AI FLASH

AI Governance in the Boardroom

What a CEO and board of directors should broadly know about the EU AI Act, EU Data Act and Swiss AI supervisory practice

2026 · AI FLASH · APPROX. 8 MIN READ · DR. IUR. DIRK SPACEK

1. Background

AI regulation has long ceased to be merely an EU topic for IT and compliance departments. It has become a leadership and governance issue that directly affects Swiss companies too, particularly financial institutions – whether because they operate in the EU market, or because FINMA (the Swiss Financial Market Supervisory Authority) is systematically sharpening its own expectations on AI governance. This article briefly outlines the regulatory compliance framework and introduces what a CEO and board of directors should specifically do in this regard.

2. The European Regulatory «Stack»

The EU does not regulate AI in a single law. Instead, several instruments build on one another like components of a stack – hence the frequently used term «regulatory stack». Two instruments are currently central for companies: the EU AI Act (which regulates AI systems themselves) and the EU Data Act (which regulates access to the data these systems work with). The two complement each other – and both are often underestimated in practice, because discussion tends to focus solely on the EU AI Act.

AI Act	**Data Act**
Regulation (EU) 2024/1689, in force since 1 August 2024 • Regulates **AI systems** themselves: the higher the risk to individuals, the stricter the obligations under this law. • Risk-based approach: three risk levels: 1. Unacceptable (e.g. social scoring), i.e. prohibited; 2. High (e.g. biometric identification), i.e. obligations for accompanying measures such as conformity assessments, a risk management system, documentation and transparency; 3. Minimal or no risk. • Obligations under the AI Act are staggered and will take full effect gradually by 2028.	Regulation (EU) 2023/2854, applicable since 12 September 2025 • Does not regulate AI, but rather **access to data** – in particular from connected devices (IoT) and digital services. • Users gain a right to «their» machine-generated data and may share it with third parties. • Prohibits one-sided, unfair data clauses in B2B contracts and facilitates switching providers.

NOTE
Please note that these articles are of a purely academic nature and do not constitute legal or business advice.

The AI Act enters into force in stages

Important in practice: the AI Act does not apply all at once, but rather **in stages**. The most recent «**Digital Omnibus**» – a comprehensive EU legislative package intended to simplify and jointly harmonise European digital law (AI Act, Data Act and GDPR) to reduce hurdles and overlaps – has pushed back the timing of the strictest AI Act obligations, but without softening their substance.

- February 2025 — Prohibited AI practices and the obligation to ensure staff AI literacy (Art. 4) take effect.
- August 2025 — Governance rules and obligations for general-purpose AI models (e.g. large language models) take effect.
- August 2026 — Transparency obligations (Art. 50) take effect: chatbots, deepfakes and AI-generated content must be labelled.
- December 2027 / August 2028 — Full obligations for high-risk AI take effect (risk management, documentation, human oversight) — these dates were rescheduled by the Digital Omnibus.

How do the AI Act and Data Act interact?

In short: the AI Act requires companies to ensure and demonstrate the quality and provenance of their AI training and operational data. The Data Act provides the foundation for this by regulating who gets access to data at all and how it may be shared fairly. Companies that focus solely on the AI Act therefore often overlook the data-access and contractual obligations that must also be met in the background. This «stack» is further supplemented by additional EU instruments on the data economy (including the EU Data Governance Act and the Digital Markets/Services Act) as well as by the European GDPR, which continues to take precedence for personal data.

3. Why does this concern Switzerland?

Extraterritorial effect

Neither the EU AI Act nor the EU Data Act applies in Switzerland – Switzerland is not an EU member state. Nor does it have its own „AI Act“. However, both instruments have **a de facto extraterritorial effect**: the AI Act captures Swiss companies as soon as they place AI systems on the EU market, make them available in the EU, or where the **output** of an AI system operated from Switzerland is used within the EU. The Data Act similarly captures Swiss manufacturers of connected products or digital services that are intended for the EU market or affect EU users. For Swiss companies operating across borders – particularly financial institutions with EU clients, EU branches or EU cloud infrastructure – the EU «stack» is therefore genuinely relevant in practice.

