

# SWITZERLAND

Martina Arioli  
*Arioli Law*

This chapter forms part of:

ARTIFICIAL INTELLIGENCE  
*Law Over Borders Comparative Guide 2024*

[www.globallegalpost.com/lawoverborders](http://www.globallegalpost.com/lawoverborders)



## INTRODUCTION

Switzerland has been a considerable player in the global artificial intelligence (AI) industry measured by patent and start-up activities, leveraging its strong foundation in research, innovation, and technology. The country is home to numerous AI start-ups and established tech companies, supported by a robust ecosystem that includes world-class academic institutions such as ETH Zurich and EPFL. These institutions contribute to cutting-edge research and development, fostering a culture of innovation and excellence.

Swiss AI enterprises span various sectors, including healthcare and medical devices, finance, manufacturing, and robotics. In healthcare, AI is developed and deployed in the fields of diagnostics, personalised medicine, and healthcare management. The financial sector benefits from AI applications in fintech, risk management, personalised customer services, and process automation. Switzerland's industrial landscape also sees AI integration in optimising manufacturing processes and advancing precision engineering.

Given that Switzerland is not a member of the European Union (EU), the EU AI Act will not directly apply in Switzerland. Switzerland currently does not have specific laws, statutory rules, or regulations that directly govern AI. The Federal Council has directed the Federal Department of the Environment, Transport, Energy and Communications (DETEC) to assess potential regulatory approaches for AI by the end of 2024 as a basis for initiating the legislative process. Within the *Plateforme Tripartite*, policymakers are currently engaging with industry stakeholders, academia, and international partners to establish a regulatory framework that balances innovation with ethical considerations and societal impacts.

A central principle of Swiss law is that it aims to be largely technology-neutral and principle-based, and it favours sectoral regulations over horizontal laws. Accordingly, the existing statutory provisions and regulations apply to AI. However, future Swiss AI regulations should align with international regulatory frameworks and, in particular, the EU AI Act, to avoid fragmentation.

As Switzerland harmonises its technical regulations with those of the EU Member States (its most important trading partners), and, in particular, in accordance with the Federal Act on Technical Barriers to Trade (THG), corresponding proposals in the EU are likely to have a major influence on future regulation in Switzerland.

Further, Switzerland actively participates in shaping global AI regulations, engaging in discussions within international bodies such as the Council of Europe Committee on Artificial Intelligence. This proactive involvement underscores Switzerland's commitment to harmonising its regulatory framework with global principles and contributing to the development of coherent international AI policies.

## 1. CONSTITUTIONAL LAW AND FUNDAMENTAL HUMAN RIGHTS

### 1.1 Domestic constitutional provisions

The Federal Constitution includes a suite of human rights that are relevant in the context of AI, including human dignity (Article 7), equality before the law

(Article 8), protection against arbitrariness and protection of good faith (Article 9), right to life and personal liberty (Article 10), protection of children and young people (Article 11), protection of privacy (Article 13), freedom of expression and information (Article 16), freedom of the media (Article 17), freedom of science (Article 20), freedom of the arts (Article 21), economic freedom (Article 27), judicial proceedings and guarantee of legal recourse (Articles 30 and 29) and political rights (Articles 34 and 39).

### 1.2 Human rights decisions and conventions

Currently, there are no decisions by Swiss courts or ongoing court cases made public. However, the decisions rendered by the European Court of Human Rights based upon the European Convention on Human Rights are of great importance to Switzerland.

## 2. INTELLECTUAL PROPERTY

The discussion in Switzerland on AI and IP focus predominantly on input- and output-related concerns. To date, academic discussions have not yet widely addressed concerns about exclusive control over essential AI technologies as gatekeepers. However, to encourage AI innovation, it may be necessary to allow broader access to data and other resources needed for development, possibly through specific exemptions or carve-outs in intellectual property laws or competition laws.

### 2.1 Patents

The Federal Act on Patents for Inventions (FPA) requires that a patentable invention must be the result of human intellectual effort. AI-generated outcomes, lacking direct human contribution to the inventive process, do not fulfil this requirement. Consequently, purely AI-generated inventions cannot be patented under current Swiss law. However, if an AI-assisted process leads to an invention where human creativity and ingenuity play a significant role, the resulting invention may be patentable. The human inventor(s) must, however, be able to demonstrate substantial contribution to the inventive process.

