PRIVACY & LAW

FS 2025

Introduction in the

AIA

(EU AI-Act)

TIME TABLE

- The Swiss AI law…
- The EU AI Act (AIA)
- Definitions of the AIA
- Provider & Deployer
- Forbidden Practices
- High-Risk-AI-Systems (HRAIS) and duties
- Controlling and Penalties
- AI-Tools in Switzerland
- 4 Examples
- My TakeAway

The Swiss AI-law… (1)

- For solely in Switzerland used AI-systems is (upon the EDÖB) the Swiss DSG sufficient. Thus the AI-provider (e.g. employer, vendor etc.) has to follow the known principles (Art. 6 DSG):
  - Inform transparently the user about the aim, the function and the recipient
  - Has to get the user's explicit consent if particularly protected personal data are processed
  - Has to respect that the user can refuse such processing
  - Has to adequately protect systems with a high risks for the users (with risk assessment, adequate risk-measures, TOMs etc.)

The Swiss AI-law… (2)

- Upon the latest statement (12.02.25) of the Federal Council he wants to adapt the AI-rules of the Europe Convention
- „Where legislative changes are needed, they should be as sector-specific as possible. Only key areas relevant to fundamental rights, such as data protection, will be subject to general, cross-sectoral regulation."
- On 20 March 2020, National Councillor Nadine Masshardt called on the Federal Council to set up a national ethics committee for artificial intelligence. The Federal Council replied on 21.05.25 (actually not).
- What to do actually? Concentrate on the Swiss Personal Data Protection Rules!
- **But: Consider Art. 2 EU AIA (AI-Act)…**

Possible Swiss Use-Cases

- **Web chatbot** of a CH e-shop → EU consumers → deployer duties + possibly provider duties (Marketplace Principle)
- **Hosting in an EU data center** may qualify as „putting into service in the EU” (Art. 11 no. 11 AIA)
- **Group AI service hub** outside the EU → hand-over to EU affiliate ⇒ importer/distributor duties!

Do you recognise the similarities with the GDPR?

The EU AI-Act (AIA)

- Came after long discussions on 1 August 2024 in force. Staggered introduction - some rules do not have to be implemented until 1 August 2027!
- „Brussels Effect": the European marked has about 450 million people. The USA about 330 million people… Thus also the US Tech-Bro's have to accept the AIA. Or have to pay even more fines.

Article 2 AIA – Extraterritorial jurisdiction/effect

„1. This Regulation applies to:

*(a) providers **placing on the market or putting into service AI systems** or **placing on the market general-purpose AI models in the Union**, irrespective of whether those providers are established or located within the Union or in a third country;*

(b) deployers of AI systems that have their place of establishment or are located within the Union;

*(c) providers and deployers of AI systems that have their place of establishment or are located in a third country, **where the output produced by the AI system is used in the Union**;*

(d) importers and distributors of AI systems;

*(e) product manufacturers **placing on the market or putting into service an AI system together with their product** and under their own name or trademark;*

(f) authorised representatives of providers, which are not established in the Union;

