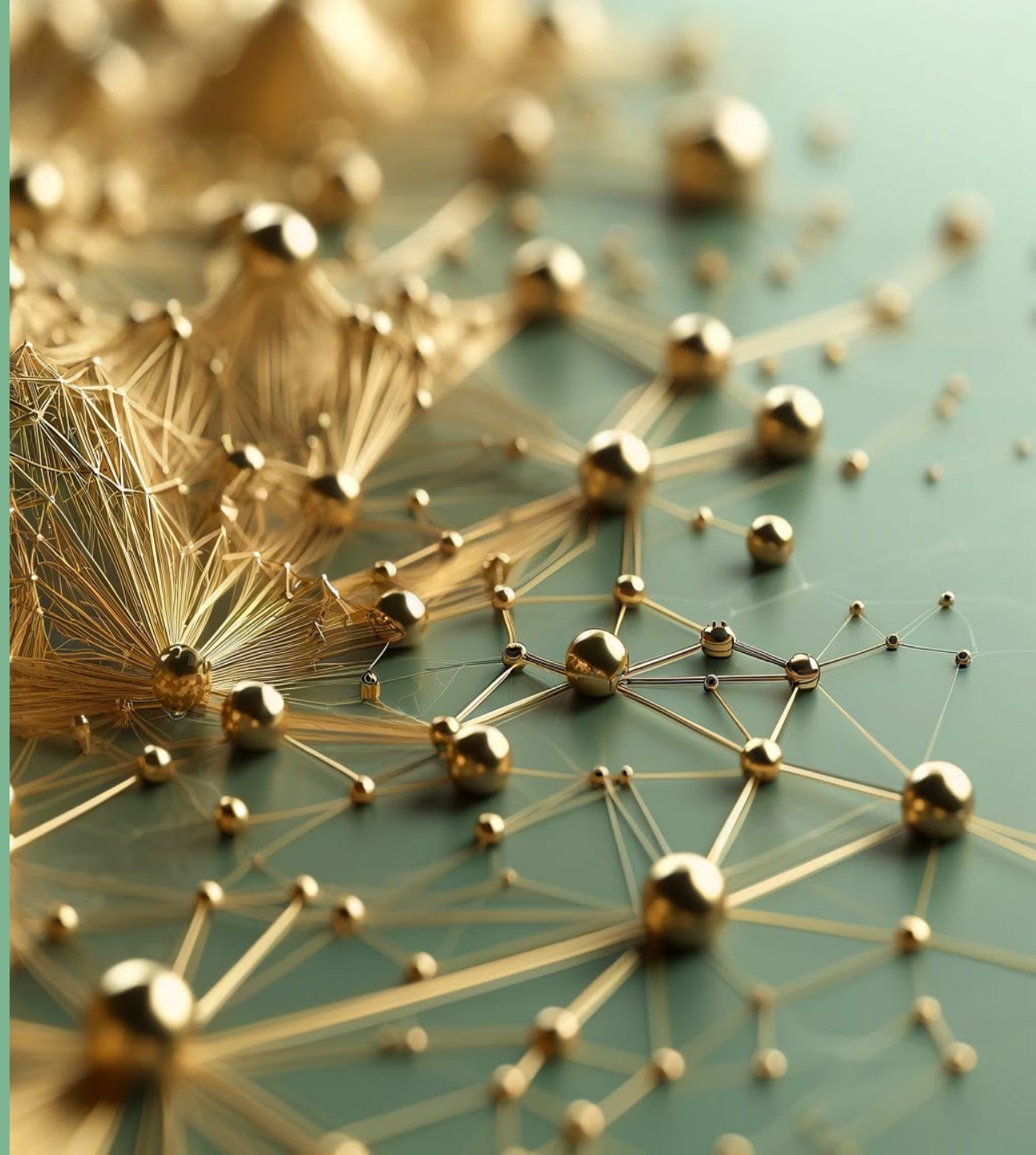


SCSD 2025

AI Regulation

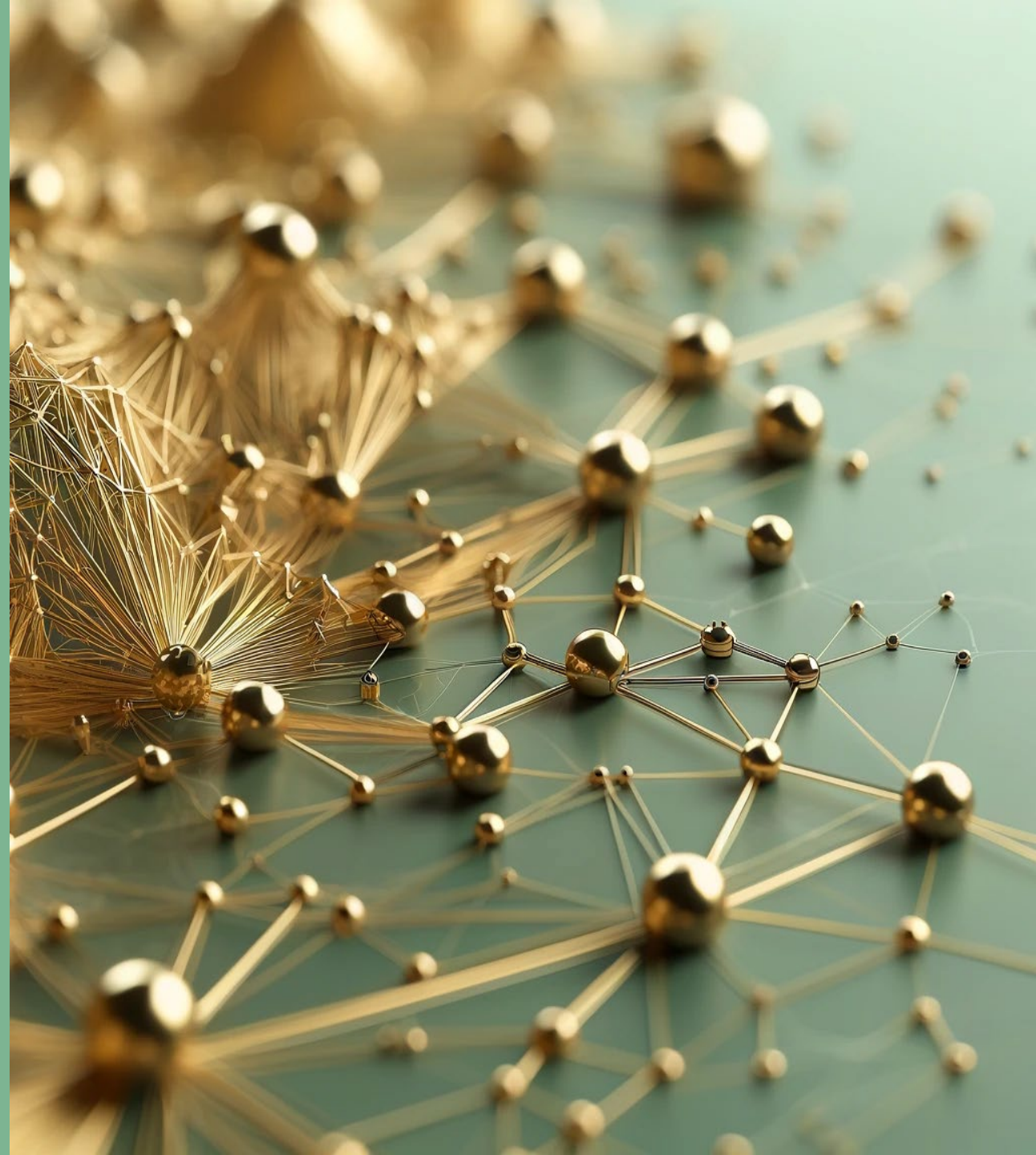
Martina Arioli, Attorney-at-Law, Partner
Arioli Law, Zurich
18 February 2025

ariolilaw/




Overview

- Swiss Approach to AI Regulation
- OECD as common denominator
- CoE AI Convention
- EU AI Act
- Threats



Breaking News!



