UNDERSTANDING AI LAW SERIES

SWISS AI REGULATION: WHAT EVERY COMPANY MUST KNOW IN 2025

Date: **October 6th, 2025**

Authors: Me Florian Ducommun; Me Crystal Dubois

Expert topic: Artificial Intelligence; AI law; regulatory; advanced technologies; technology law

Artificial intelligence ("**AI**") has rapidly transformed from buzzword to business opportunities. Organizations across all sectors are investing heavily in AI to drive productivity gains, enhance innovation, and maintain competitive advantage, while individuals leverage AI tools to amplify their capabilities and streamline daily workflows.

The financial sector exemplifies this trend. A recent survey conducted by the Swiss Financial Supervisory Authority (FINMA)[1] found that 50% of the 400 licensed banks and other supervised financial institutions surveyed either use AI or have applications in development, with an average of five applications in use and nine in development.

At Bonnard Lawson, we've immersed ourselves in AI law over the past several years. We actively contribute to expert working groups and industry conferences, counsel clients on AI development and deployment matters, represent them in legal proceedings, and deliver specialized training to boards, legal, and product teams. We also use AI tools in our own work to stay ahead in this rapidly changing field.

Whilst we continue our work in the field and dive deeper into our experience, we are starting this series of articles called "Understanding AI Law", to share our knowledge and help guide our clients in their regulatory efforts.

This first article is aimed at **addressing the key regulatory points that apply to AI in Switzerland and that business leaders, product teams, legal teams and other players should consider when they are developing AI models, providing AI systems to others, or deploying such AI systems internally**.

This article covers the EU AI Act's extraterritorial reach, Switzerland's regulatory approach, FINMA's new AI guidance, data protection requirements, and provides a practical governance checklist for organizations.

Future articles in our Understanding AI Law series will explore intellectual property, liability, and other critical AI law topics in greater detail.

[1] FINMA survey communication from April 24, 2025, available at: https://www.finma.ch/en/news/2025/04/20250424-mm-umfrage-ki/.

1. How the EU AI Act affects Swiss companies: extraterritorial scope Explained

Whilst the purpose of this article is not to delve in detail about the provisions of the EU Artificial Intelligence Act (the **"EU AI Act**")[2], it is however necessary for Swiss stakeholders to consider that this regulation does apply to Swiss-based actors involved with AI in certain circumstances.

The EU AI Act entered into force on 1 August 2024 and becomes applicable in stages. It establishes a harmonized legal framework for the development, placing on the market, putting into service, and use of AI systems and general-purpose AI ("**GPAI**") models within the European Union ("**EU**"). This landmark legislation employs a risk-based approach, categorizing AI systems based on the potential harm they could cause to individuals and society.

For Swiss actors, a critical aspect of the EU AI Act is its **extraterritorial scope**. The legislation is designed to regulate the EU market, meaning its reach extends to entities located outside the EU if their AI products or services are used within the EU.

Specifically, the EU AI Act applies to **providers placing AI systems or GPAI models on the EU market or putting them into service in the EU, irrespective of whether those providers are established within or outside the EU**[3]. The term "placing on the market" refers to the first making available of an AI system or a GPAI model on the EU market. "Putting into service" denotes the supply of an AI system for its first use directly to the deployer or for own use within the EU.

Furthermore, the EU AI Act applies to **providers and deployers of AI systems who have their place of establishment or are located in a third country, where the output produced by the AI system is used within the EU**[4]. This means that even though Swiss actors might not offer directly their AI products or services to EU customers, they would still fall within the scope of the EU AI Act if the output produced by the AI system is intended to be used in the EU, taking into account that coincidental use of output is not sufficient. Such outputs could for instance be predictions, content, recommendations or decisions.

More information about the scope of application of the EU AI Act, especially the exemptions from the Act, the types of actors, and the requirements set by the regulation will be further developed in other articles.

However, **Swiss actors must be aware of the following**:

- Since February 1st, 2025, it is **strictly forbidden to provide AI systems that present a prohibited level of risks in the EU**.

- Furthermore, all organizations subject to the EU AI Act must **comply with the AI literacy obligation**, meaning that organizations need to ensure that their staff is equipped with skills, knowledge and understanding of AI in order to assess both the risks and opportunities of AI;

- Finally, since August 1st, 2025, **providers of GPAI models in the EU are subject to specific obligations** regarding **documentation and transparency requirements**, and for some providers of GPAI models which are deemed "high-risk", with **security requirements**.

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence.
[3] Article 2 (1) (a) EU AI Act.
[4] Article 2 (1) (c) EU AI Act.