*(g) **affected persons that are located in the Union**"*

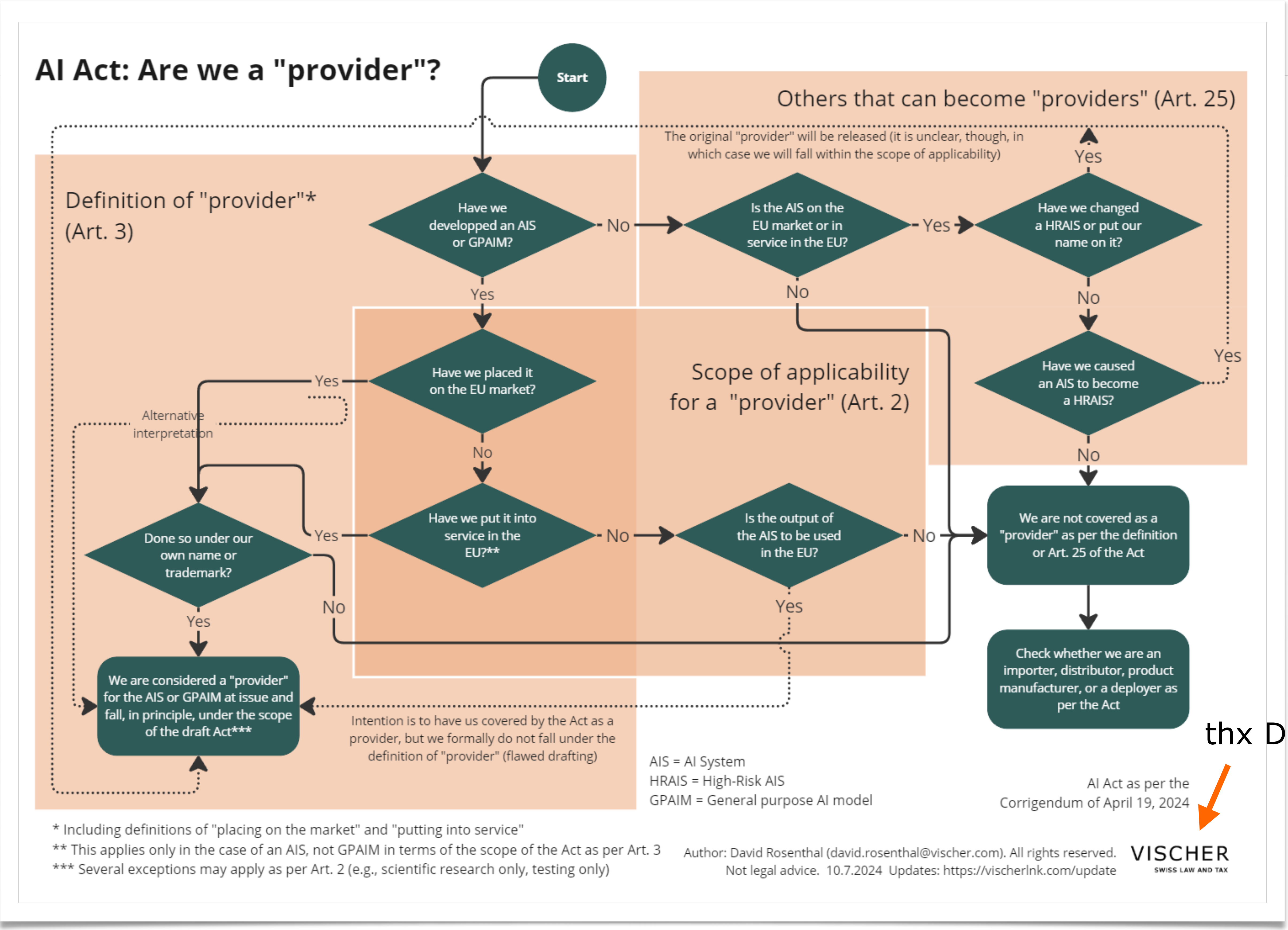
Definitions of AI-systems…

- AI **Systems** („AIS", Art. 3 no. 1 AIA) -> **Applications** with specific AI-functionality, also integrating one of the various AI-models (example: ChatGPT/Gemini/CoPilot/Perplexity etc.). Very open formulated and highly discussed. Possible solution: the OECD-definition: *„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."*
- General Purpose AI **Models** („GPAIM", Art. 3 no. 63 AIA) -> MODELS of generative AI's with at least one Billion parameters (consideration no. 98). The developer of such models must have a strategic to comply with the EU Copyright law… BUT: if it's a FOSS = „free open source software" (Art. 53 (2) AIA, the Rules for GPAIM shall not be applicable…
- *„General-Purpose AI **System**' means an AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems;"* (Art. 3 no 66 AIA)

Definitions & different Roles (Art. 3 AIA)

- **Provider** (Art. 3 no. 3, „Anbieter"): develops or first places/puts an AIS into service in the EU. Implementing of AIS in a new product and selling it in the EU (Art. 2 (1), lit. e AIA)
- **Deployer** (Art. 3 no. 4, „Betreiber"): operates AIS-system "under its authority" in a company. Example: Customer chatbot on a website

Implication:
Every company has to evaluate for every AIS or GPAIM which role it has! Most duties have the providers. Most companies that use AI-tools professionally are „Deployers"



AI Act: Are we a "provider"?

