Navigating AI with Pestalozzi – Part 1: Governance

15.10.2024

Key Takeaways

- **A clear allocation of the different levels of responsibility regarding AI is essential for a safe use of AI tools.**
- **Establishing policies and (ethical) guidelines, regular audits, and trainings to raise awareness are key to mitigating risks posed by AI.**
- **AI governance – like all good governance – is not a linear process, which can be completed once, but is cyclical in nature and must be continually evaluated and revised.**

Necessity of AI Governance

AI presents substantial savings and opportunities for companies, which drives its adoption across nearly all sectors. Nevertheless, according to the December 2023 IAPP-EY Professionalizing Organizational AI Governance Report, 57% of European companies indicated that they do not control their use of AI. Integrating AI into products and internal processes without robust AI governance entails significant legal, financial, and reputational risks. While Swiss law currently does not provide specific regulations for AI, it does emphasize the board's responsibility to oversee AI initiatives as part of their general duties. In addition, the extraterritorial scope of regulations like the EU AI Act, which establishes comprehensive compliance obligations for providers and users of AI applications, makes it insufficient to consider only national laws. Regardless of whether the EU AI Act applies to your company, AI governance should be a top priority for the board of directors of Swiss companies. Ideally, this governance should be considered before the implementation of AI projects.

Effective AI governance balances the need for innovation with the imperatives of compliance with existing regulations, ethical considerations, and commercial value. The framework should

be as adaptive as AI itself, focusing on a risk-based approach that evaluates the likelihood of harm occurring, the severity of that harm, and appropriate mitigation measures associated with each AI use case. This chapter offers practical guidance on establishing a robust and dynamic AI governance framework in a company. It focuses on key elements, such as allocating responsibility and possible implementation methods of AI governance. Ultimately, each company should tailor its AI governance program to meet its individual business needs and objectives.

Allocating Responsibility

A successful AI governance framework is built on clearly defined roles, responsibilities and decision-making processes. Assigning accountability is essential to ensuring that AI initiatives align with organizational goals and defined ethical standards.

Four Levels of Responsibility

1. Board: The board of directors is responsible for overseeing all major company initiatives, including AI. This oversight includes understanding the potential risks associated with AI and ensuring that proper governance frameworks are in place to mitigate these risks, and that adequate staffing is ensured. Also, the board's involvement is crucial for aligning AI strategies with the company's goals and values, and for setting an effective tone from the top. The board of directors might also invite experts or external advisors to provide feedback on the company's AI governance strategy. Furthermore, it should be determined how the board will be regularly and appropriately informed about AI developments by the management or other functions, such as the AI committee (see below).

2. Management: While the board has ultimate oversight, the day-to-day management and operationalization of AI strategies are typically delegated to the management. Management is responsible for developing AI policies, integrating AI into business processes, and ensuring compliance with governance frameworks set by the board. The actual monitoring of adherence to regulations and internal policies should be delegated down to project leaders (see below), compliance or HR department.

   Management must also assess the impact of AI on various aspects of the business, such as efficiency, risk, and competitiveness, and regularly report these findings to the board. It also plays a key role in the coordination and collaboration across various functions within the organization. This includes working closely with the AI committee to ensure that AI initiatives are aligned with governance frameworks, and that all relevant departments, such as IT, legal, compliance, and business units, contribute effectively to AI projects. Furthermore, management must ensure that project leaders are appointed for each AI initiative. By embedding AI governance responsibilities within the management structure, the company can achieve a cohesive and effective implementation of AI that supports its strategic objectives.

3. AI Committee: Management should consider establishing an expert AI committee / task force with employees from different backgrounds, such as IT, finance, legal, compliance,

risk management, and from different business units. Evaluating governance issues related to AI increasingly requires a deep understanding of the technology context. These challenges require breaking down silos and working closely together on an ongoing basis, especially between legal, compliance and IT teams.

The committee should meet regularly and be the driving force within the company to promote and ensure a value-adding implementation of AI by:

- Mapping and monitoring how AI systems are being used internally;
- drafting of internal guidelines and processes for the deployment of AI and development of use cases, including best practices;
- keeping the board and management informed about technological and regulatory developments; and
- training employees on appropriate and effective use of AI.

4. AI Project Leader: For each AI initiative, a project leader should be designated to manage the day-to-day operations, ensure adherence to governance policies, and report progress to the AI committee and/or management. No AI use case should proceed without an assigned project leader responsible for following internal policies.

Reporting Structures

Establishing clear reporting structures will ensure that AI governance is effectively implemented and maintained. The AI committee should be in regular contact both with the AI project leaders as well as legal, compliance and IT teams to provide guidance and support. In turn, the AI committee should report regularly to the management and assist management in its reporting to the board on AI governance matters. A company with intensive use of AI is advised to make this report on a quarterly or semi-annual basis. In addition, a company-wide reporting system will help both the AI committee and the AI project leaders to be informed about the performance or reported problems of AI systems. Finally, clear escalation pathways should be defined.