2. SWITZERLAND'S REGULATORY STRATEGY FOR AI

In Switzerland, the Federal Council recently clarified the approach taken towards AI regulation. Three main objectives were identified for AI regulation in Switzerland, namely **(a) strengthening the country as an innovation hub, (b) safeguarding fundamental rights (including economic freedom), and (c) increasing public trust in AI**.

First of all, it was decided to opt for a **topic and sector-specific approach** rather than enacting a comprehensive horizontal AI law like in the EU. This approach is explained by the fact that the Swiss legal regime is technology-neutral and principle-based, and thus, that the regulation of AI shall fall within the scope of those rules, varying based on how the technology is used, instead of being regulated by a one-fit-all regulation. Nevertheless, this does not mean that Swiss laws are not expected to be adjusted to AI. Indeed, AI raises new questions and legal challenges that require adjustments to the topic.

Second, on March 27, 2025, the Swiss Federal Council signed the **Council of Europe's AI Convention**[5], referred as the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law[6] (the "**AI Convention**"). At the date of writing of this article, this AI Convention has a global focus and has been ratified by 15 signatories, including the United States. It is aimed at ensuring that the use of AI complies with existing international legal standards on human rights, democracy and the rule of law.

The AI Convention defines **a set of principles** that states must follow when dealing with AI. The provisions are directly applicable to public authorities that deal with AI-related activities, whilst for private actors, it mostly depends on how states decide to address the risks and impacts of AI-related activities into their existing laws. Indeed, contracting parties to the Convention have wide latitude in choosing appropriate legislative, administrative or other measures to implement the provisions.

Swiss law appears to offer a sufficient level of protection for some provisions of the AI Convention, such as with respect to integrity of democratic processes and respect for the rule of law[7], and the requirement for public consultation on important questions in relation to AI[8]. However, it is considered that **adjustments to Swiss law** would be necessary regarding the transparency and oversight[9] principles, safe innovation[10], remedies[11], and procedural safeguards[12].

Furthermore, **new legal bases** would have to be created to set standards for the risk and impact management framework for AI systems[13] and for effective oversight mechanisms to oversee compliance with the obligations of the AI Convention[14].

However, following legal scholars' opinion[15] and industry lobbying[16], the Federal Council decided that, **when possible, non-legal measures should be sought, that legal measures should be focused on sector-specific, and that only fundamental rights, such as data protection, shall be subject to cross-sectoral regulation**

The Federal Department of Justice and Police (FDJP), in collaboration with the Federal Department of the Environment, Transport, Energy and Communications (DETEC) and the Federal Department of Foreign Affairs (FDFA), have been tasked with **drawing up a bill, that includes the legal and non-**

---

[5] https://www.news.admin.ch/en/nsb?id=104110.
[6] https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.
[7] Article 5 AI Convention.
[8] Article 19 AI Convention.
[9] Article 8 AI Convention.
[10] Article 13 AI Convention.
[11] Article 14 AI Convention.
[12] Article 15 AI Convention.
[13] Article 16 AI Convention.
[14] Article 26 AI Convention.
[15] As recommended in a set of articles published by university professors and supported by the Foundation Mercator: https://www.itsl.uzh.ch/de/Forschung-und-Beratung/Forschungsprojekte/nachvollziehbare-algorithmen.html.
[16] https://www.economiesuisse.ch/fr/articles/comment-la-suisse-peut-devenir-un-site-cle-pour-lia

legal measures, to be submitted for consultation by the end of 2026. It is not yet clear as to how the administration intends to implement the AI Convention.

On the one hand, a minimum implementation would still require adjustments to the current legal framework and introduction of new provisions, with regards to the **transparency and risk and impact assessment provisions.** It could for instance be required that AI systems used by the state be registered in a public register and that public actors and a limited group of private actors be required to conduct a risk and impact assessment prior to using an AI system. Furthermore, no new authority would be created to supervise compliance with the AI Convention and existing supervisory authorities will take on this duty in their respective sectors on top of their existing supervisory activities.

On the other hand, **more ambitious measures could be taken**, such as providing for similar obligations to public and private actors and creating new rights and obligations in the area of non-discrimination, especially for private actors, to whom the current provisions of the Convention are not directly applicable. This will likely take the form of **non-binding measures**. Furthermore, the group of private actors subject to the risk and impact assessment of AI provisions could be defined more broadly, a higher level of details could be required, and such assessments could have to be reviewed by a public authority, enhancing the level of safety. Existing supervisory authorities could be given more extensive powers and a new coordination office could be created to ensure a coherent approach to cross-sectoral issues.