 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Federal Office of Communications
OFCOM**

Digitalisation and Internet	Telecommunication	Electronic media	Frequencies and antennas	Equipments and installations	OFCOM	
-----------------------------	-------------------	------------------	--------------------------	------------------------------	-------	--

[Homepage](#) > [Digitalisation and Internet](#) > [Digitalisation](#) > [Artificial Intelligence](#)

[← Digitalisation](#)

Artificial Intelligence

Artificial Intelligence

[AI - Guidelines](#)

Overview and Switzerland's regulatory approach

Artificial intelligence (AI) has developed rapidly in recent years. With the broad availability of generative AI applications such as ChatGPT, the topic of AI has also entered the public debate. For Switzerland as a business and innovation location, AI offers great opportunities. At the same time, new legal challenges arise, for example regarding the transparency and traceability of AI-based decisions.

In response to these challenges, new legal frameworks such as [the Council of Europe's AI Convention](#) and [the EU's AI Act](#) have been developed.

[Overview of 12 February 2025](#)



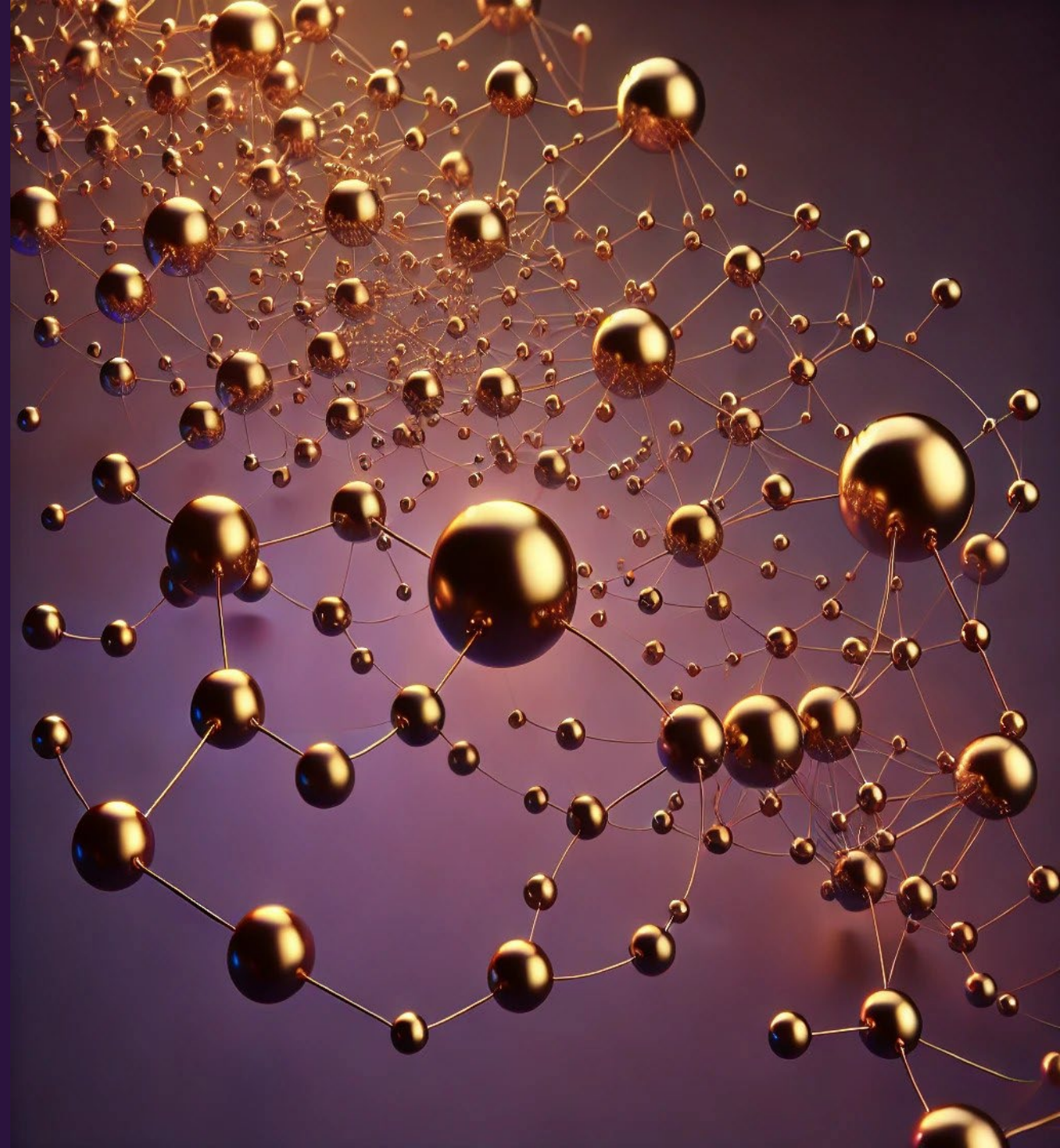
The Swiss Approach

Dec 2019:	Report to the Federal Council 'Challenges of AI: <i>"no action required"</i>
Nov 2020:	AI Guidelines for the Federal Administration
Aug 2021:	Creation of the CNAI (Competence Network for Artificial Intelligence) and AI database
Apr 2022:	Report 'AI and international regulations' (FDFA) <i>"need for action"</i>
Dec 2022:	Data science strategy of the Confederation

12 Feb 2025: Assessment of the requirements to legislate on AI finally published

1. AI needs to be regulated
2. Switzerland will **not adopt the EU AI Act, August 2024**
3. Switzerland will ratify the **AI Convention issued by the Council of Europe, May 2024**
4. Legislative changes necessary for the ratification of the AI Convention will be **sector-specific**. Only **key areas** relevant to fundamental rights will be general, cross-sectoral. Supplementary non-binding measures.

OECD AI Principles



What Switzerland, EU and CoE have in common:

1. Definition of AI System [OECD]

“An AI system is a **machine-based system** that, for explicit or implicit **objectives**, **infers**, from the input it receives, how to generate **outputs** such as predictions, content, recommendations, or decisions that can **influence** physical or virtual environments. Different AI systems vary in their levels of **autonomy** and **adaptiveness** after deployment.”

Similar definition under the AI Act and the Council of Europe’s AI Convention, now adopted by Swiss Government.