Embedding Responsibilities in Bylaws

Defining AI governance responsibilities in corporate bylaws and policies both increases accountability and limits liability. The more specific the bylaws and policies, the better the company and its directors are protected from potential liability under Swiss law. Therefore, in particular the relevant policies should clearly state the structure of the company's AI governance system, the division of responsibilities, and the allocation of duties with respect to AI governance. Expanding the bylaws to include AI governance is the board's responsibility.

Risk Assessment

Effective AI governance requires robust risk management practices to identify, assess, and mitigate potential risks associated with AI deployment.

First, a risk assessment framework specific to AI projects should be developed. This should include identifying potential risks, such as data breaches, ethical violations, and operational failures, and assessing their impact and likelihood. Second, strategies to mitigate identified risks should be defined, documented, and implemented. This could involve technical measures, such as encryption and anonymization of (personal) data, as well as organizational measures, such as internal guidelines (see below), employee training and awareness programs. Finally, an incident response plan to address AI-related incidents promptly should be established. This plan should outline the steps to be taken in the event of a data breach, ethical violation, or other AI-related incidents.

Risk assessment and management are of particular relevance in the following areas: Data protection and cybersecurity (see Part 4: Data Protection), intellectual property rights (see Part 5: Intellectual Property), and employment related issues (see Part 6: Employment).

Internal Policies and Guidelines

Based on the risk assessment, the implementation of internal guidelines that address both legal and (non-legal) ethical principles are crucial for effective AI governance. While legal requirements are defined by the regulators to which the company is subject, ethical standards are to be established by each company individually. Companies need to define acceptable and prohibited AI practices, set guidelines for transparency and quality standards, and develop assessment procedures.

There are various proposals of AI guidelines or principles from international organizations and authorities that can be used as a source of reference. Following the key principles recommended by the EU for achieving trustworthy AI, we recommend:

- Human Agency and Oversight: Companies should respect human autonomy and fundamental rights and ensure users can understand and interact with AI. There should always be human oversight, allowing individuals to override AI decisions when necessary.
- Technical Robustness and Safety: AI systems must be secure, reliable, and robust enough to handle errors and inconsistencies throughout their lifecycle. This includes cybersecurity measures and processes to assess and mitigate safety risks.
- Privacy and Data Protection: Compliance with data protection regulation is mandatory. AI systems that are used should protect privacy and personal data, using techniques like anonymization and data encryption.
- Transparency and Avoidance of Bias: Data sets and processes used in AI development should be documented and traceable. AI systems should be identifiable as such, and their decisions must be explainable and understandable to humans, especially in high-stakes applications like healthcare and finance. AI tools should be regularly audited to ensure they are using appropriate data quality, operating fairly and not perpetuating bias.
- Accountability: Mechanisms to ensure responsibility and accountability for AI systems are essential. This includes independent audits, reporting negative impacts, and impact assessment tools. Decisions on ethical trade-offs should be continuously re-evaluated.

Once these principles are established, they should be documented and translated into actionable instructions for employees. Smaller companies may use concise general guidelines in a one-pager format, while larger companies with different use cases sare advised to create an overarching AI strategy along with more detailed policies and directives for different implementation areas. This ensures that the information is available in a digestible and clear manner, and that employees know where to look for relevant information and understand their responsibilities when using AI.

AI policies should be coordinated with existing data protection, IT, and HR directives. Some documentation obligations in the EU AI Act, for example, overlap with regulations in the GDPR and the Swiss Act on Federal Data Protection. One such obligation is the data protection impact assessment, which should be conducted when new technologies are implemented (see Part 4: Data Protection).

Furthermore, it is generally advisable to involve legal counsel familiar with regulatory requirements, when drafting internal guidelines and implementing the governance framework to ensure adherence to legal standards. This includes compliance with data protection laws, industry-specific regulations, and emerging AI-specific legislation (see Part 2: Regulation).

10 Practical Steps to Implement AI Governance



Important to remember is that AI governance is not a one-time effort but an ongoing process that requires continuous monitoring and improvement to ensure its effectiveness. Hence, the steps mentioned above should be regularly re-performed based on the then established framework.

Contributors: Christoph Lang (Partner), Sarah Drukarch (Partner), Simon Winkler (Associate), Luise Locher (Junior Associate)

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.

© 2024 Pestalozzi Attorneys at Law Ltd. All rights reserved.

Christoph Lang

Partner
Attorney at law
Chair, Head Corporate / M&A

Pestalozzi Attorneys at Law Ltd
Feldeggstrasse 4
8008 Zurich
Switzerland
T +41 44 217 92 39
christoph.lang@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