Otherwise, the AI Convention **could be implemented in line with the EU AI Act**, in the way of a comprehensive product regulation of AI systems based on the EU AI Act. This means that on top of adjusting the current Swiss legal regime to the AI Convention, a new product-focused regulation applicable to both public and private actors could be enacted, in line with the various risk levels and requirements laid down in the EU AI Act. This could benefit Swiss-based product manufacturers that integrate AI components in their products and could therefore gain access to the EU internal market with fewer hurdles.

Nevertheless, this regulatory approach would lead to a high density of AI regulation in Switzerland, which is not wanted by the industry. Nevertheless, based on the extra-territorial scope of application of the EU AI Act described earlier, Swiss companies may already be subject to its requirements, therefore, lawmakers should take this into consideration when adapting the Swiss legal regime to AI, in order to ease the burden on Swiss companies.

Finally, looking at **industrial products being exported to the EU,** the Federal Council makes us aware that 12 of the 20 product sectors listed in the existing MRA CH-EU[17], the agreement that regulates the trade of industrial goods between the EU and Switzerland, are affected by the AU AI Act if the products in question contain AI systems[18]. In fact, in such cases, products under these 12 product categories, including medical devices and machinery, would classify as high-risk AI systems under the EU AI Act if they are subject to the conformity assessment procedure by a conformity assessment body acting as a third party in accordance with existing EU harmonization legislation.

Currently, the technical regulations of Switzerland and the EU are recognized as equivalent. However, **this will no longer be the case from August 2027**, when the requirements of the EU AI Act for high-risk systems will be added, which will be applied to products in those 12 sectors. From then on, such products would be required to go through an additional conformity assessment conducted by a conformity assessment body in the EU, and Swiss-based companies will need to comply with additional requirements, leading to additional work and costs.

Considering the above, **an extension of the MRA to the AI sector would help reduce the effort and costs involved in the commercialization of AI systems from Swiss companies to the EU**. In consequence, Swiss law would have to provide for equivalent obligations to the EU AI Act in key aspects. There are some big uncertainties about how the administration will deal with this challenging situation,

[17] https://www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/Technische_Handelshemmnisse/Mutual_Recognition_Agreement_MRA0/MRA_Schweiz_EU.html.

[18] Report, section 7.2, p. 14 ; Report, section 9, p. 17.

and in particular if an extension of the MRA to the AI sector could be planned within the updated version of the MRA CH-EU which is meant to enter into force by 2028 at the earliest[19].

Switzerland's approach to AI regulation reflects its pragmatic national character: **promoting innovation while protecting fundamental rights**. By implementing measured oversight rather than burdensome restrictions, Swiss authorities aim to strengthen the country's position as an innovation hub while building public confidence in AI technologies.

However, it is important to note **that Swiss actors are not operating in a regulatory vacuum**. Indeed, they remain subject to numerous existing legal frameworks, including the Federal Data Protection Act (FDAP), the Copyright Act (CopA), and broader Swiss civil and criminal law provisions regarding liability, as well as industry-specific regulations.

We will continue monitoring how Switzerland's balanced regulatory framework will evolve in the coming months.

3. FINMA'S GUIDANCE 08/2024 ON ARTIFICIAL INTELLIGENCE

In December 2024, FINMA published guidance on AI use in financial institutions[20] (the "**AI Guidance**"). This AI Guidance represents the first sector-specific non-legal measure, regulating the use of AI by supervised financial institutions. It builds on its existing guidelines and supervision over risk management within financial institutions, addressing specific requirements for the usage of AI.

FINMA's AI Guidance makes no distinction between various AI technologies or implementation methods. Rather, it covers the **entirety of AI utilization** within these institutions encompassing proprietary AI applications developed internally, custom in-house AI systems or applications developed by third-parties, and third-party AI systems accessed through APIs, subscription services, or even free platforms. This broad scope ensures consistent oversight regardless of how financial institutions integrate AI into their operations.

The AI Guidance establishes a structured set of measures financial institutions must implement to mitigate risks associated with artificial intelligence deployment. Through its supervisory activities, FINMA has identified **several key risk categories**:

- operational vulnerabilities stemming from AI systems' lack of robustness, accuracy, explainability, or inherent biases;
- heightened IT and cybersecurity exposures; and
- data protection concerns.

Additionally, FINMA recognizes the emerging challenges of increased **third-party dependencies** and the potential **legal and reputational consequences** that may arise from AI implementation.

