

SWITZERLAND

Martina Arioli
Arioli Law

This chapter forms part of:

ARTIFICIAL INTELLIGENCE

Law Over Borders Comparative Guide 2026

www.globallegalpost.com/lawoverborders

363

INTRODUCTION

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

Given that Switzerland is not a member of the European Union (EU), the EU AI Act does not directly apply in Switzerland. Switzerland has no horizontal AI statute in force as of 2026. The present framework is technology neutral and heavily sectoral and fragmented. AI is therefore governed primarily through existing rules on data protection, intellectual property, competition, contract, tort, financial regulation, medical devices, public law and fundamental rights.

Swiss policy has nevertheless moved materially. On 12 February 2025, the Federal Council decided that Switzerland should ratify the Council of Europe AI Convention and make the necessary amendments to Swiss law. Switzerland signed the Convention on 27 March 2025. The Federal Department of Justice and Police (FDJP), together with the Federal Department of Environment, Transport, Energy and Communications (DETEC), the Federal Department of Foreign Affairs (FDFA) and other federal offices, has been tasked with preparing a consultation draft by the end of 2026. That draft is expected to set out the legal measures required for implementation, particularly in the areas of transparency, data protection, non-discrimination and supervision, and to be accompanied by a separate package of non-binding measures.

Switzerland will not simply copy the EU AI Act. At the same time, it cannot ignore the EU framework. For many Swiss companies, the EU AI Act is commercially relevant through market-access, distribution and output-in-the-EU scenarios. In addition, Switzerland traditionally aligns parts of its technical product framework with the EU where this is necessary to reduce technical barriers to trade.

For that reason, the practical Swiss position is twofold. Domestically, AI is currently assessed mainly under existing laws, supplemented by non-binding guidelines and measures. Cross-border and commercially, however, Swiss businesses often need to analyse the EU AI Act in parallel.

1. CONSTITUTIONAL LAW AND FUNDAMENTAL HUMAN RIGHTS

1.1 Domestic constitutional provisions

The Federal Constitution contains a broad set of guarantees that may become relevant in AI matters. The most important are human dignity (Article 7), equality and non-discrimination (Article 8), protection against arbitrariness and protection of good faith (Article 9), personal liberty (Article 10), privacy and informational self-determination (Article 13), freedom of expression and information (Article 16), media freedom (Article 17), freedom of science (Article 20), freedom of the arts (Article 21), economic freedom (Article 27), and procedural guarantees, including the right to be heard and access to justice (Articles 29 and 29a). Depending on the use case, further guarantees may also be engaged, including political rights (Article 34) and sector-specific constitutional mandates.

These guarantees shape statutory interpretation, administrative discretion and judicial review. This is especially important in the public sector, where state use of AI must satisfy legality, public interest and proportionality.

1.2 Human rights decisions and conventions

Switzerland is bound by the European Convention on Human Rights, and Strasbourg case law influences Swiss debates on procedural fairness, surveillance, discrimination, freedom of expression, and algorithmic decision-making.

The leading published Swiss AI decision to date is the Federal Administrative Court's DABUS judgment (B-2532/2024, 26 June 2025), discussed in Section 2, below. Beyond that, Switzerland does not have a substantial body of published court decisions dealing specifically with AI.

2. INTELLECTUAL PROPERTY

The Swiss debate on AI and intellectual property has so far focused chiefly on three issues: inventorship and authorship; the protection status of AI-generated outputs; and the lawfulness of using protected content as training material.

2.1 Patents

The Federal Act on Patents for Inventions (PatA) 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.

The most important recent authority is the Federal Administrative Court's DABUS judgment. The court held that an AI system cannot be entered in the patent register as the inventor and that an application may not proceed without an inventor designation. At the same time, the court adopted a functionally relevant understanding of inventorship: a natural person may qualify as inventor where that person makes relevant contributions within the AI data-processing workflow, recognises the patentable result and applies for protection. Where AI is used as a tool within a human-led inventive process, patent protection remains possible, subject to the ordinary patentability requirements.

2.2 Copyright

Swiss copyright law protects only works that are intellectual creations with individual character and are attributable to a human author. A purely machine-generated output with no human authorship is therefore unlikely to qualify for copyright protection under current Swiss copyright law.

Where a human uses AI merely as a sophisticated tool, the answer depends on the facts. If the human contribution remains sufficiently creative and shapes the protected expression, copyright may subsist in the output. If the allegedly creative contribution is in substance generated by the model and the human role is confined to functional prompting, selection or minor post-editing, copyright protection is far less certain.