[Recommendation](#) of the OECD Council on Artificial Intelligence (8 Nov 2023)

What Switzerland, EU and CoE have in common:

2. OECD AI Principles

The OECD AI Principles promote use of AI that is **innovative** and **trustworthy** and that **respects human rights and democratic values**.






Adopted in **May 2019**, they set **standards** for AI that are “practical and flexible enough to stand the test of time”.

<https://oecd.ai/en/ai-principles>






Currently **1000 AI policy initiatives** from **69** countries, territories and the EU.

<https://oecd.ai> and <https://oecd.ai/en/dashboards/overview>

Values-based principles

-  Inclusive growth, sustainable development and well-being >
-  Human-centred values and fairness >
-  Transparency and explainability >
-  Robustness, security and safety >
-  Accountability >

Recommendations for policy makers

-  Investing in AI R&D >
-  Fostering a digital ecosystem for AI >
-  Providing an enabling policy environment for AI >
-  Building human capacity and preparing for labour market transition >
-  International co-operation for trustworthy AI >

What Switzerland, EU and CoE have in common:

3. Exclusion of National Security

- AI in **defence and national security**.

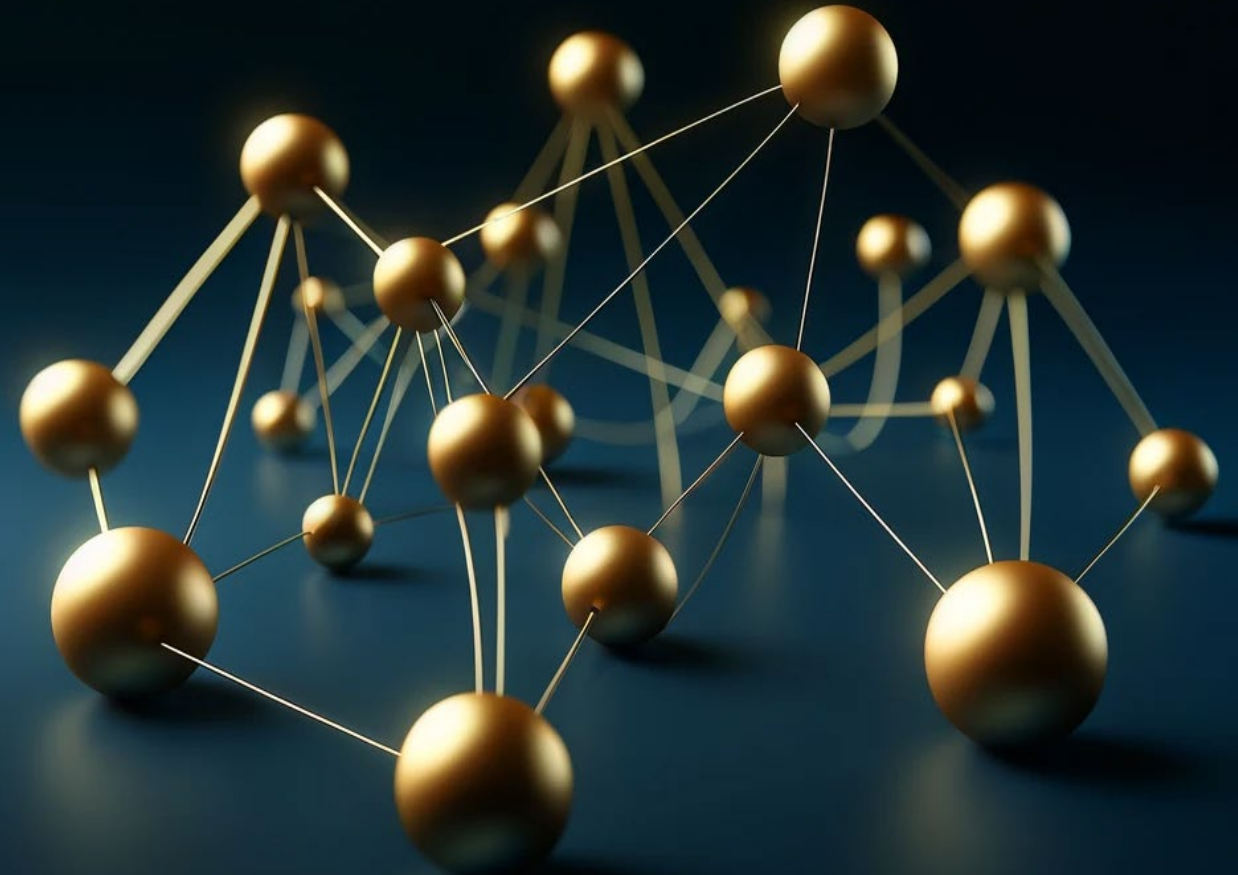
This includes for **Switzerland**:

- police emergency response, state security and criminal prosecution;
- prevention, preparedness and management of natural and man-made disasters and emergencies;
- prevention and defence against military attack;
- safeguarding Switzerland's interests abroad and contributing to international crisis management

However, the Department of Justice assumes that AI systems developed / deployed by the Federal Intelligence Service (NDB) would be covered by the CoE AI Convention safeguarding human rights.

- Also excluded: **AI in research!**

AI Framework Convention of the Council of Europe



Council of Europe AI Framework Convention

- Issued in May **2024**
- Aims to establish a **global minimum standard** for protecting **human rights, democracy and the rule of law**
- underlying core principles and key obligations include a **risk-based approach** and **obligations** considering the entire **life cycle** of an AI system (similar to EU AI Act)
- **Not** directly applicable! Contains **broad principles** rather than prescriptive rights and obligations. Needs to be implemented into national laws.

[Council of Europe Website](#)

Council of Europe AI Framework Convention

- Issued in May 2024
- Aims to establish a **global minimum standard** for protecting human rights, democracy and the rule of law
- underlying core principles and key obligations include a **risk-based approach** and **obligations** considering the entire **life cycle** of an AI system (similar to EU AI Act)
- *Not* directly applicable! Contains **broad principles** rather than prescriptive rights and obligations. Needs to be implemented into national laws.