In order to address those risks, the AI Guidance recommends the following:

1) **AI governance**: development of **a strong AI governance framework** that must **clearly define roles and responsibilities for the development, implementation, monitoring and use of AI, covering both internally developed and outsourced solutions**. Based on the recent survey conducted by FINMA[21], only half of the survey respondents that indicated using AI have developed a strategy relating to AI. This means that there is significant potential for improvement

[19] https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2023/europa.html; Report, section 7.2, p. 14 ; Report, section 9, p. 17.
[20] https://www.finma.ch/en/news/2024/12/20241218-mm-finma-am-08-24/.
[21] https://www.finma.ch/en/news/2025/04/20250424-mm-umfrage-ki/.

and that financial actors need to bridge the gap if they don't want to face FINMA's enforcement measures.

2) **Inventory and risk classification**: institutions must keep a centrally managed inventory of all AI applications, with risk classifications and mitigation measures documented.

3) **Data quality requirements**: the AI Guidance mandates that supervised institutions establish explicit requirements within their internal governance framework to ensure **data integrity**. These requirements must address data completeness, accuracy, and consistency while safeguarding appropriate access controls and availability protocols. This emphasis on data quality reflects FINMA's recognition that compromised data inputs inevitably lead to unreliable or biased AI outputs. Such requirements are particularly critical for AI systems that directly leverage institutional data, including analytical applications, retrieval-augmented generation (RAG) systems, and internal conversational agents or AI tools that operate on the organization's proprietary knowledge base.

4) **Tests and ongoing monitoring**: FINMA requires financial institutions to implement scheduled testing protocols and ongoing monitoring for AI applications. This includes for example, statistical validation, adversarial testing, bias audits, performance monitoring, and data quality verification to ensure systems operate reliably while allowing for prompt risk identification. Financial institutions may also request an independent review of the model development process by qualifies personnel in order to identify and reduce model risks.

5) **Documentation**: FINMA requires financial institutions to maintain **comprehensive documentation that upholds the principle of transparency**. Supervised entities must **document the application's purpose, data selection and preparation processes, model selection criteria, performance metrics, underlying assumptions, operational limitations, testing protocols, control mechanisms, and fallback solutions**. During assessments, FINMA will evaluate whether institutions have adequately documented data sources and quality verification procedures, how they ensure application robustness, reliability and traceability, and whether appropriate risk categorization has been implemented.

6) **Explainability**: the AI Guidance mandates that financial institutions maintain the capacity **to explain AI-generated decisions to all relevant stakeholders, including investors, clients, employees, FINMA, and external auditors**. Supervised entities must therefore ensure sufficient transparency in their AI systems to articulate the rationale and process behind any automated decision-making. This requirement establishes accountability by ensuring financial institutions can clearly explain how their AI applications arrive at specific outcomes or recommendations.

4. Swiss Data Protection Requirements

The Swiss Federal Data Protection and Information Commissioner (FDPIC) has confirmed that the Federal Data Protection Act (FDPA), in force since September 1, 2023, applies directly to AI systems processing personal data[22]. Organizations deploying AI must therefore ensure compliance with Swiss data protection principles alongside any AI-specific regulations.

All **principles set forth in FDPA apply to AI processing: data minimization, purpose limitation, accuracy, storage limitation, and security**. Organizations must provide comprehensive information regarding personal data collection, including processing purposes, retention periods, and data recipients. For instance, companies deploying AI systems must clearly inform users that their data is processed for specific purposes (such as service improvement or personalization), specify how long data will be retained, and identify any third-party AI service providers involved.

[22] https://www.edoeb.admin.ch/en/09112023-current-data-protection-legislation-is-directly-applicable-to-ai; https://www.edoeb.admin.ch/en/update-current-legislation-directly-applicable-ai.

The FDPA establishes specific obligations for **automated decision-making**[23]. When AI systems produce decisions that significantly affect individuals, organizations must:

- provide notice of automated decision-making processes;
- enable human intervention for decision review;
- allow data subjects to express their position and contest decisions.

Express consent is mandatory for high-risk profiling conducted by private entities and all profiling by federal bodies. Examples include AI systems for credit scoring, automated recruitment screening, insurance premium calculations, or behavioral analysis for targeted advertising that creates detailed personality profiles.

FDPA mandates **Data Protection Impact Assessments (DPIA) for AI processing likely to result in high risks to individual rights and fundamental freedoms**[24]. This applies particularly to high-risk profiling and large-scale processing of sensitive data. Organizations must consult the FDPIC when significant residual risks persist following mitigation measures. DPIAs are typically required for AI applications such as large-scale employee monitoring systems, predictive policing algorithms, or AI-powered medical diagnosis tools processing health data.