Switzerland has no AI-specific text-and-data-mining exception comparable to the broader EU discussion and has not yet reached a consensus on training data in the context of copyright law.

2.3 Trade secrets and confidentiality

Swiss trade secrets are protected through a mix of unfair competition law, contract law, employment law and, in some constellations, criminal law. Article 6 of the Federal Act against Unfair Competition prohibits the exploitation or disclosure of manufacturing or trade secrets that one has improperly obtained or otherwise learned of improperly. In practice, however, contractual confidentiality architecture remains critical.

In the AI context, the core risks are operational rather than conceptual: confidential prompts and datasets fed into third-party tools; leakage through model fine-tuning or retention settings; access rights that are too broad; insufficient segregation in enterprise environments; and inadequate restrictions on vendor use of customer inputs and outputs. For most businesses, the real protection work is therefore done through governance, vendor contracting and internal controls, not through abstract references to trade-secret doctrine alone.

2.4 Notable IP cases

The key Swiss authority is the Federal Administrative Court's judgment B-2532/2024 of 26 June 2025 (DABUS) (see Section 2.1, above).

3. DATA

Switzerland is not a member of the EU. EU data legislation therefore does not apply domestically as Swiss law. That said, the practical relevance of EU law is often significant because many Swiss businesses process personal data cross-border, target EU markets or operate within multinational groups. Further, 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), in force in its revised form since 1 September 2023, is technology neutral and applies fully to AI-related processing of personal data. The essential principles therefore govern AI as they govern any other data processing: lawfulness, good faith, proportionality, purpose limitation, data accuracy, transparency, data security and accountability.

Specifically, Article 21 of the FADP governs automated individual decisions. The provision applies where a decision is based solely on automated processing and produces legal effects concerning the data subject or significantly affects the data subject. Where Article 21 applies, the controller must inform the data subject and, on request, provide an opportunity to state a point of view and to request review by a natural person, unless a statutory exception applies. The statutory trigger is narrow and should not be overstated. Not every automated process, recommendation, scoring mechanism or AI-supported workflow is an "automated individual decision" within the meaning of the FADP. The practical

limitations of Article 21 of the FADP have drawn criticism. However, the Swiss Parliament confirmed that Article 21 of the FADP shall only apply in the event that the decision is based exclusively on automated processing and will not be amended for the time being.

The Federal Data Protection and Information Commissioner (FDPIC) has repeatedly stressed that — of course — current Swiss data protection law already applies to AI. In its 2025 communication, the FDPIC also stated that providers and deployers of AI systems must make the purpose, functionality and data sources of AI-based processing transparent, and that users of directly communicating language models must know whether they are interacting with a machine and whether entered data is used to improve self-learning programmes. Those statements are regulatory guidance beyond the black-letter text of the FADP, not enacted AI-specific legislation.

3.2 General data protection regulation

Given that Switzerland is not a member of the EU, Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)) does not apply directly in Switzerland (see Section 3.1, above).

3.3 Open data and data sharing

The Federal Act on the Use of Electronic Means for the Fulfilment of Official Tasks (EM BAG), in force since 1 January 2024, strengthens the Swiss open-government-data framework at federal level. As a matter of principle, federal administrative units subject to EM BAG must publish data they obtain or generate in fulfilment of their statutory tasks where the statutory conditions are met, free of charge, promptly, in machine-readable form and in an open format. The principle is commonly described as “open by default”.

The EM BAG can increase the availability of certain public sector datasets and may therefore be relevant as one lawful source of training or testing data. However, EM BAG is not a general free-data charter as its scope is limited, and statutory exceptions remain important.

3.4 Biometric data: voice data and facial recognition data

Biometric data that uniquely identifies a natural person qualifies as sensitive personal data under the FADP. Its processing is therefore subject to heightened legal and organisational scrutiny. Switzerland does not currently have a dedicated horizontal AI statute that, like the EU AI Act, lists prohibited AI practices or expressly categorises biometric systems across all sectors. That does not mean biometric AI is legally unregulated. Depending on the context, the FADP, employment law, fundamental rights, cantonal police laws, employment law, administrative law legality requirements and sector-specific health or financial rules may all become relevant.

4. BIAS AND DISCRIMINATION

4.1 Domestic anti-discrimination and equality legislation treatment

Swiss anti-discrimination law remains comparatively fragmented. Article 8 of the Federal Constitution establishes equality and non-discrimination as a

constitutional guarantee, but private law implementation is selective rather than comprehensive. Statutory regimes include, in particular, the Gender Equality Act, the Disability Discrimination Act and sector-specific employment, tenancy and public law protections. Swiss criminal law also prohibits certain discriminatory conduct, for example, under Article 261 *bis* of the Swiss Criminal Code.