The Swiss approach: sectoral rather than horizontal

On 12 February 2025, the Federal Council decided against a comparable AI Act and in favour of a **sectoral regulatory approach** (i.e. it is examining whether sector-specific legislation or statutory amendments may be needed). Switzerland is to ratify the **Council of Europe's AI Convention** (signed in March 2025) and transpose it selectively into existing law, supplemented by non-binding measures (self-regulation, industry guidelines, codes of ethics). Note: the Council

NOTE
Please note that these articles are of a purely academic nature and do not constitute legal or business advice.

of Europe is a separate international organisation, not the EU – non-EU countries are members too. The lead agency, the Federal Department of Justice and Police («**FDJP**»), together with the Department for Environment Traffic Energy and Communications («**DETEC**») and the Department for Foreign Affairs («**DFA**»), is currently preparing a consultation draft by the end of 2026 on the topics of transparency, data protection, non-discrimination and AI oversight. A **horizontal AI law modelled on the EU is, however, not expected for the foreseeable future** – though selective adjustments in individual areas of law and sectors are likely.

FINMA and other supervisory authorities become more concrete

In the financial sector, **FINMA** set out its expectations for **governance and risk management in AI deployment** in its **Supervisory Communication 08/2024** (December 2024) – technology-neutral, following the principle „same business, same risks, same rules". It requires in particular a central inventory of AI applications, clearly defined responsibilities, documentation, testing, ongoing monitoring and training; FINMA identifies the main risks as operational risks (model risks such as bias or lack of explainability), data risks, IT/cyber risks, and growing third-party dependency. A FINMA survey from early 2025 shows that around half of supervised institutions already use AI, with a further quarter planning to do so within the next three years. FINMA has since deepened the topic in **further supervisory communications** – for example on digital fraud risks and deepfakes (Communication 02/2026) and on cyber risks accelerated by quantum computing (Communication 05/2026) – a clear signal that AI governance is, and is meant to remain, a board-level matter from the supervisor's perspective.

4. What should a CEO and board of directors concretely do and implement now?

Regardless of whether the EU AI Act formally applies: within the European market it de facto sets the standard for «good» AI governance, one that FINMA's expectations also draw on. For the board of directors and executive management – especially at financial institutions – the following approach is generally recommended:

AI Governance & Responsibilities

- **AI inventory**: record all systems in use, procured or under development, including role (provider/operator), purpose and data processed.
- **Clear responsibilities**: define them (a board member responsible for AI governance, an AI officer or AI committee at executive level) with regular reporting to the board.
- **Risk classification per use case** – based on the AI Act's logic – as the basis for the scope of necessary internal controls.

Identifying and containing «shadow AI»

A point missing from many governance concepts: AI adoption rarely begins with a formal strategy, but rather with a team trying out a new tool, an employee using an AI assistant, or a vendor building AI features into an existing platform. This is not inherently problematic – it is often exactly what companies want: innovation and efficiency. It becomes critical, however, when AI usage grows

NOTE
Please note that these articles are of a purely academic nature and do not constitute legal or business advice.

faster than the organisation can track – when management knows which tools are officially approved, but not which tools employees actually use, what data is entered into them, and who ultimately remains responsible for AI-supported decisions. That is precisely why shadow AI is not just an IT issue, but a governance warning sign for a company: you cannot manage what you cannot see.

- **Visibility (documentation) before bureaucracy**: build a reliable picture of which AI tools are used for what, what data they process, who is responsible for each use case, and which cases require approval or additional controls.
- **Governance process**: the core building blocks are an AI policy, an onboarding process for new tools, an AI inventory, clear responsibilities, approval pathways and documentation of key decisions. But beware: a process that is too slow or complicated only pushes usage further into the shadows.
- **Differentiate governance by risk**: an AI tool used for non-critical internal drafting needs different controls than one that works with customer, HR or health data, or materially influences decisions.
- **Involving users:** not banning, but involving: employees will keep experimenting with AI – the more effective strategy is to allow actual usage within a framework of visibility, accountability and proportionate controls, rather than blocking the benefits of the technology.