International AI data transfers require adequate protection levels or appropriate safeguards such as standard contractual clauses and transfer impact assessments.

The FDPA requires data controllers and processors to adopt **appropriate technical and organizational measures to ensure adequate security of personal data**[25]. For AI systems, this includes:

- encryption of personal data during processing and storage;
- access controls and authentication mechanisms ;
- regular security assessments of AI models and infrastructure;
- secure data transmission protocols ; and
- protection against unauthorized access, alteration, or destruction.

Finally, beyond personal data protection, AI systems often process **confidential business information** requiring additional safeguards:

- **Trade secrets protection**: implement contractual confidentiality clauses with AI service providers and technical measures to prevent unauthorized disclosure.
- **Professional secrecy**: ensure compliance with sector-specific confidentiality obligations (legal, medical, financial).
- **Business confidential information**: establish data classification schemes and access controls for proprietary information.
- **Contractual safeguards**: include specific confidentiality and data protection provisions in AI service agreements.
- **Technical isolation**: segregate confidential data processing from other AI operations where feasible.

5. Conclusion and Checklist

Switzerland's AI regulatory landscape requires **immediate attention** from **business leaders and legal teams**. While comprehensive AI legislation is still in development, existing data protection laws, FINMA guidance, and the EU AI Act's extraterritorial reach create immediate compliance obligations for Swiss organizations.

[23] Article 21 FDPA.
[24] Article 22 FDPA.
[25] Article 8 FDPA.

The key to successful AI governance lies in **understanding your specific regulatory obligations based on your role in the AI ecosystem and implementing robust frameworks that can adapt to evolving requirements**. Organizations that proactively address these obligations will not only ensure compliance but also build **competitive advantages** in an AI-driven economy.

The time for action is now. Assess your AI applications, implement necessary safeguards, and establish governance structures that protect both your organization and the individuals whose data you process.

Use this checklist to assess your organization's AI compliance obligations and identify necessary actions:

EU AI Act applicability

- ✓ Do you place AI systems or GPAI models on the EU market?
- ✓ Do you put AI systems into service in the EU?
- ✓ Are outputs from your AI systems intended for use within the EU?
- ✓ Have you identified if your AI systems qualify as prohibited, high-risk, or limited-risk under the EU AI Act?

Your role in AI development and deployment

- ✓ Are you a provider (developing/manufacturing AI systems)?
- ✓ Are you a deployer (using AI systems in your operations)?
- ✓ Are you using third-party AI services (APIs, cloud-based AI)?
- ✓ Do you operate in the financial sector subject to FINMA supervision?
- ✓ Have you classified all AI applications by risk level and use case?

Swiss legal obligations

- ✓ Have you conducted DPIAs for high-risk processing of personal data in your AI systems?
- ✓ Do you provide adequate information about automated decision-making to affected individuals?
- ✓ Have you implemented human intervention rights for AI decisions?
- ✓ Are appropriate security measures in place for personal and confidential data?
- ✓ Have you established safeguards for cross-border AI data transfers?
- ✓ Do you comply with sector-specific regulations (FINMA guidance for financial institutions)?

Internal AI governance

- ✓ Have you established an AI governance framework with clear roles and responsibilities?
- ✓ Do you maintain a centralized inventory of all AI applications with risk classifications?
- ✓ Are data quality requirements defined and implemented for AI systems?
- ✓ Have you implemented testing protocols and ongoing monitoring for AI applications?
- ✓ Is comprehensive documentation maintained for all AI systems?
- ✓ Do you have explainability processes for AI-generated decisions?

External documentation and compliance

- ✓ Have you updated privacy policies to cover AI processing activities?
- ✓ Are appropriate contracts in place with AI service providers including confidentiality clauses?
- ✓ Do you have standard contractual clauses for international AI data transfers?
- ✓ Have you prepared breach notification procedures for AI-related incidents?
- ✓ Is technical documentation ready for regulatory inspections?
- ✓ Have you established procedures for responding to individual rights requests regarding AI processing?

Stay informed on the latest developments in AI law by following our Understanding AI Law series and subscribing to our newsletter.

Our firm is committed to providing tailored legal solutions for your organization, including customized advisory services, specialized training, regulatory assessments, and comprehensive support for contract drafting and documentation review.

To discuss your specific legal needs, please contact us directly by email or phon

***

Your contacts

Florian Ducommun
Partner
Profile

fd@bonnard-lawson.com
+41 (0)21 348 11 88

Crystal Dubois
Senior Associate
Profile

cd@bonnard-lawson.com
+41 (0)21 348 11 88