. If the product is only intended for the Swiss market or a non-EU market, the new provisions of the AI Act do not have to be observed. However, Switzerland may supplement strictly regulated areas with new AI rules in order to maintain market access in the EU (key factor: product certification) and so that Swiss rules will continue to be recognised as equivalent (to prevent the need for additional EU certification for Swiss products).

5. Requirements in relation to high-risk AI systems: what special requirements apply to high-risk AI systems with regard to the EU AI Act?

Depending on the role of the company, different requirements must be observed under the AI Act. Swiss companies can take on the role of provider or deployer.

The requirements that apply to providers as defined by the AI Act (Art. 8–15) include (but are not limited to) the following:

- In-depth risk management must be used, especially in the form of risk assessments that are repeated over the entire life cycle of the AI system with appropriate tests of the AI system and measures to monitor identified risks;
- The data used for training, inspections and tests must fulfil certain quality criteria;
- Detailed technical documentation of the AI system must be created and maintained;
- The AI system must automatically create logs in which it suitably records what it does so that its correct functioning can be monitored over time.

To prove compliance with these requirements, providers in Switzerland who fall within the scope of the EU AI Act must, for example, keep documentation, have a quality management system in place and store the logs generated by their AI systems.

In accordance with the AI Act (Art. 16–22, 26), **deployers** must ensure, among other prerequisites, that:

- the AI system from the provider fulfils all requirements established by Art. 8–15 (i.e. that the provider has adhered to the requirements);
- they have a quality management system (like the provider);
- they keep legally stipulated documents at the disposal of the responsible national authorities for ten years from the date of placing on the market or putting into service of the high-risk AI system (documentation keeping);
- the logs that are automatically generated by the high-risk AI system are stored for at least six months (retention of automatically generated logs).

Specific requirements also apply to the roles of importer and distributor.

6. Who is liable in Switzerland if an AI system causes damage and are there any specific AI liability rules?

The current Swiss liability law with its open general clauses also covers technical developments in the field of AI. In accordance with the general conditions of liability established in Art. 41 Swiss Code of Obligations (CO), any person who unlawfully causes damage to another, whether wilfully or negligently, is obliged to provide compensation. As in other areas, the prerequisites for non-contractual liability are therefore damage, illegality, causality and fault.

The existing regulations on strict liability and insurance obligations (e.g. for driving) seal the liability gaps in key AI application areas. Due to the technical development of products, including with regard to AI, the modernisation of the Product Liability Act could become a matter for discussion in Switzerland at a legal level.

7. What are the differences between the requirements of the Council of Europe's AI Convention, signed by the Federal Council, and the European Union AI Act?

The Council of Europe (not to be confused with the EU Council) is an international organisation with 46 members that is committed to promoting democracy, respect for human rights and the rule of law. The AI Convention is a document of principles with a strong focus on fundamental rights. It provides a basis for common binding standards and practices in the regulation of AI and focuses on aspects such as data protection, privacy and protection against discrimination. The Council of Europe's AI Convention must first be signed by the Council of Europe member states and then transposed into national, domestic law. The EU AI Act, on the other hand, is an EU law that is directly applicable. It regulates the topic of AI comprehensively and in great detail, stipulating specific requirements with a particular focus on the risk classification and minimisation of AI systems.

8. Are there any other international AI regulations that could affect companies in Switzerland?

Further to the EU AI Act, there are other international AI regulations with extraterritorial effect that could affect Swiss companies. An analysis by OFCOM and the FDFA has shown that very different approaches to the regulation of AI exist around the world and that no standardised model has yet prevailed. Many countries do at least have an AI strategy or action plan, but at the end of 2024, few had yet introduced binding legislation. AI regulations from other countries are of particular relevance if companies operate in these countries or offer services to their citizens. In countries such as Canada, Brazil and South Korea, Swiss companies can also be affected by legally binding rules in the field of AI. The EU AI Act is the world's first comprehensive, binding AI legislation, the scope of which is much broader than any other legislation to date.

9. What penalties do companies face if they do not comply with the AI Act?

The AI Act obliges member states to transpose offences subject to penalties into national law. The AI Act sets out a three-tier penalty system depending on the severity of the infringement: the highest administrative fine level applies to infringements of the prohibited practices in relation to AI systems, with maximum fines of 35 million euros or 7% of the total annual turnover. The medium administrative fine limit apples to certain breaches of obligations in the area of high-risk AI systems, breaches by notified bodies with regard to internal organisational obligations and conformity assessment procedures, and breaches of transparency obligations for the providers and deployers of certain AI systems. In such cases, administrative fines of up to 15 million euros or 3% of the annual turnover can be imposed.

The lowest administrative fine limit comes into play if inaccurate, incomplete or misleading information is provided to notified bodies or national authorities. In this case, fines of up to 7.5 million euros or 1% of the annual turnover can be imposed.

The AI Act allows member states to establish additional penalties (e.g. warnings and other non-monetary measures) in addition to the administrative fines.

This document is intended to provide an overview in relation to Swisscom's data and AI Governance services. It does not claim to be exhaustive or without error. Furthermore, it does not constitute an offer and is not intended to have any other legal effects, especially not in relation to existing or future contracts.

Swisscom presents its opinion and views in this document, including with regard to legal assessments – for example, concerning data protection law – but does so without guarantee or liability. Swisscom does not provide legal advice, either in this document or in its consultations. It is the sole responsibility of each party concerned to carefully study its own circumstances and subsequently draw its own conclusions and define requirements. Swisscom recommends that all parties consult experts as necessary to clarify any questions that arise, especially with regard to data protection law.

This document and its content are protected by copyright. Any use other than personal use requires the prior written consent of Swisscom.