N

Monthly Newsletter Oct 2024

Banking & Finance

Schellenberg Wittmer

AI Regulation in the Financial Sector

Grégoire Tribolet

Key Take-aways

1.
Switzerland has not yet introduced an AI-specific regulatory framework. Financial institutions utilizing AI must comply with the general legal framework and FINMA's supervisory expectations.

2.
The EU AI Act introduces new regulations on AI systems, affecting not only EU entities, but also Swiss companies that supply AI systems to the EU or deploy systems whose output is used within the EU.

3.
Financial institutions and insurance companies must adopt AI governance frameworks and stay informed about regulatory developments to ensure compliance.

1 Introduction

Artificial intelligence **(AI)** has become a **key driver of innovation in the financial industry,** where it is employed in a wide range of use cases, including fraud detection, risk management, cash flow forecasting, process automation, credit risk analysis, customer relationship management, trading algorithms, IT development and information analysis. While recent developments in generative AI offer considerable opportunities, they also present risks. As a result, financial regulators worldwide are intensifying their supervision of AI applications used by financial institutions.

This newsletter provides a high-level overview of the current state of the Swiss regulatory framework applicable to financial institutions using AI applications, as well as the EU AI Act, which may affect financial institutions that supply AI systems to EU-based entities or deploy AI systems whose output is used in the EU.

2 Swiss Legislative Framework

Switzerland has not yet adopted a comprehensive AI-specific regulatory framework. In 2020, the Federal Council has adopted the Guidelines on Artificial Intelligence for the Confederation which apply only to the Federal Administration. Regarding the private sector, a Report by the State Secretariat for Education, Research and Innovation **(SERI)** to the Federal Council, published in 2019, concluded that there was no immediate need to introduce Swiss legislation dealing with AI.

Swiss financial institutions must comply with FINMA's supervisory expectations.

However, in 2023, recognizing the growing global momentum toward AI regulation, the Federal Council tasked the Department of the Environment, Transport, Energy, and Communication (DETEC) with drafting a report on possible regulatory approaches by the end of 2024. This report will serve as the foundation for a **potential Swiss AI regulatory framework proposal in 2025.**

In the interim, Swiss businesses must comply with the **general legal framework** when developing or deploying AI applications, such as the Data Protection Act **(FADP)** (see 2.1 below) and personality rights under Swiss law, relevant intellectual property laws and notably the Copyright Act **(CopA)**, as well as the Unfair Competition Act (UCA), in line with Switzerland's principle-based and technology-neutral approach.

Additionally, Swiss financial institutions utilizing AI must fulfil the **supervisory expectations of FINMA** (see 2.2 below) and comply with other relevant regulations, such as the Swiss bank secrecy provisions of the Banking Act, FINMA Circular 2018/3 (Outsourcing), and FINMA Circular 2023/1 (Operational Risks and Resilience).

2.1. Data Protection Act

In November 2023, the Federal Data Protection and Information Commissioner **(FDPIC)** issued a statement emphasizing that **Swiss data protection legislation is directly applicable to AI-driven data processing.** The statement reminded manufacturers, providers and deployers of AI applications that they must ensure transparency regarding the purpose, functionality and data sources of AI-driven data processing activities and must safeguard the highest possible degree of digital self-determination for data subjects.

The requirements of Swiss data protection legislation apply to most AI applications used by financial institutions. Financial institutions must in particular assess whether the AI application generates **automated individual decisions** within the meaning of Article 21 FADP. This assessment is particularly relevant for AI applications used in credit scoring, digital onboarding, customer segmentation or filtering job applications.

The FDPIC also pointed out that certain AI applications require a **data protection impact assessment** pursuant to Article 22 FADP. This applies particularly in cases where (i) large volumes of sensitive personal data are processed, (ii) personal data is systematically collected for AI processing (other than for statistical or non-personal purposes) or (iii) AI application's output has significant consequences for the concerned data subjects.