[Council of Europe Website](#)

Signatory states are obliged to **implement** national laws covering:

- **Protection of human rights, human dignity**
- **Integrity of democratic processes and respect for the rule of law**
- **Transparency and oversight**
- **Accountability and responsibility**
- **Equality and non-discrimination**
- **Privacy rights**
- **Reliability**
- **Safe innovation**
- **Risk and impact management framework**



Council of Europe AI Framework Convention

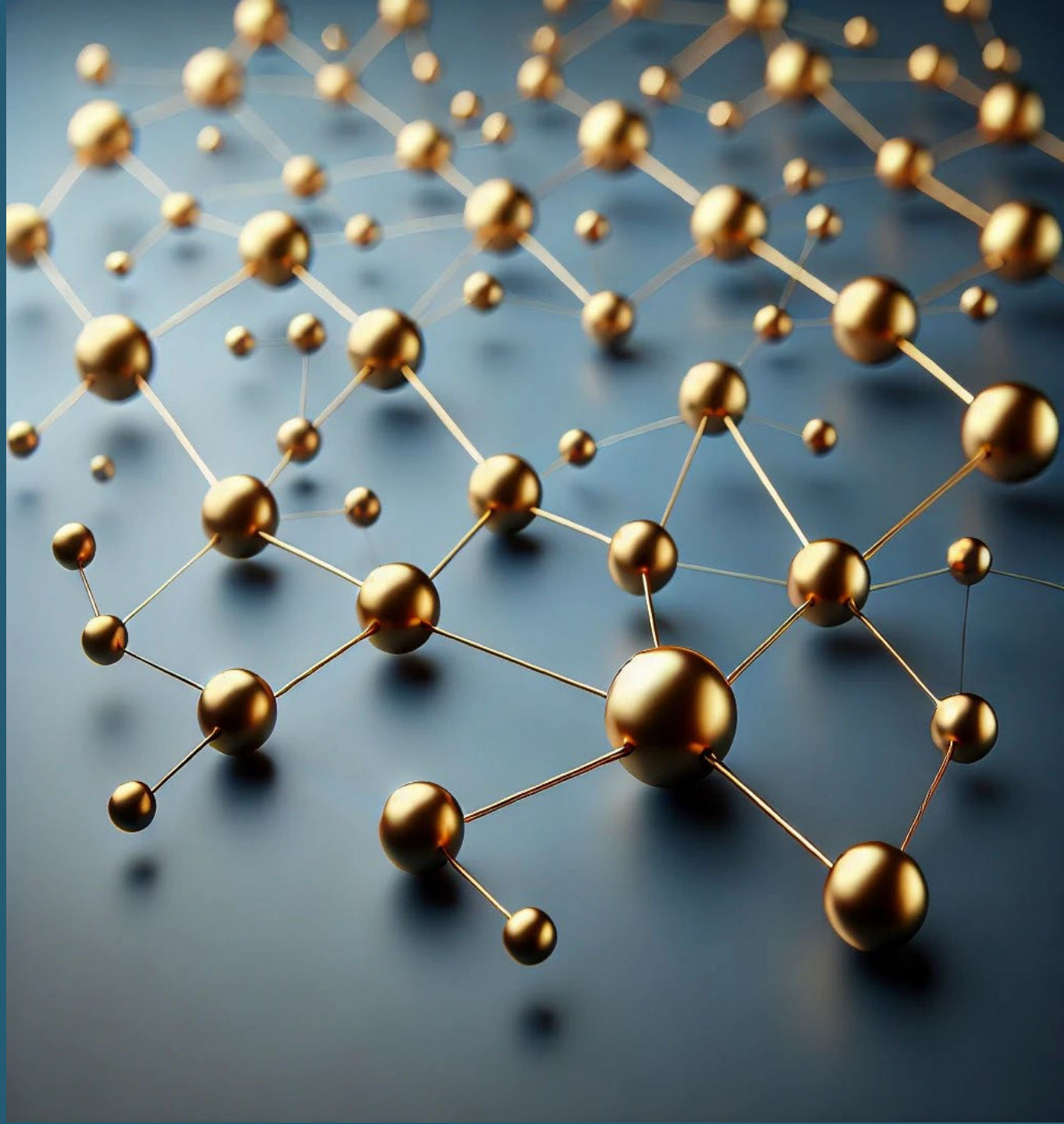
- Issued in May 2024
- Aims to establish a **global minimum standard** for protecting human rights, democracy and the rule of law
- underlying core principles and key obligations include a **risk-based approach** and **obligations** considering the entire **life cycle** of an AI system (similar to EU AI Act)
- *Not* directly applicable! Contains **broad principles** rather than prescriptive rights and obligations. Needs to be implemented into national laws.

[Council of Europe Website](#)

Signatory states are obliged to **implement** national laws covering:

- Protection of **human rights**, human dignity
- Integrity of democratic processes and respect for the rule of law
- **Transparency and oversight**
- **Accountability and responsibility**
- **Equality and non-discrimination**
- **Privacy rights**
- **Reliability**
- **Safe innovation**
- **Risk and impact management framework**
- **Switzerland has a need for regulation!**

EU AI Act

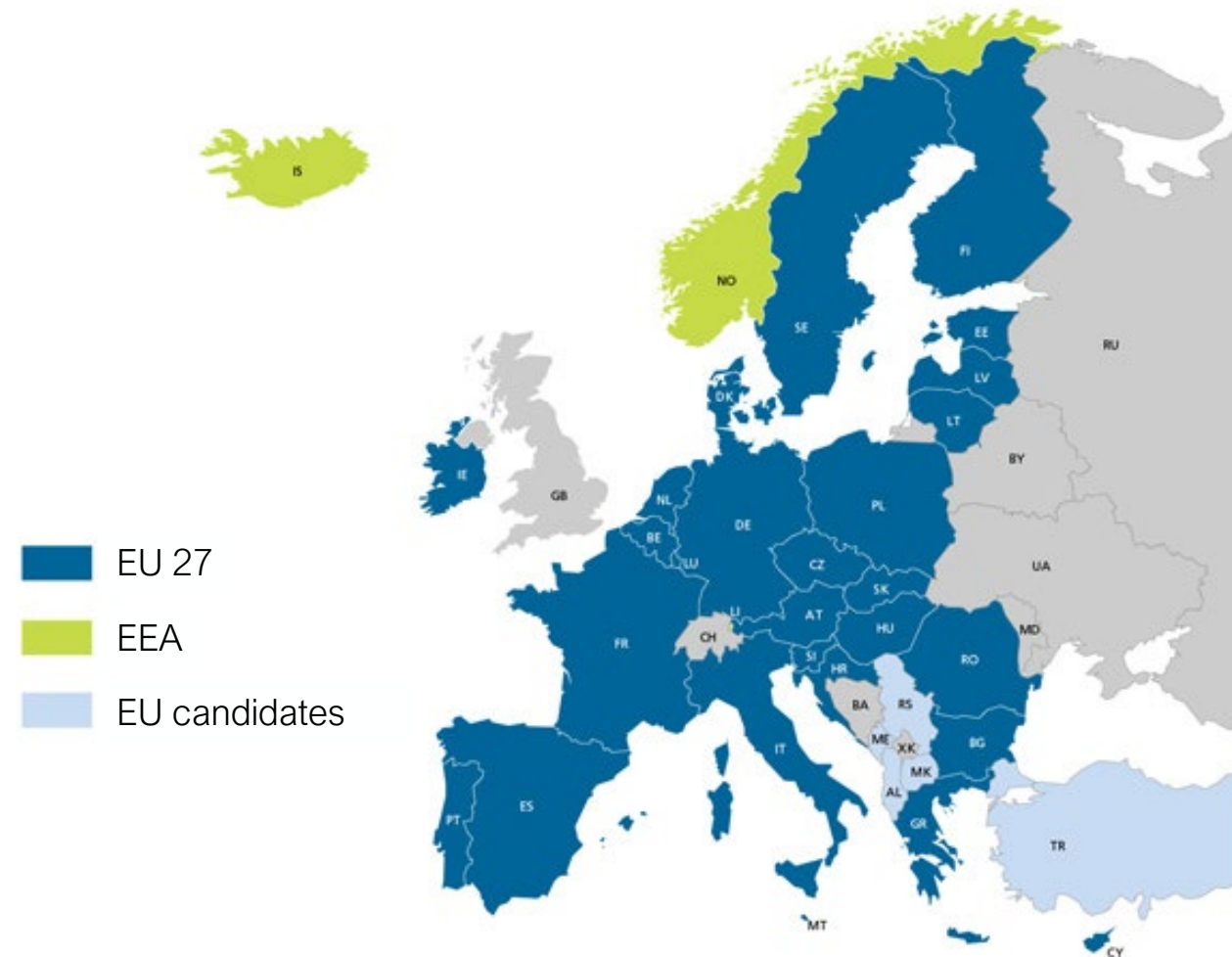




Scope and Applicability

The AI Act applies to anyone who:

- **puts** an AI system on the EU market,
 - **uses** an AI system in the EU,
 - **outputs are used in the EU or affect EU citizens.**
- **extraterritorial effect:** AI Act is applicable if services are used within the EU market, regardless of where the company is established.
- Compliance obligations primarily on **providers**
- **Harmonized standards** available in spring 2025
- Applies both private *and* public actors, *not applicable to private users!*





EU AI Act

- improve the functioning of the **internal market**
- promote human-centric and trustworthy AI
- ensure **health, safety, fundamental rights, democracy, rule of law, environmental protection**, against the harmful effects of AI systems in the EU
- **Horizontal**
- essentially **product safety regulation!**
- Regulation of the **technology "AI"**
- **Risk-based**
- In line with the Council of Europe's AI Convention



EU AI Act

- ensure **health, safety, fundamental rights, democracy, rule of law, environmental protection**, against the harmful effects of AI systems in the EU
- promote human-centric and trustworthy AI
- improve the functioning of the **internal market**
- **horizontal**
- essentially **product safety regulation!**
- regulation of the **technology "AI"**
- **risk-based**
- In line with the CoE AI Convention

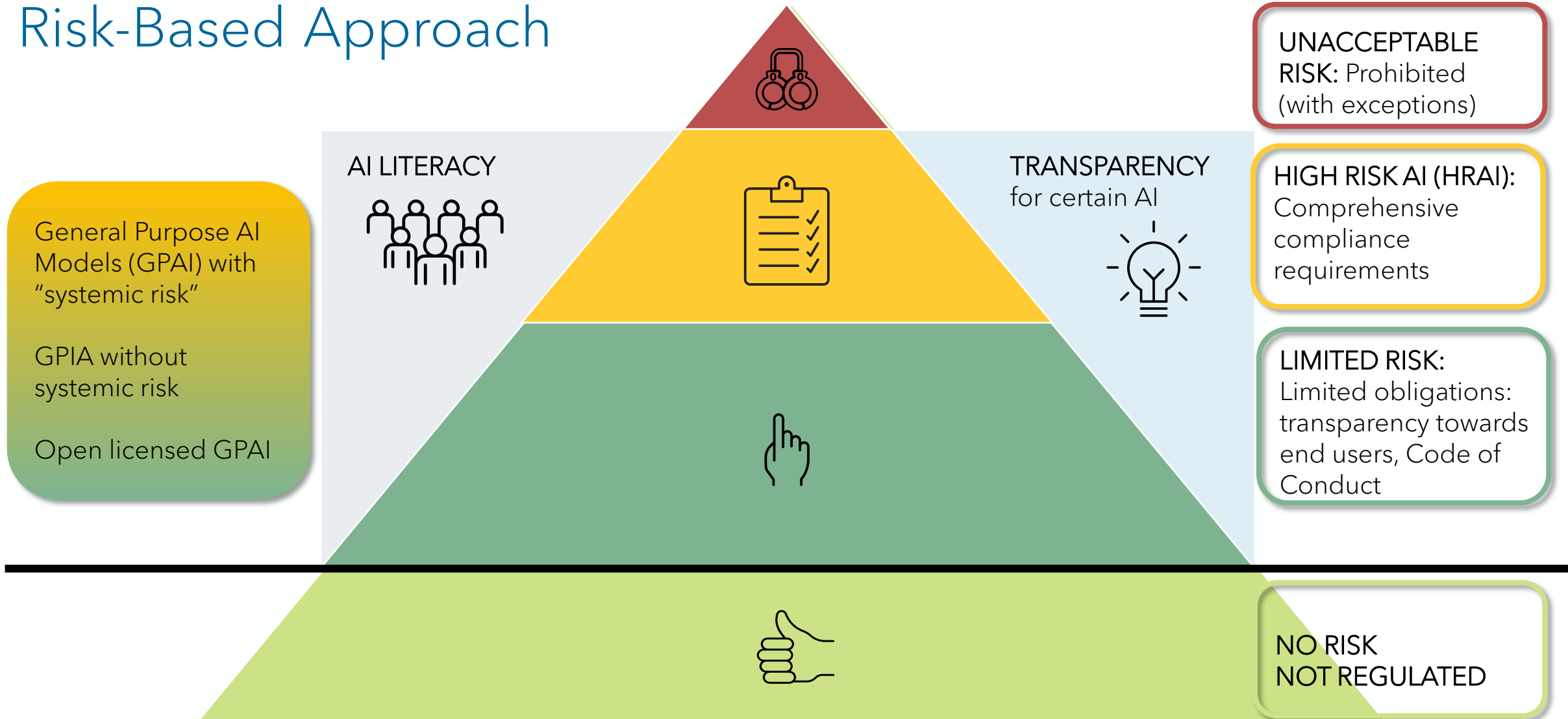


Swiss Approach

- *not yet fully covered*
- essentially **sectoral** approach
- *limited* product safety approach
- **technology-neutral** and **principle-based**
- *no classification according to risks*
- *not yet in line with CoE AI Convention*