### 2.2 Copyright

Under the Federal Copyright Act (CopA), only works originating from a human author are protected by copyright. If an individual uses AI as a tool, but the creative input is primarily human, copyright protection is applicable to the output.

Conversely, if the “creative service” is rendered by AI, the work does not originate from a human and therefore is not protected by copyright, allowing free use of the output. However, if the AI-generated output contains identifiable copyrighted material, those portions remain protected, and the output can only be used with permission from the copyright holder.

There is currently no consensus in Switzerland on the copyright implications of using content for AI training. Switzerland is closely monitoring the court cases in the United States and the United Kingdom on this topic.

### 2.3 Trade secrets and confidentiality

In Switzerland, trade secrets are protected primarily through the Federal Act against Unfair Competition (UCA). Article 6 of the UCA explicitly prohibits the unauthorised use or disclosure of manufacturing or trade secrets. This provision safeguards confidential business information against misappropriation by competitors or other third parties.

Trade secrets encompass any confidential business information that provides a competitive edge, provided it is subject to reasonable efforts to maintain its secrecy. Protection under the UCA requires that the information remains undisclosed and retains economic value due to its confidentiality.

### 2.4 Notable cases

Currently, there are no court cases in Switzerland made public that deal with AI, IP and trade secrets.

## 3. DATA

Switzerland is not a member of the EU, thus the entire suite of data-related EU Regulations and Directives do not apply. However, Switzerland is closely monitoring the legislative developments in the EU and assessing whether adaptations to Swiss law are sensible and/or necessary.

### 3.1 Domestic data law treatment

The Federal Act on Data Protection (FADP) was completely revised on 1 September 2023 in order to adapt to Convention 108+ of the European Council and the EU General Data Protection Regulation (GDPR) and also to secure Swiss adequacy status by the European Commission. The FADP is technology-neutral and, thus, applies to AI as well. If personal data is being processed in the development or use of an AI system, all the general data protection principles and obligations must be complied with.

Specifically, Article 21 of the FADP governs automated individual decisions: controllers should inform data subjects of any decision based solely on automated processing which produces legal effects concerning him or her or significantly affects them. Further, upon request, controllers should give data subjects the opportunity to state their point of view, and such data subjects may request that the automated individual decision be reviewed by a natural person. However, these provisions do not apply if the automated individual decision is directly related to the conclusion or performance of a contract between the controller and the data subject or the data subject has expressly consented to the decision being taken by automated means. The Swiss Parliament confirmed its view on 17 May 2024 that Article 21 of the FADP shall only apply in the event that the decision is based solely on automated processing and shall not be amended for the time being.

In November 2023, the Federal Data Protection and Information Commissioner (FDPIC) has pointed out (the obvious) that the FADP shall apply to AI as well. However, the FDPIC seems to interpret the FADP in view of AI in a highly extensive

manner, in particular in view of transparency obligations on manufacturers, providers and users of AI who, according to the FDPIC, must:

- make the purpose, functionality and data sources of AI-based processing transparent;
- inform the data subjects if they are interacting with a machine; and
- clearly indicate if the personal data of data subjects is being processed to improve self-learning programs.

Further, together with nine other national data protection authorities across the globe, the FDPIC published a joint statement to social media platform operators in August 2023 on the protection of personal data against data scraping. Social media companies and other website operators are required to actively provide information on how they protect their customers against data scraping and on the measures their customers can take in order to protect their own data.

### 3.2 General Data Protection Regulation

Given that Switzerland is not a member of the EU, the GDPR does not apply directly in Switzerland (see above, Section 3.1).

### 3.3 Open data and data sharing

The Federal Act on the Use of Electronic Means for the Fulfilment of Official Tasks (EMBAG), which entered into force on 1 January 2024, is dedicated to open government data. It defines the principle of free access to open government data (OGD) and introduces the principle of “open by default” by stipulating that all data published by the Federal Administration that is subject to Article 10 of the EMBAG must be published free of charge, promptly, in machine-readable form and in an open format on the internet. The administrative units subject to this Act shall make publicly accessible the data that they obtain or generate to fulfil their statutory tasks and that are stored electronically and in a structured manner. The central portal for OGD in Switzerland is *opendata.swiss*. The data can then be used freely, (provided the source is cited) which can be highly useful for training of AI applications.

### 3.4 Biometric data: voice data and facial recognition data

Biometric data is considered sensitive data under the FADP, and its processing must, therefore, comply with the general data protection principles and obligations set out under the FADP. There are no statutory or regulatory provisions in Switzerland specifically addressing this technology. In particular, there are, to date, no explicit lists of forbidden applications or use cases in certain contexts such as emotion recognition in the workplace or facial recognition in public spaces comparable to the EU AI Act.