For AI, that means two things. First, discriminatory outcomes can still be legally relevant even in the absence of a dedicated AI discrimination statute. Second, Swiss law does not yet provide the kind of broad, harmonised anti-discrimination toolbox that some stakeholders would like to see for algorithmic systems. However, the Swiss Government has, to date, expressed no intentions of expanding anti-discrimination principles in view of the adaptation of the Council of Europe's Framework Convention on Artificial Intelligence.

5. CYBERSECURITY AND RESILIENCE

5.1 Domestic technology infrastructure requirements

Switzerland does not have a comprehensive cybersecurity law. Cybersecurity is instead governed through a combination of general information security law, sector-specific regulation, contractual controls and technical standards.

The Federal Act on Information Security (ISA), effective since January 2024, mandates that federal agencies, private institutions that fulfil public tasks, and, to a certain extent, critical infrastructure providers implement robust information security practices. An amendment to the ISA, which came into force in April 2025, introduced a mandatory obligation for critical infrastructure operators to report cyberattacks to the National Cybersecurity Centre (NCSC) within 24 hours of detection. Further, there are sector-specific statutes and regulations (in particular, in the finance and healthcare sectors) that contain cybersecurity related provisions. Like the ISA, such sector-specific regulations contain generic, largely technology-neutral obligations that do not address AI specifically.

6. TRADE, ANTITRUST 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"). AI can intensify familiar competition law concerns such as exclusionary access practices, self-preferencing, data-based entry barriers and lock-in around critical infrastructure, computer or proprietary datasets. 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. As in other jurisdictions, the analytical difficulty lies less in identifying the concern than in proving the infringement where the relevant mechanism is opaque, adaptive or decentralised.

6.2 Domestic (antitrust) regulation

Swiss competition law remains technology neutral. That is still true after the partial revision of the Cartel Act passed on 19 December 2025. The reform modernises merger control and amends other areas of competition law, but it does not introduce AI-specific rules on algorithmic collusion, AI-driven discrimination or AI gatekeeper power as such.

7. AGENTIC AI

7.1 Legal status and recognition of AI agents

Swiss law does not recognise AI systems or AI agents as legal persons. They cannot bear rights or obligations in their own name, contract on their own behalf or own assets. Any legal effects produced through AI-assisted conduct are attributed through ordinary rules to the relevant human or legal entity.

7.2 Sector-specific agentic AI regulations

There is currently no Swiss sector in which agentic AI enjoys independent legal capacity. Sector-specific rules may constrain or condition the use of autonomous systems, for example in finance, healthcare, aviation, road traffic or defence. But those rules regulate the conduct of companies, providers, deployers and public authorities. They do not confer legal personhood on the system.

8. PRODUCT LIABILITY AND AI

8.1 Application of existing product liability frameworks to AI

Swiss law does not yet have an AI-specific liability regime. Liability must therefore be analysed through existing frameworks: the Product Liability Act (PLA), product safety law, contract law, tort law and sector-specific rules.

The PLA applies to defective products and imposes strict liability on the producer for death, personal injury and certain property damage. The difficult question in AI matters is not whether Swiss law has a liability regime; it is whether the relevant AI constellation falls within product liability at all. For AI embedded in tangible products, the answer is comparatively straightforward. For standalone software, cloud-based AI and service-based models, the position is less clear and may instead need to be analysed under contract and general tort law.

8.2 Strict liability and AI systems

Strict liability under the PLA can apply where the statutory requirements are met and the relevant AI functionality forms part of a defective product. Outside that setting, liability will often shift to contract and fault-based tort analysis, unless a sector-specific strict regime applies.

8.3 Product recall and safety measures

Providers and deployers of AI systems embedded in physical devices are legally required to act promptly when defects or risks are discovered. This may include updates, patches, or issuing warnings and recalls. Under the PLA, liability arises, regardless of fault, if a defective AI system causes harm, making timely corrective measures critical.

Sector-specific regulations may impose additional obligations. The Ordinance on Medical Devices (MedDO) requires post-market surveillance, risk management, and field safety corrective actions for medical devices. In transportation, deployers and providers must ensure that autonomous vehicles or drones are updated, corrected, or temporarily withdrawn if safety is compromised. All corrective actions must be documented and communicated transparently to regulatory authorities and, where appropriate, to end users.

These measures collectively aim to ensure safety, compliance, and accountability, including with respect to AI-related risks.