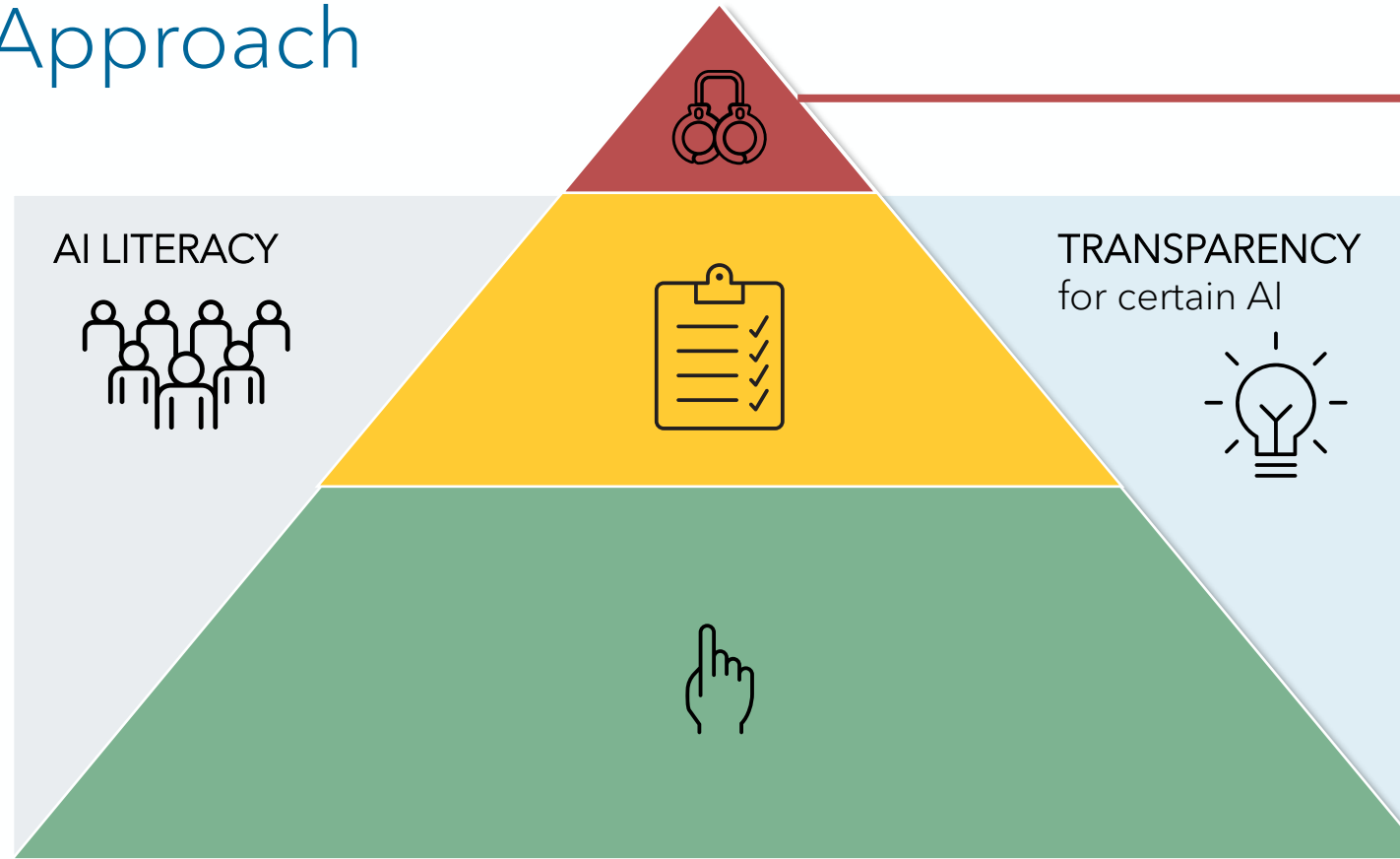


Risk-Based Approach





Risk-Based Approach



PROHIBITED DUE TO UNACCEPTABLE RISK:

(with exceptions) are AI Systems used for:

- biometric identifications and categorization
- emotion recognition
- social scoring
- behavioural manipulation
- exploitation of vulnerabilities of children

➤ **strong stance on societal values**

No respective prohibition in Switzerland!



Risk-Based Approach: High-Risk AI Systems (HRAI)

Art. 6.1 and Annex I

AI systems used as a product or security component of a product **in regulated industries**: (i.e. require pursuant to product safety regulations a conformity assessment, conformity declaration, CE mark), in particular:

- medical devices
- civil aviation
- vehicle security
- marine equipment
- transportation
- toys

Swiss product safety laws need amendment!

Art. 6.2 and Annex III

high-risk areas of application:

- biometric systems
 - critical infrastructure
 - education sector: admission, assessment, monitoring
 - work environment: application, promotion
 - public services, credit rating
 - law enforcement
 - migration, asylum and border control
 - administration of justice and democratic processes
- *There are exceptions (Art. 6.3 AI Act)!*
- *Annex III can be changed by the EU Commission*

No respective legislation in Switzerland!



Obligations regarding High-Risk AI Systems (HRAI)

Provider (Art. 16)

Quality Management System (Art. 17)

Accuracy, robustness and cybersecurity (Art. 15)

Risk Management System (Art. 9)

Documentation for supervisory authorities

Data Governance (Art. 10)

Conformity and CE (Art. 43, 47, 48)

Technical Documentation (Art. 11)

Registration (Art. 49)

Record-keeping (Art. 12)

Document Compliance

Transparency / instructions for use (Art. 13)

Post-Market-Monitoring (Art. 72)

Ensure human oversight (Art. 14)

Corrective measures (Art. 20)

Deployer (Art. 26 and 27, Art. 86)

Information of the natural person

Information of employees

TOM according to instructions for use

DPIA according to the instructions for use

Data Governance

Fundamental Rights Impact Assessment

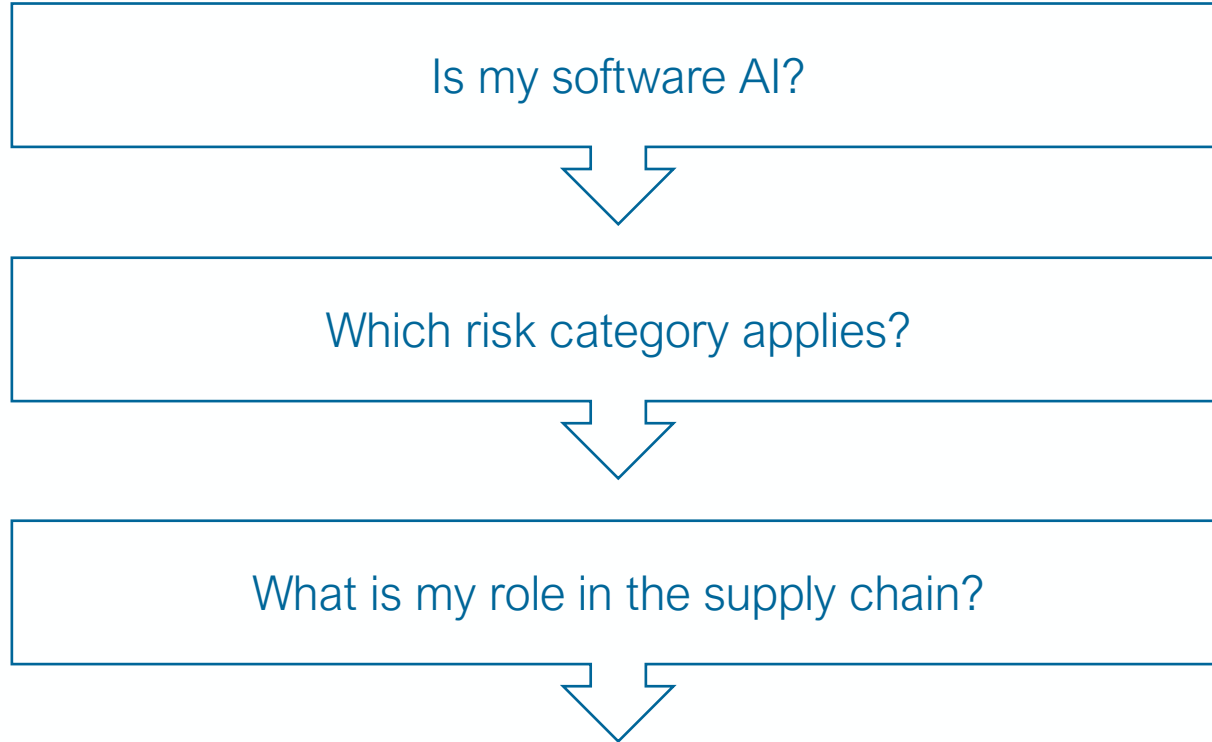
Record-keeping

Explanation of individual decision-making (Art. 86)

Notification of supervisory authority and Provider

Authorisation of remote biometric identification

Summary of Initial Compliance Steps



- Broad definition of AI
- Determine forbidden / high-risk / low / no risk in order to determine applicable provisions
- Provider? Deployer? Importer? Distributor? Important to determine compliance obligations



When will the EU AI Act take effect?