2.2. FINMA's Supervisory Expectations

FINMA has been monitoring the development and use of AI for several years. In the years 2021 and 2022, it conducted surveys on the use of AI in the insurance, banking and asset management sectors, established an inventory of areas in which AI applications were used and set up a specialized AI service. In its Risk Monitor 2023, FINMA outlined its **supervisory expectations for financial institutions using AI,** focusing on **four critical areas:**

- **Governance and Responsibility:** Financial institutions must clearly define roles and responsibilities for AI-related decisions, ensuring that accountability remains with human actors, not the AI systems themselves. This is particularly important when AI errors may go unnoticed, where processes become overly complex, or where there is a lack of expertise within the institution.
- **Robustness and Reliability:** AI systems must be tested for accuracy and reliability, especially considering the risks of „drift" in self-learning models. These systems should undergo rigorous testing, particularly in risk management areas. AI systems also pose cybersecurity risks, which must be addressed.
- **Transparency and Explainability:** Institutions must ensure that AI systems, especially those affecting customer outcomes, are transparent and that decisions made by these systems can be understood and explained by human operators.
- **Equal Treatment:** AI systems used in financial services, such as credit scoring, must avoid biases or discriminatory practices. FINMA requires institutions to monitor their AI systems to prevent any form of unequal treatment.

By publishing these expectations, FINMA is positioning itself at the forefront of a trend among financial market regulators, who are increasingly issuing guidance regarding the use of AI through whitepapers, guidelines or statements. Recent examples include the Statement of the European Securities and Markets Authority **(ESMA)** offering initial guidance to firms using AI when providing investment services to retail clients (May 2024), the expert article by the German Federal Financial Supervisory Authority **(BaFIN)**

on the risk of discrimination in AI use (August 2024), and the AI Update from the UK Financial Conduct Authority (April 2024).

3 EU AI Act

The EU AI Act came into force on 1 August 2024, and represents the **most comprehensive AI-specific regulation so far.** The Act takes a risk-based approach, categorizing AI systems based on their potential impact on safety and fundamental rights.

3.1 Timeline

The EU AI Act's provisions are phased in over several years. Key implementation deadlines include:

2 February 2025	Prohibition of AI practices with unacceptable risks and AI literacy requirements
2 August 2025	General-purpose AI (GPAI) models and provisions on Member State penalties
2 August 2026	The majority of the Act's rules, including those concerning high-risk AI systems and transparency provisions, will take effect.
2 August 2027	High-risk AI under specific sector legislation; GPAI models already on the market

These transition periods allow businesses time to comply with the Act's various provisions, although early planning is crucial, especially for entities dealing with high-risk AI systems.

3.2 Territorial scope

The **territorial scope of the EU AI Act is exceptionally broad,** applying to:

- Providers of AI systems that are put into service or placed on the market in the EU;
- Deployers of AI systems established in the EU; and
- Providers or deployers of AI systems where the system's output is used in the EU.

The EU AI Act impacts both EU and non-EU AI providers and deployers.

Swiss financial institutions developing or deploying AI systems may therefore be **subject to the EU AI Act,** even if they have no physical presence in the EU, particularly if they (i) develop AI systems and supply them to EU-based entities or (ii) deploy AI systems whose output is used in the EU (e.g., by clients residing in the EU).

While the GDPR applies to entities outside the EU when their activities are at least partly aimed at the EU, it is **unclear** whether the EU AI Act applies in cases where the provider or deployer established outside of the EU has made **no attempt to target the EU market.** Recital 22 indicates that a provider or deployer outside the EU is subject to the Act if the AI system's output is intended for use in the EU. However, Article 2(1)(c) of the AI Act does not include the element of intent and indicates instead that a provider or deployer is subject to the Act if the output of its AI systems is used in the EU.

It is also uncertain how the **term "output"** will be interpreted, but the Act provides the example of "predictions, content, recommendations, or decisions." For instance, investment recommendations generated by an AI system and addressed by a Swiss financial institution to clients in the EU may trigger the applicability of the EU AI Act.

Additionally, if the provider of a high-risk AI system is based in a third country, it must appoint an **authorized representative** in the EU.

High-risk AI systems face stringent requirements under the EU AI Act.