## 4. BIAS AND DISCRIMINATION

### 4.1 Domestic anti-discrimination and equality legislation treatment

Whilst the Federal Constitution contains the fundamental right of equality before the law (Article 8), protection against discrimination is, unfortunately, not

comprehensive in Swiss law as it is enshrined only in the Federal Act on Gender Equality as well as in the Disability Equality Act.

## **5. CYBERSECURITY AND RESILIENCE**

### **5.1 Domestic technology infrastructure requirements**

Switzerland does not have a comprehensive cybersecurity law. The Federal Act on Information Security (ISAC), effective since January 2024 and already under revision again, mandates that federal agencies, private institutions that fulfil public tasks, and, to a certain extent, critical infrastructure providers, implement robust information security practices. Further, there are sector-specific statutes and regulations (in particular, in the finance and healthcare sectors) that contain cybersecurity related provisions. Like the ISAC, such sector-specific regulations contain generic, largely technology-neutral obligations that do not address AI specifically.

## **6. TRADE, ANTI-TRUST AND COMPETITION**

### **6.1 AI related anti-competitive behaviour**

Simulations and empirical evidence show that algorithms can learn collusive strategies, leading to prices above competition and pricing algorithms can lead to higher prices, algorithmic price discrimination and potential tacit collusion (“algorithmic collusion”). From a legal perspective, the biggest challenges today are that collusion without explicit agreements is not prohibited and that deep learning algorithms often work as a black box leaving no traceability of the decision-making processes. This makes it more difficult to identify competition law infringements.

### **6.2 Domestic regulation**

Current legislation in Switzerland only takes limited account of algorithmic practices. There is a legal gap regarding the specific regulation of AI and competition law. An amendment to the Cartel Act may be necessary to establish clear guidelines and measures to combat algorithmic collusion, price discrimination, exclusionary behaviour and self-preferencing by digital platforms. Further, given that mergers involving algorithms can facilitate collusion, there are calls for a revision of the merger guidelines and an obligation to analyse existing algorithms and their potential collusive effects prior to a merger.

## **7. DOMESTIC LEGISLATIVE DEVELOPMENTS**

### **7.1 Proposed and/or enacted AI legislation**

As indicated under Section 1, the Federal Department of the Environment, Transport, Energy and Communications must publish its assessment of potential regulatory approaches for AI by the end of 2024 as a basis for initiating the legislative process in 2025. Currently, however, heated discussions are underway as there are mainly two differing views. On one hand, given that the EU is the

main trading partner of Switzerland, and the EU AI Act has not only extensive extraterritorial effect but also establishes a system of conformity assessment procedures for high-risk AI systems involving notified bodies, there is also a strong argument for following an approach similar to the EU AI Act to secure free trade. On the other hand, the notion of a specific law addressing a specific form of technology that applies across industries and sectors comparable to the EU AI Act is arguably alien to the Swiss law tradition: Swiss law aims to be principle-based and largely technology-neutral, and favours sectoral regulations over horizontal laws.

Further, the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, issued on 17 May 2024, will most likely form the guiding principle and essential basis for the legislative process in Switzerland. However, it pursues a largely self-regulatory approach as opposed to the prescriptive approach under the EU AI Act.

It remains to be seen how a future Swiss AI regulation(s) will align with international regulatory frameworks and, in particular, the EU AI Act, to avoid fragmentation.

## 7.2 Proposed and/or implemented Government strategy

The Federal Council defined AI as a central topic of the “Digital Switzerland” strategy back in 2018. The Government strategy is set out in the “Guidelines on Artificial Intelligence for the Confederation: General frame of reference on the use of artificial intelligence within the Federal Administration”, adopted by the Federal Council on 25 November 2020 and based upon the “Challenges of Artificial Intelligence” published by the Federal Council on 13 December 2019. The “Digital Switzerland” strategy and the Digital Foreign Policy Strategy 2021–2024 will serve as a reference framework.