8.4 Notable AI liability cases and trends

As of early 2026, there are no reported court cases specifically addressing AI product liability in Switzerland.

9. DOMESTIC LEGISLATIVE DEVELOPMENTS

9.1 Proposed and/or enacted AI legislation

The key policy development is the Federal Council's decision of 12 February 2025 to ratify the Council of Europe AI Convention and to prepare the legal amendments required for ratification (see Section 1, above).

Switzerland will not adopt the EU AI Act, whether directly, by dynamic incorporation or by autonomous wholesale transposition. This means that Switzerland is deliberately not following the EU's product-safety logic under the EU AI Act, under which providers of high-risk AI systems are subject to *ex ante* obligations before placing such systems on the market or putting them into service. Instead, Swiss law will continue, at least for the time being, to rely predominantly on *ex post* control: general private law, data protection law, sector-specific supervision and enforcement after risks have materialised or infringements have already occurred.

That choice has consequences. The EU model is designed to intervene upstream. It imposes compliance, documentation, risk-management, transparency and, in some cases, conformity-assessment obligations before particularly risky AI systems are deployed. The Swiss model is lighter for providers and more hospitable to innovation, but it is also less preventive. It offers fewer front-loaded legal safeguards against unsafe or rights-infringing AI and places a greater burden on affected individuals, courts and regulators to react once harm, discrimination, opacity or other adverse effects have already occurred.

In market terms, however, the EU AI Act remains highly relevant to Swiss companies. Providers established in Switzerland may fall within its scope where they place AI systems or General-Purpose AI (GPAI) models on the EU market, put them into service in the EU, or where the output is used in the EU. This is not a point of Swiss domestic law, but it is a major practical point for Swiss industry.

9.2 Proposed and/or implemented Government strategy

AI has been part of the Federal Council's digital policy agenda for several years, but the federal approach has recently become more concrete, coordinated

and implementation driven. AI is now a formal focus theme of the Digital Switzerland Strategy, covering both the regulation of AI in Switzerland and the deployment of AI systems within the Federal Administration.

The current strategy architecture includes, in particular, the Strategy Use of AI Systems in the Federal Administration, the related work on the further development of internal federal AI coordination, the legislative package to implement the Council of Europe Framework Convention on Artificial Intelligence, and a separate implementation plan for non-binding measures under that Convention. In addition, AI use is being advanced in specific administrative contexts, including office automation. The federal strategy on AI is therefore no longer limited to general principles.

10. FREQUENTLY ASKED QUESTIONS

May a Swiss public authority use cloud-based generative AI tools for internal work?

In principle, yes. In practice, however, only with considerable caution. For Swiss public authorities, the issue is not merely whether the use of such tools is technically useful or economically attractive. The decisive question is whether the intended use is compatible with the applicable legal framework, in particular the requirement for a sufficient legal basis in law as well as data protection, information security, procurement compliance and, where relevant, official secrecy or other statutory confidentiality obligations.

The legal risk often lies less in the output than in the input. If personal data, non-public administrative information, or information protected by official secrecy is entered into an external AI tool, the authority must assess carefully whether such disclosure is permissible at all, whether the provider acts purely on instructions, whether cross-border access takes place, and whether sufficient contractual, organisational and technical safeguards exist. Public bodies should therefore not permit broad or informal use of such tools without a comprehensive tailor-made contract, a defined governance framework, clear use-case limitations and strict rules on what information may never be entered into the system.

Can an employer in Switzerland use AI to screen candidates or rank job applicants?

Yes, in principle. Swiss law does not prohibit AI-assisted recruitment as such. However, employers may only process data relevant to the applicant's suitability for the role or necessary for the employment relationship (Article 328b of the Swiss Code of Obligations (CO)). They must also comply with the FADP, in particular, the principles of proportionality, purpose limitation and transparency. If AI effectively determines the outcome, Article 21 of the FADP on automated individual decisions may apply. Employers must also consider discrimination risks, in particular under Article 8 of the Federal Constitution and, in cases of gender discrimination, under the Gender Equality Act.

Does Article 21 of the FADP apply whenever AI is used in HR or customer-facing processes?

No. Article 21 of the FADP does not apply merely because AI is involved. Its scope is narrower. It applies only where there is a decision based solely on automated processing and that decision either produces legal effects concerning the individual or significantly affects that person.