Data & Third Parties

- **Data governance** modelled on Art. 10 AI Act: document data quality, provenance and bias testing of AI systems.
- **Where personal data is involved**: demonstrate the lawfulness/authorisation for using such data in AI systems, and implement safeguards for data-protection-compliant processing (under both the GDPR and the Swiss Data Protection Act).
- **Contracts with AI and cloud providers**: review for **Data Act compliance** (no abusive clauses, sufficient exit/switching options, interface interoperability). The aim of this review is to ensure that your company has adequate exit options (no vendor lock-in) and that contractual access to your own (machine-generated) data is secured.
- **Due diligence on third-party AI providers**: proof of conformity, documentation and contractual safeguards (liability, information rights, outsourcing rules) should also be in place with these third-party providers.

Evidence and training obligations

- **Ensure AI literacy within the company** (a training concept, particularly for employees in sensitive areas such as HR or lending).

NOTE
Please note that these articles are of a purely academic nature and do not constitute legal or business advice.

- **Implement transparency measures** (labelling of chatbots, AI-generated content, deepfakes) – worthwhile for reputational and trust protection even without a direct Swiss obligation.
- **Traceable documentation and monitoring processes**: establish processes that provide robust evidence in the event of an audit.

Strengthening cybersecurity alongside AI expansion

Another aspect often overlooked when building AI governance: it is not only companies that are increasingly relying on AI – cybercriminals have long since discovered it too. Attackers increasingly use AI-powered tools to scan for vulnerabilities automatically, automate attacks, and craft phishing emails in a fraction of the previous time – resulting in a higher frequency and success rate of attacks. Anyone investing in **building their own AI capabilities** should also advance **cybersecurity at least at the same pace**.

- **Cybersecurity tools**: deploy tools specifically designed for AI-powered attack patterns (automated scans, adaptive malware, AI-driven phishing).
- **Cybersecurity training**: do not cut it back, expand it – technology alone does not protect; good digital security habits (including multi-factor authentication, password hygiene, recognising AI-generated phishing) remain essential.
- **Plan the cybersecurity budget and AI investment budget together**, so that security measures do not lag behind AI adoption.

Specific to financial institutions

- Aligning internal governance with **FINMA Supervisory Communication 08/2024**: inventory, responsibilities, testing, monitoring and training as a minimum standard.
- For AI use in critical processes or in calculating regulatory metrics, engage with FINMA early.
- Ensure explainability and independent review of models, particularly in lending, fraud detection and transaction monitoring.
- Actively track regulatory developments (EU Digital Omnibus, the Swiss consultation due end of 2026, further FINMA communications, e.g. on post-quantum-computing encryption etc.) and periodically update the governance framework.

4. Key Takeaways for the CEO and Board

> AI governance is not an IT project but a leadership matter that brings together risk management, data law, contract drafting and supervisory compliance monitoring. Companies that approach this «stack» in a structured way not only reduce regulatory risk but also lay the foundation for responsibly capturing all opportunities AI offers. An in-depth analysis of individual aspects – such as risk classifications under the EU AI Act, specific contractual

NOTE
Please note that these articles are of a purely academic nature and do not constitute legal or business advice.

> clauses under the EU Data Act, or FINMA's detailed requirements – is not undertaken here and remains subject to separate case-by-case review.
>
> .

This short publication is for general information purposes only and does not replace legal advice in an individual case.

Dirk Spacek, Dr. iur., LL.M. is an attorney and partner in Zurich. He advises companies on all contractual and commercial law matters, with a particular focus on issues at the intersection of technology, intellectual property and data/cyber law.

NOTE
Please note that these articles are of a purely academic nature and do not constitute legal or business advice.