The EU AI Act has entered into force on **1 August 2024**. Simplified, the following **transition periods** apply:

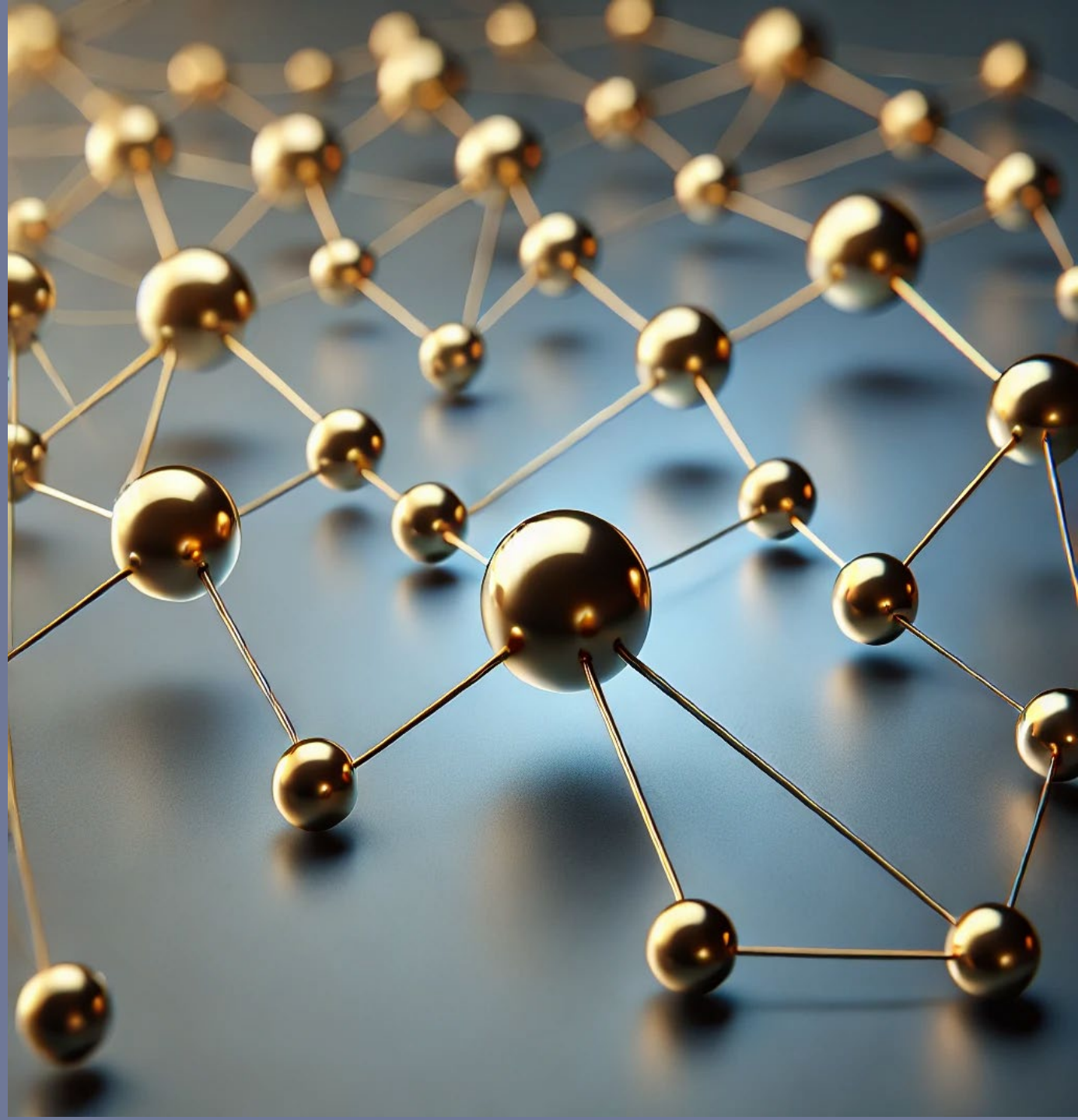
2.2.2025: Prohibited AI, AI Literacy, general provisions

2.8.2025 General-purpose AI models, penalties, enforcement

2.8.2026: standalone HRAI (Annex III), transparency, regulatory sandboxes

2.8.2027: HRAI (Annex I), general-purpose AI models already on the market

AI and Cyber Threats Switzerland



Threats:

- Periodic table © Iryna Schwindt

Spi: susceptibility to prompt injections

Sjb: susceptibility to jailbreak attacks

Its: insufficient tenant segregation

Me: model extraction

Pgc: poor guardrails configuration

Check harmonized standards be [CEN and CENELEC](#)

See also the [MIT AI Risk Repository](#)

The AI Risk Database captures 1000+ risks extracted from 56 existing frameworks and classifications of AI risks