The Guidelines of 2020 are intended to ensure a coherent policy with regard to AI and sets out seven guiding principles:

- 1) Putting humans at the centre. Dignity and well-being of people, protection of fundamental rights and the common good should be paramount.
- 2) Regulatory conditions for fostering the development and use of AI in Switzerland.
- 3) Transparency, traceability and explainability.
- 4) Accountability and liability. Responsibility cannot be delegated to machines.
- 5) Safety. AI systems must be designed to be safe, robust and resilient in order to have a positive impact and not be susceptible to misuse or misapplication.
- 6) Active participation in shaping the global governance of AI.
- 7) Involvement of all relevant national and international stakeholders.



## FREQUENTLY ASKED QUESTIONS (FAQS)

### **As a Swiss company that develops software and apps for Swiss multinational companies, does the EU AI Act apply to our company directly?**

The EU AI Act has an extensive extraterritorial effect in that it applies to providers of AI systems that are established outside the EU (EEA) to the extent that the output produced by the AI systems is intended to be used or actually is used in the EU. A Swiss company that develops software and apps may be deemed a “provider” within the meaning of the EU AI Act if it develops an AI system or General-Purpose AI (GPAI) model under its own name or trademark and falls within the scope of the EU AI Act if it:

- makes an AI system or GPAI model available on the EU market;
- supplies an AI system or GPAI model for a deployer to use in the EU market; or
- where the output of its AI system is used in the EU.

Providers that meet any of these criteria must comply with the EU AI Act irrespective of their place of establishment and location, and whether the AI system or GPAI is provided for payment or free of charge. In a literal interpretation, the EU AI Act applies even if the provider has made no attempt to aim its activities at the EU, does not know that the customer will use it in the EU (EEA) or even if the use of the output of the AI system in the EU (EEA) has been contractually excluded. Subsequent guidance (to be issued by the EU Office of AI) may clarify the position.

### **Our employees wish to use OpenAI’s ChatGPT. Do we need to inform our customers and business partners of the deployment of ChatGPT in order to comply with the Federal Data Protection Act?**

Transparency is an essential principle of the FADP (see Article 6, paragraphs 2 and 3 of the FADP). Pursuant to Article 19 of the FADP, controllers shall, when collecting personal data, provide data subjects with the information required to enable them to assert their rights under the FADP and to ensure transparent data processing. Accordingly, controllers must provide data subjects with information relating to their identity and contact details, the purpose of the processing and, where applicable, the recipients or categories of recipients to whom the personal data are disclosed, and, where applicable, the categories of personal data being processed, as well as (if applicable) the countries and guarantees deployed in the event of cross-border transfer.

The FDPIC mandates in a statement published in November 2023 that manufacturers, providers and users of AI systems must provide sufficiently transparent information on the functionality and the data sources utilised in AI-based processing. This is an extensive interpretation by the FDPIC that has no basis in the FADP.

In view of the current hype surrounding AI and the legal uncertainty in Switzerland, and consistent with the above, it may be wise to provide sufficient transparency information on the concrete use cases and the type of AI systems deployed, and amend Privacy Notices accordingly. However, for the use of ChatGPT or similar tools there is no information obligation under Swiss law.

*Continued on the following page.*

**AUTHOR BIOGRAPHY****Martina Arioli**

Martina Arioli established Arioli Law in 2013 in the heart of Zurich as one of the first one-woman pure technology law firms in Switzerland. Martina Arioli has been listed by Chambers Europe for TMT since 2019 and recognised as one of Switzerland's leading business lawyers since 2016 by Who's Who Legal. She has been selected as Thought Leader Data in Switzerland since 2019 and won the Client Choice Award Data Switzerland 2020. The renowned Swiss business magazine BILANZ has ranked Arioli Law amongst Switzerland's top law firms in TMT and IP law since the first ranking issued in 2017.

Martina Arioli is an experienced legal counsel, with more than 20 years of international practice, specialised in IT law, digital transformation, cloud and outsourcing. She has supported outsourcing engagements in all stages, from contract drafting, negotiating global and local agreements to implementation and transition, conflict mediation, termination and resourcing to new suppliers. Martina combines in-depth knowledge on complex contractual matters in outsourcing and information technology projects with the experience of implementing such global projects as in-house lawyer.

Previous positions include senior roles at Zurich Insurance Company and UBS AG, as well as the law firm Walder Wyss Ltd and TIMES Attorneys.

Martina studied law, philosophy and political science at the University of Bern where she graduated in 1996 (*magna cum laude*), passed the Bar in 1999 with excellence and received an LL.M. from the London School of Economics and Political Science (LSE) in IP in 2001. Since 2008 she has chaired a prestigious annual conference on data protection in Switzerland. She lectures law at various Swiss universities.