FINMA guidance on governance and risk management when using AI

17.01.2025

Key takeaways

- **To date, there is no specific legislation on artificial intelligence (AI) in Switzerland.**
- **The Swiss government included AI as a cornerstone of the Digital Switzerland Strategy and has already commissioned two expert reports on how to regulate AI in Swiss law, the second of which is expected for publication in early 2025. The Federal Data Protection and Information Commissioner also made it clear in 2023 that the Federal Data Protection Act directly applies to data processing with the use of AI.**
- **Most recently, the Swiss Financial Market Supervisory Authority (FINMA) published guidance on governance and risk management for supervised financial institutions when using AI in December 2024. Businesses from other sectors are also invited to take note of the general directions as FINMA adopts certain regulatory ideas originating in EU law.**

Introduction

On 18 December 2024, the Swiss Financial Market Supervisory Authority (FINMA) published Guidance Note 08/2024 on governance and risk management when using artificial intelligence (AI). FINMA regularly publishes guidance notes to inform market participants of its observations from ongoing supervision activities. This latest guidance note draws attention to the risks associated with the use of AI in the financial services industry.

In its press release, FINMA expresses concerns that the rapid adoption of AI in finance leads to specific risks that may often be difficult to assess. Such risks include a broad array of operational risks, in particular model risks, data-related risks, IT and cyber risks, increasing

third-party dependencies as well as legal and reputational risks.

FINMA found that most financial institutions are still in the early stages of developing AI use cases and establishing the corresponding governance and risk management structures. FINMA highlighted the need for the supervised institutions to appropriately identify, assess, manage and monitor the risks resulting from their AI use cases.

AI regulations in Switzerland

General

To the present day, Swiss laws and regulations do not include any provisions that deal specifically with artificial intelligence (see our Legal Update "Navigating AI with Pestalozzi – Part 2: Regulation"). In view of the recent technical developments, the Federal Council has instructed the Federal Department of the Environment, Transport, Energy and Communications (DETEC) to identify potential approaches to regulating AI by the end of 2024, and to involve all federal agencies responsible in the legal areas affected. The analysis is intended to reflect existing Swiss law and identify possible regulatory approaches for Switzerland that are compatible with the EU AI Act as well as the Council of Europe's AI Convention, to which Switzerland actively contributed. This report is expected to be released in early 2025.

FINMA's AI guidance is closely related to this legislative backdrop. It is also closely related to FINMA Circular 2023/1 on operational risks and resilience which covers many ICT-related risks. Both the new AI guidance and the circular on operational risks are based on FINMA's authority to issue interpretative guidance (Article 7 para. 1 let. b of the Financial Markets Supervisory Act (FINMASA)) and the provisions on proper organisation contained in the various acts, including the Banking Act and the Financial Institutions Act. Finally, supervised entities are required to submit relevant information to FINMA based on their general reporting duty (Art. 29 para. 1 FINMASA).

Empirical evidence from FINMA supervisory activities

FINMA had taken a first look at the use of AI in the Swiss financial market in its Risk Monitor for the year 2023. In that publication, FINMA described the risks arising from the use of AI systems as mainly coming from the area of operational risks. FINMA identified the following issues:

- Robustness, correctness and bias of output by AI applications
- Lack of output explainability
- Data protection issues
- Operational risks including IT and cyber risks and model risks

It seems a pertinent observation that such risks are further heightened by a growing dependence on third parties such as providers of hardware solutions, models or cloud services

in an increasingly concentrated market (see our Legal Update on recent trends in outsourcing). FINMA also mentioned legal and reputational risks that might arise from an inappropriate allocation of responsibilities due to the autonomous actions of AI systems that can be difficult to explain. Indeed, the AI-specific issues of opacity and the associated lack of explainability have often been mentioned in government reports and expert reports. Clear roles and responsibilities as well as risk management processes need to be defined and implemented. FINMA makes it clear that the responsibility for decisions cannot be delegated to AI or third parties (see decision 4A_305/2021 of 2 November 2021 by the Swiss Federal Supreme Court). All employees involved must have sufficient expertise in AI to perform their tasks.