Periodic Table of (Gen)AI Risks

A quick reference for cybersecurity professionals

Platform		Integration							Application		Data
Identifier	Short form	Name							Runtime	Dev/Test	
P 01 •	Opa	Ich							A 04	A 10 •	D 01
	Overprivileged access	Insecure credentials handling							Mio	Icd	Ptd
		Traditional cybersecurity risk							Missing input/output validation	Insecure CI/CD pipelines	Poisoned training data
P 02 •	Idc	I 01 •	M 01		M 06	A 01		A 05	A 11 •	D 02	
	Insecure default configuration	Ic	Spi		Sjb	Ndo		Nsm	Ich	Cio	
		Insecure connectivity	Susceptibility to prompt injections		Susceptibility to jailbreak attacks	Non-deterministic outputs handling		No security metrics/logging & monitoring events	Insecure credentials handling	Confidential information oversharing	
P 03 •	Oei	I 02	M 02	M 07	A 02		A 06	A 12	D 03 •		
	Overexposed interfaces	Pm	Me	Nvc	Mir		Pgc	Msd	Oa		
		Permission mismatch (between components)	Model extraction	No change/version control	Missing incident response plans		Poor guardrails configuration	Missing secure defaults for AI services	Overprivileged access		
P 04 •	Its	I 03 •	M 03	M 08	A 03		A 07	A 13	D 04 •		
	Insufficient tenant segregation	Utp	Pd	Lt	Hcd		Urc	Ntm	It		
		Untrusted 3rd party components	Purpose drift/erroneous behaviour	Low transparency/lack of a model card	High cost of defense tools		Unlimited resource consumption	No or limited threat modeling	Insecure transit		
P 05	Mlm	I 04	M 04	M 09	M 11		A 08	A 14 •	D 05		
	Missing logging & monitoring	Ase	Oe	Mdp	Or		Lat	Kv	Mm		
		Attack surface extension	Overexposure	Missing decommissioning process	Overreliance		Lack of adv. testing/robustness tests	SBOM/libraries with known vulnerabilities	Manual modification/missing integrity checks		
P 06	Mt	I 05 •	M 05	M 10	M 12		A 09	A 15	D 06		
	Missing responsible AI tooling	Las	Id	Uls	Oos		Nta	Aus	Ldq		
		Legacy apps/protocols support	Insecure deployment	Unfair localisation support & low performance	Use for out-of-scope cases		No test adoption to new threats & non-deterministic results	No verification/adversarial user stories	Low data quality for training & evaluation		
P 07	Ip	P 08 •	M 10	M 12	M 12		A 09	A 15	D 07 •		
	Insecure ML/AIOps practices	Loc	Id	Uls	Oos		Nta	Aus	Is		
		Lack of change control	Insecure deployment	Unfair localisation support & low performance	Use for out-of-scope cases		No test adoption to new threats & non-deterministic results	No verification/adversarial user stories	Insecure storage		
People		Low AI literacy		Lack of AI risk knowledge	Lack of cross-functional collaboration	Lack of AI learning opportunities	Limited cybersecurity awareness	Lack of knowledge sharing	Inability to make informed decisions		
Processes		ineffective AI governance		Missing organisational roles & responsibilities for AI	Non-transparent AI risk assessment & management	Effort duplication	Low data governance maturity	No adaptation to emerging risks	Lack of R&D support		

Threats

The Washington Post
Democracy Dies in Darkness

National

Elon Musk's DOGE is feeding sensitive federal data into AI to target cuts

At the Education Department, the tech billionaire's team has turned to artificial intelligence to hunt for potential spending cuts — part of a broader plan to deploy the technology across the federal government.

Updated February 6, 2025

🕒 6 min 🔖 📌 🗨️ 1400

[The Washington Post](#)

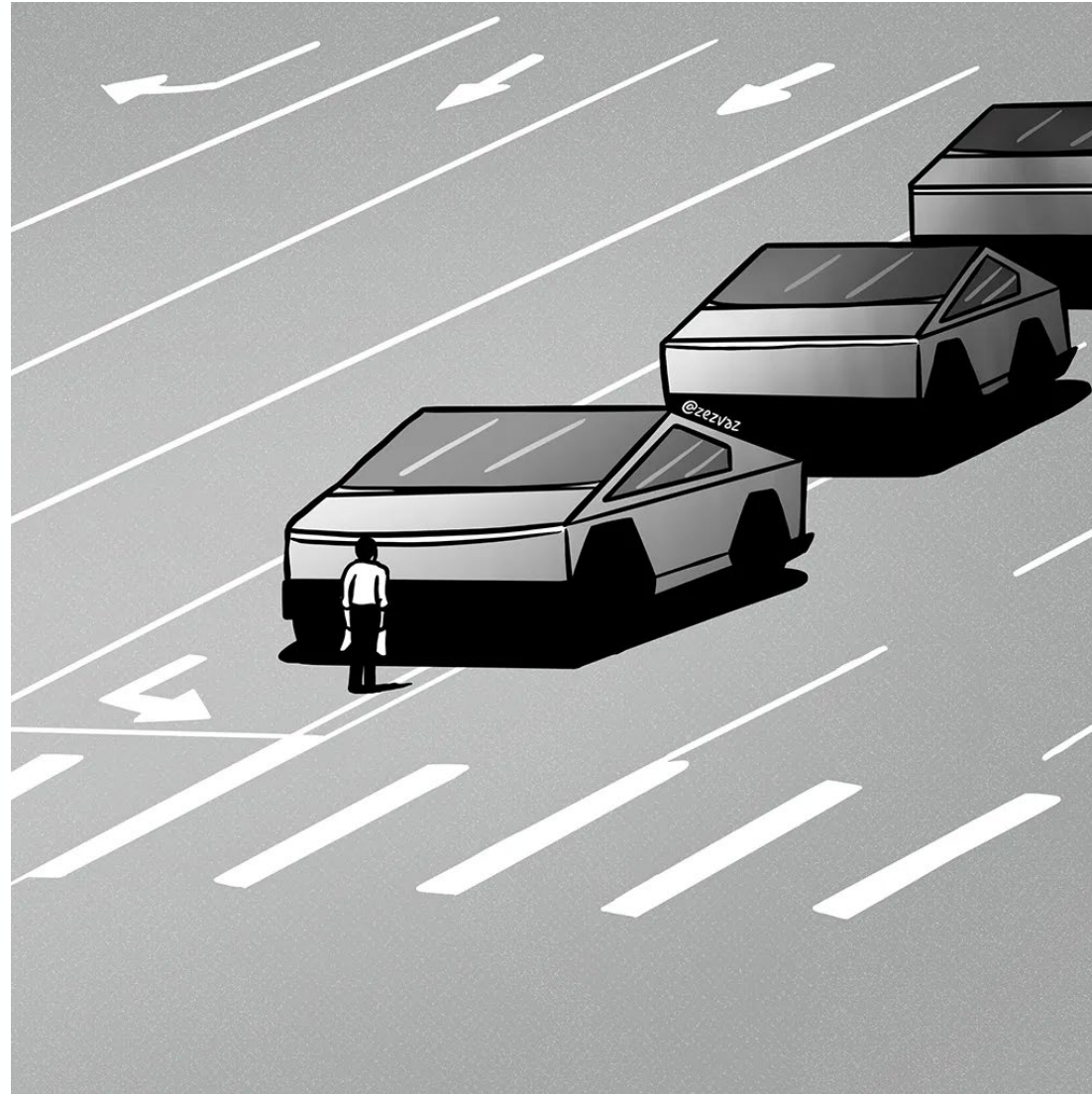
Cyber-Intelligence Brief

Over the past month, an unprecedented number of critical government systems, including those at the nation's nuclear research labs, have been exposed to the open internet. This exposure jeopardizes both U.S. national security and the privacy of millions of Americans.

Notably, this alarming trend seems to coincide with DOGE's unrestricted access to federal networks.

[Cyber Intelligence Brief](#)

Threats



[©2025 Zez Vaz](#)

tl;dr

[too long, didn't read]

Conclusion from a Swiss Perspective

- The ratification of the **CoE AI Convention** is only a **first step**
- There is **need for regulation**, in particular regarding product safety laws. Hoping for an inclusion into the **MRA CH-EU** is overly optimistic
- Switzerland should **adopt general provisions** on prohibited AI, transparency and accountability as quickly as possible to ensure human-centric trustworthy AI
- **EU AI Act does not apply in Switzerland**
- **Switzerland will not adopt the AI Act**
- If Swiss providers play a part in the AI value chain they need to comply with the EU AI Act (**extraterritorial effect**)
- Compliance according to **norms and harmonized standards** is recommended

ariolilaw

Hornbachstrasse 22

8008 Zürich

+41 44 201 66 11

martina.arioli@arioli-law.ch