3.3 Risk-Based Categorization of AI Systems

The EU AI Act categorizes AI systems into four key risk levels:

- **Prohibited AI Systems:** These include AI systems that present unacceptable risks, such as manipulating individuals through subliminal techniques, exploiting vulnerabilities (e.g., age or disability), or creating social scoring systems that discriminate based on personal behavior. Such AI systems are forbidden under the EU AI Act subject to very limited exceptions.
- **High-Risk AI Systems:** These AI systems are subject to stringent regulations. For financial institutions, the following high-risk AI systems may be particularly relevant:
  - AI systems used to evaluate the creditworthiness of natural persons or establish their credit scores (except for detecting financial fraud);
  - AI systems used for risk assessment and pricing in life and health insurance;
  - AI systems used for recruitment or selection of individuals, including placing targeted job advertisements, analyzing and filtering job applications, and evaluating candidates.
- **Limited-Risk AI Systems:** These systems are subject to transparency requirements. For example, AI systems interacting directly with consumers (e.g. chatbots) must inform users that they are interacting with AI. Similarly, AI-generated content (e.g. synthetic media or deep fakes) must be labeled as such to prevent deception.
- **Minimal-Risk AI Systems:** These systems face no mandatory regulatory requirements, but businesses are encouraged to adopt codes of conduct to promote ethical AI use.

3.4 Specific Requirements for High-Risk AI Systems

Providers and deployers of high-risk AI systems must comply with extensive requirements, including:

- **Risk Management:** Comprehensive risk management systems shall be implemented to address potential risks throughout the AI system's lifecycle. These systems must identify foreseeable risks to health, safety, and fundamental rights and ensure that appropriate mitigation measures are in place.
- **Data Governance:** The EU AI Act requires that training, validation, and testing datasets for high-risk AI systems be representative, relevant, and free of errors. Specific attention must be paid to preventing bias in datasets, particularly in systems affecting fundamental rights, such as those used for recruitment or credit assessments.

- **Transparency and Human Oversight:** High-risk AI systems must be designed to allow for effective human oversight, with mechanisms in place to halt operations if necessary. Human operators must be able to interpret the system's output, understand its limitations, and override AI decisions when needed.
- **Conformity Assessments:** Before placing a high-risk AI system on the market, providers must conduct a conformity assessment to ensure the system meets regulatory standards. Depending on the system, third-party assessments may be required.

The EU AI Act seeks to address potential overlap between some of its requirements and those imposed on financial services entities by existing EU financial services law. As a result, financial services entities providing or deploying high-risk AI systems benefit from limited derogations in specific areas.

3.5 Compliance and Enforcement Mechanisms

The EU AI Act establishes a **multi-tiered supervision and enforcement structure.** At the EU level, the European Artificial Intelligence Board will oversee the Act's implementation, while each Member State must designate national authorities to enforce the Act within its jurisdiction. These authorities will have the power to conduct market surveillance, investigate non-compliance, and impose sanctions. For the financial sector, the competent authorities for supervising financial institutions under the financial market laws are expected to also supervise compliance with the EU AI Act.

Non-compliance with the EU AI Act can result in **significant penalties.** Companies engaging in prohibited AI practices may face fines of up to EUR 35 million or 7% of total annual global turnover, whichever is higher. For violations related to high-risk and certain other AI systems, fines can reach EUR 15 million or 3% of annual global turnover.

4 Conclusion

While Switzerland has not yet introduced a comprehensive AI-specific regulatory framework, financial institutions are required to navigate the existing general legal landscape, particularly in areas such as personality rights and data protection, and comply with FINMA's supervisory expectations. These obligations are principle based and concern primarily transparency and accountability in the use of AI. They are also relevant for other sectors, such as insurance companies. In contrast, the EU AI Act sets forth a more detailed, granular and far-reaching regulatory framework, applying not only to EU-based entities but also to third-country providers or deployers of AI systems whose outputs are used in the EU – potentially impacting also Swiss financial institutions and insurance companies. To stay compliant, to the extent they are utilizing AI, they should already start adopting an AI governance framework and stay informed about future regulatory developments.

Grégoire Tribolet
Partner
gregoire.tribolet@swlegal.ch

Stéphanie Chuffart-Finsterwald
Partner
stephanie.chuffart@swlegal.ch

Roland Mathys
Partner
roland.mathys@swlegal.ch

Olivier Favre
Partner
olivier.favre@swlegal.ch

Schellenberg Wittmer Ltd
Attorneys at Law

Zurich
Löwenstrasse 19
P.O. Box 2201
8021 Zurich / Switzerland
T +41 44 215 5252
www.swlegal.com

Geneva
15bis, rue des Alpes
P.O. Box 2088
1211 Geneva 1 / Switzerland
T +41 22 707 8000
www.swlegal.com

Singapore
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapore 049909
T +65 6580 2240
www.swlegal.sg