Start
Others that can become "providers" (Art. 25)
The original "provider" will be released (it is unclear, though, in which case we will fall within the scope of applicability)
Definition of "provider"* (Art. 3)
Have we developped an AIS or GPAIM?
No
Is the AIS on the EU market or in service in the EU?
Yes
Have we changed a HRAIS or put our name on it?
Yes
No
Yes
No
Have we caused an AIS to become a HRAIS?
Yes
No
Have we placed it on the EU market?
Yes
Alternative interpretation
Scope of applicability for a "provider" (Art. 2)
No
Have we put it into service in the EU?**
Yes
No
Is the output of the AIS to be used in the EU?
No
Yes
Done so under our own name or trademark?
No
Yes
We are not covered as a "provider" as per the definition or Art. 25 of the Act
Check whether we are an importer, distributor, product manufacturer, or a deployer as per the Act
We are considered a "provider" for the AIS or GPAIM at issue and fall, in principle, under the scope of the draft Act***
Intention is to have us covered by the Act as a provider, but we formally do not fall under the definition of "provider" (flawed drafting)

AIS = AI System
HRAIS = High-Risk AIS
GPAIM = General purpose AI model

AI Act as per the
Corrigendum of April 19, 2024

* Including definitions of "placing on the market" and "putting into service"
** This applies only in the case of an AIS, not GPAIM in terms of the scope of the Act as per Art. 3
*** Several exceptions may apply as per Art. 2 (e.g., scientific research only, testing only)

Author: David Rosenthal (david.rosenthal@vischer.com). All rights reserved.
Not legal advice. 10.7.2024 Updates: https://vischerlnk.com/update

VISCHER
SWISS LAW AND TAX

thx David!

Eight forbidden AI practices (Art. 5 AIA) (1)

1. Use of **subliminal**, **deliberately manipulative** or **deceptive techniques** that aim to or result in significantly distorting behaviour or impairing the person's ability to make an informed decision, if this could lead to a decision that is likely to cause or could cause significant harm.

2. **Exploiting the vulnerabilities or vulnerability of persons** due to their age, disability or particular social or economic situation in order to significantly alter their behaviour in a manner that is likely to cause or be likely to cause substantial harm.

3. **Biometric categorisation** to draw conclusions about a person's race, political opinion, trade union membership, religious or philosophical beliefs, sex life or sexual orientation (i.e. based on biometric data).

4. **Evaluation or categorisation of persons** (individually or in groups) over a period of time based on their **social behaviour** or known, inferred or **predicted personal characteristics**, if this social evaluation results in adverse or unfavourable treatment that is unrelated to the original context of the data or is unjustified or **disproportionate in relation to their social behaviour or its significance**.

Eight forbidden AI practices (Art. 5 AIA) (2)

5. **Remote and real-time biometric identification in publicly accessible spaces for law enforcement purposes**, with the exception of targeted searches for victims of certain crimes, the prevention of certain specific threats in the event of a serious and imminent threat, or the localisation or identification of suspects of certain defined categories of offences (Annex II), subject to additional conditions (e.g. judicial authorisation, permission only for the search for specific target persons).

6. Creating profiles or assessing personality traits or characteristics of individuals **to assess or predict the risk of committing offences**, except to support the risk assessment of individuals involved in an offence.

7. **Building or expanding a facial recognition database** based on non-targeted scraping on the internet or CCTV footage (i.e. surveillance cameras).

8. **Drawing conclusions about the emotions (including intentions)** of individuals in the workplace or in educational institutions, unless this is for medical or safety reasons.