That threshold is not met in every AI-supported workflow. Systems used for triage, prioritisation, drafting, anomaly detection or recommendations do not automatically trigger Article 21 if a human still exercises meaningful judgment. Conversely, if the human role is only formal and the system in substance determines the result, Article 21 may well become relevant. The legal analysis therefore depends less on whether a system is called “AI” and more on how the decision is actually made, what role the human retains, and what consequences the outcome has for the person concerned.

What are the main legal pitfalls when AI systems are used in a multijurisdictional outsourcing or business process outsourcing (BPO) context?

The main mistake is to treat AI as merely another tool. In a multijurisdictional outsourcing or BPO, AI can change the delivery model itself: how services are performed, where and by whom they are delivered, how decisions are made, and how risk, control and accountability are allocated across the service chain. The contract should therefore not merely permit AI in general terms. It should define the permitted use cases, conditions of use, required human oversight, approval rights and change-control triggers. It should also address data use, model training and improvement, confidentiality, security, audit rights, service levels, incident management, subcontracting, liability and business continuity.

A central risk lies in the allocation of the compliance burden. The contract should clearly state which party is responsible for identifying, monitoring and implementing the laws and regulatory requirements applicable to the AI-enabled services in each relevant jurisdiction. A generic duty to comply with “applicable law” is rarely enough. The better approach is to define the relevant legal categories, allocate monitoring and implementation duties, require notification of relevant legal or regulatory changes, and specify when such changes trigger remediation or formal change control.

Equally important is how compliance is evidenced. If the customer remains accountable to regulators, auditors or affected individuals, contractual assurances alone will not suffice. The customer will usually need transparency into the AI-enabled delivery model, including documentation of permitted use cases, subcontracting chains, controls, testing, override and escalation procedures, incident logs, and robust audit and information rights. In regulated or public sector environments, the supplier should not be allowed to hide behind black-box language, proprietary tool arguments or subcontractor opacity.

Clauses allowing the supplier to introduce AI unilaterally under broad formulations such as “continuous improvement” or “industry-standard tools” should therefore be treated with caution. If AI changes the legal, operational or control profile of the services, it should require prior customer approval and, where material, formal change control. In a multijurisdictional outsourcing, AI is not merely a tooling issue. It is a governance, compliance and control issue.

Is Switzerland more business-friendly than the EU for AI startups?

In broad terms, yes. Switzerland has chosen not to replicate the EU AI Act's horizontal product-safety model. Instead, it continues to rely primarily on technology-neutral legislation, sector-specific rules and *ex post* enforcement. For businesses, this generally means fewer *ex ante* compliance burdens and greater regulatory flexibility than under the EU regime.

However, this does not mean that AI startups may proceed informally. It means that they must identify and manage the relevant legal issues themselves across multiple areas of law, including data protection, employment law, contract law, procurement law, supervisory requirements and internal governance. The Swiss model is therefore not a model of non-regulation. It is a model of fragmented regulation, with more responsibility placed on organisations and their advisers to structure compliance properly from the outset.

AUTHOR BIOGRAPHY



Martina Arioli

Martina Arioli is the founder of Arioli Law and one of Switzerland's most established practitioners in technology law. With more than 25 years of international experience, she advises on IT, digital transformation, cloud and outsourcing projects, particularly where contractual complexity, regulatory sensitivity and operational reality intersect. Her work covers the full lifecycle of major sourcing and technology projects, from contract architecture and negotiation to implementation, transition, dispute resolution, termination and re-sourcing. Prior to establishing Arioli Law, Martina held senior legal positions at Zurich Insurance Company and UBS AG and practised at Walder Wyss Ltd and TIMES Attorneys. She studied law, philosophy and political science at the University of Bern, qualified for the Bar in Bern with distinction, and earned an LLM in Intellectual Property from the London School of Economics and Political Science. She regularly lectures at Swiss universities. Martina Arioli has been ranked by Chambers Europe for technology, media, and telecommunications since 2019 and has been recognised by Who's Who Legal among Switzerland's leading business lawyers since 2016. She has been named Thought Leader – Data in Switzerland since 2019 and received the Client Choice Award – Data – Switzerland in 2020.

FIRM PROFILE

Arioli Law

Arioli Law is a Zurich boutique advising on technology transactions, outsourcing, cloud, digital regulation, data protection and intellectual property. The firm focuses on high-value, complex mandates requiring close integration of regulatory and contractual analysis. Arioli Law was established in 2013 in Zurich as one of the first one-woman pure technology law firms in Switzerland and has since grown into a highly specialised boutique law firm. The renowned Swiss business magazine BILANZ has ranked Arioli Law among Switzerland's top law firms in technology, media, and telecommunications and intellectual property law since the first ranking issued in 2017.