FINMA proposes several measures to be taken by supervised entities. The first measure for establishing a suitable governance structure is creating an inventory of AI systems used in the organisation. Creating and maintaining a detailed inventory including all relevant tools, data flows and data sources is a well-known approach used in other areas such as data protection. A robust governance framework should clearly define responsibilities and accountabilities for the development, implementation, monitoring and use of AI tools. Financial institutions should avoid decentralised approaches where risks are not properly identified, and teams do not interact or communicate with each other to share best practices. As is the case for outsourcing in general, financial institutions should instead follow an integrated, comprehensive approach covering all the links of their value chains. Sufficient staff training is essential to ensure the proper and ethical use of AI applications. Comprehensive and easily accessible documentation should support employees, providing clear guidance for responsible AI use and decision-making. Finally, regular testing, evaluation and continuous monitoring of AI tools are mandatory for supervised financial institutions. This involves assessing the performance and accuracy of AI outputs, conducting routine quality and reliability checks, and documenting findings and processes. Where appropriate, independent reviews should be commissioned to ensure transparency and accountability. Another measure relates to ensuring proper data quality; in FINMA's view, data quality is often more important than model selection. The fact that reliance on historical data may be dangerous due to hidden biases is an issue well-known in econometrics and financial analysis. With respect to new AI use cases, the problem may become even more serious.

Next, financial institutions are called upon by FINMA to test their AI systems regularly with the use of ongoing monitoring. This measure aims to ensure the correctness and ongoing quality of outputs.

Finally, FINMA sets out that all AI processes should be carefully documented and be subject to independent reviews.

We have addressed many of these aspects in our publication "Navigating AI with Pestalozzi – A Practical Legal Guide". For more details on the definition of roles and responsibilities, data quality and monitoring, please refer to Part 1: Governance, while further explanations on inventories may be found in Part 4: Data Protection.

Initial conclusions for Swiss financial markets legislation

The technology-neutral, principle-based regulatory approach is an important concept in Swiss financial market law. It has also been adopted to regulate digital finance in Switzerland. Therefore, as is the case for traditional and digital finance, FINMA expects supervised institutions to actively consider the impact of their use of AI on their risk profile and to align their governance, risk management and control systems accordingly based on the general requirement to ensure appropriate business organisation. Risk managers at financial services providers are expected in particular to consider the materiality of the AI systems used and the probability that the associated risks will materialise.

FINMA announced that it will monitor the use of AI by supervised institutions and continue to closely observe developments in the use of AI in the financial industry, while engaging in close dialogue with relevant stakeholders and keeping up to date with international developments.

Outlook

Internationally, one such major development is the entry into effect of the EU AI Act (i.e. Regulation (EU) 2024/1689 of 13 June 2024 which stipulates harmonised rules on artificial intelligence), according to which AI systems deemed to present an unacceptable risk will already be prohibited as of 2 February 2025. All the measures proposed by FINMA in its latest guidance note can be found as special due diligence requirements for high-risk AI systems in in Art. 9-15 of the second section of the EU AI Act. AI systems intended to evaluate the creditworthiness of natural persons are explicitly listed in Annex III to the EU AI Act and therefore qualify as high-risk. Whether or not other AI use cases in the financial industry all qualify as high-risk AI systems must be assessed on a case-by-case basis. In view of this and based on the measures proposed by FINMA, it certainly seems advisable to all Swiss financial institutions to monitor the implementation of the EU AI Act closely and to consider its requirements at least as guidance when establishing relevant internal processes even if those requirements do not directly apply to them.

How the financial industry and other business sectors will implement these requirements in practice is still not entirely clear. More guidance and insights will undoubtedly be published over the coming months and years.

Next steps

With its latest guidance note, FINMA intends to strengthen the reputation of the Swiss financial centre and help financial institutions to sustainably protect their business models against risks related to the use of AI, by fostering a strong risk culture and governance and by introducing proactive risk management.

FINMA has announced its intention to refine its expectations of appropriate governance and risk management on the part of supervised institutions in connection with AI and, where necessary, to make them transparent in the market by issuing further guidance notes or circulars. Such guidance will take into account relevant international developments.

Further insights into future Swiss legislative developments can be expected from the upcoming DETEC report on AI.

Authors: Markus Winkler (Counsel), Sarah Drukarch (Partner), Andrea Huber (Partner)

No legal or tax advice

This Legal Update provides a high-level overview and does not claim to be comprehensive. It does not represent legal or tax advice. If you have any questions relating to this Legal Update or would like to have advice concerning your particular circumstances, please get in touch with your contact at Pestalozzi Attorneys at Law Ltd. or one of the contact persons mentioned in this Legal Update.

© 2025 Pestalozzi Attorneys at Law Ltd. All rights reserved.

Markus Winkler

Counsel
Attorney at law, Dr. iur., Dr. sc. math. ETH

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 92 59
markus.winkler@pestalozzilaw.com

Sarah Drukarch

Partner
Attorney at Law

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 93 23
sarah.drukarch@pestalozzilaw.com

Andrea Huber

Partner
Attorney at law, LL.M.

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 92 41
andrea.huber@pestalozzilaw.com