High-Risk-AI-Systems (HRAIS, Art. 6 (1) AIA)

- Systems that are mentioned in Annex 3 of the AIA… Topics without the details:

1. Biometric identification and categorisation of natural persons
2. Management and operation of critical infrastructure
3. Education and vocational training
4. Employment, workers management and access to self-employment
5. Access to and enjoyment of essential private services and public services and benefits
6. Law enforcement
7. Migration, asylum and border control management
8. Administration of justice and democratic processes

Duties for Providers of a HRAIS (Art. 9 – 22 AIA)

- Establish, implement, document and maintain a **Risk management syste**m (Art. 9 AIA)
- **Strict Data & data governance** (Art. 10 AIA)
- **Technical documentation** before that system is planned on the market (Art. 11 AIA)
- **Record-keeping (logs)** over the lifetime of the system (!) (Art. 12 AIA)
- **Transparency** and provision of information to deployers (Art. 13 AIA)
- Human oversight in a way that the HRAIS c**an be effectively overseen by natural persons** during the period in which they are in use = human control (Art. 14 AIA)
- **Accuracy, robustness and cybersecurity** - HRAIS shall be designed & developed in such a way that they achieve an appropriate level of (Art. 15 AIA)
- **Duties to document** the above mentioned tasks (Art. 16 & 18 AIA)
- **Quality management system** (Art. 17 AIA)
- **Automatically generated logs** (Art. 19 AIA)
- **Corrective actions and duty of information** (Art. 20 AIA)
- **Cooperation** with competent authorities (Art. 21 AIA)
- **Authorised representatives** of providers of HRAIS (Art. 22 AIA)
- **AND: registration in the EU database for HRAIS!! (Art. 71 AIA)**

Duties for Deployers of a HRAIS (Art. 26 AIA)

- Take appropriate technical & organisational measures (Art. 26 (1) AIA)
- Human oversight (Art. 26 (2) AIA)
- Monitoring the operation of the HRAIS on the basis of the instructions for use (Art. 26 (5) AIA)
- Automated logging and keep them for at least 6 month (Art. 26 (6) AIA)
- Information duties for using HRAIS on a work place (Art. 26 (7) and (11) AIA)

It's complicated… Support from the European AI Office (Art. 64 AIA) and…

- The AI Office supports the implementation of the AIA with guidelines, Code of Practice, tools and controls.
- Private organisations as future of life institute or datenrecht.ch or VISCHER AG (mainly David Rosenthal)

Controlling (Art. 74 AIA) and Penalties (Art. 99 AIA)

- The EU and the EU-members establish organs (similar the GDPR) to control the marked
- *„Non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to* ***EUR 35 000 000*** *or, if the offender is an undertaking,* ***up to 7 % of its total worldwide annual turnover*** *for the preceding financial year, whichever is higher."* (Art. 99 (3) AIA)
- Further fines stated in Art. 99 (4) AIA
- *„1. The Commission may impose on providers of general-purpose AI models fines not exceeding 3 % of their annual total worldwide turnover in the preceding financial year or EUR 15 000 000, whichever is higher., when the Commission finds that the provider intentionally or negligently…"* (Art. 101 (1) AIA)
- Actually no AIA-sentences are known.

Finally - using AI-tools in Switzerland

- Using ChatGPT etc. (AIS) in a business context: no secret or personal data as long as the AIS is not running locally!
- Using AIS as part of a „product“? Risk-assessment! Also to comply with the personal data protection laws!
- Carefull assess if we are Provider or Deployer! As Provider we have more duties!

Examples:

- ***AlpineVision*** *AG* (Zurich) trains its own diffusion model, hosts the API in a Swiss data centre and markets the service on a subscription basis to designers in Germany and France.
- ***Clinique du Léman SA*** buys a CE-marked AI software for melanoma detection from an Italian manufacturer (already AIA-compliant) and runs it on local workstations for Swiss and EU cross-border patients.
- ***HelvetiaBank AG*** fine-tunes the open-source model *Llama 3-8B* with proprietary data to power a customer-service chatbot that will be rolled out in its Luxembourg branch. The fine-tuned weights are hosted on a Luxembourg cloud VM.
- ***PromoBoost GmbH*** builds a SaaS dashboard that calls an EU vendor's text-generation API via SDK. PromoBoost adds business logic but **does not access or alter the model weights**. The SaaS targets SMEs worldwide; some EU customers sign up indirectly.

My Take Away?

- ...
- ...
- ...
- ...
- ...