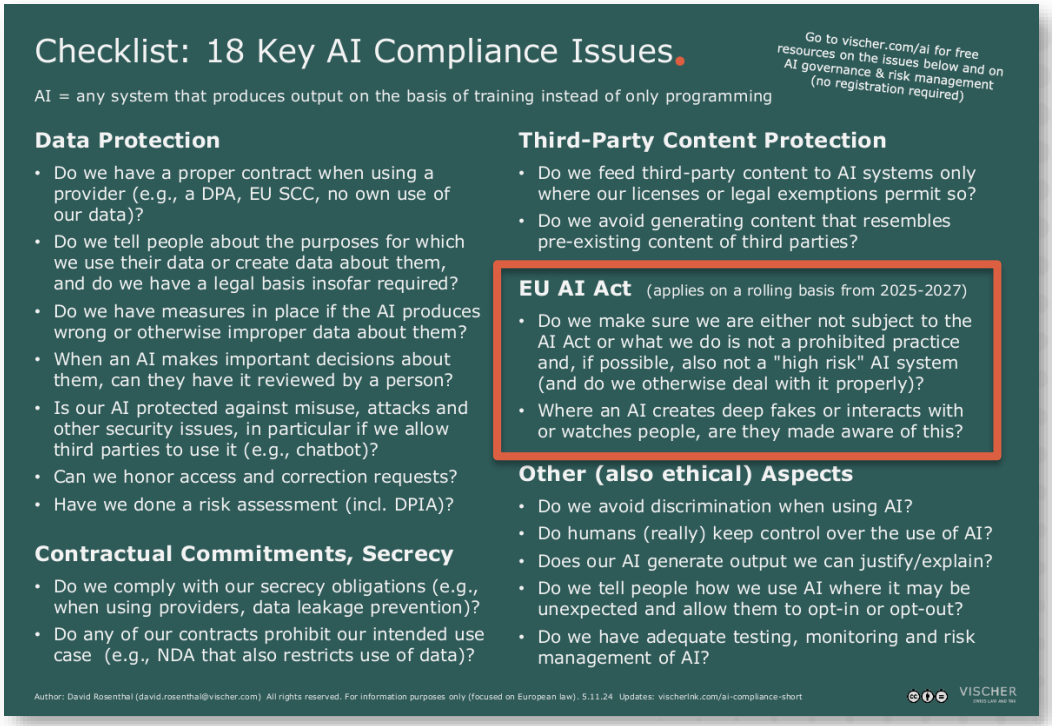
VISCHER

EU AI Act and its impact on Switzerland.

Practical thoughts and recommendations

David Rosenthal, VISCHER AG
March 7, 2025

Legal AI topics – the context



Checklist: 18 Key AI Compliance Issues.

Go to vischer.com/ai for free resources on the issues below and on AI governance & risk management (no registration required)

AI = any system that produces output on the basis of training instead of only programming

Data Protection

- Do we have a proper contract when using a provider (e.g., a DPA, EU SCC, no own use of our data)?
- Do we tell people about the purposes for which we use their data or create data about them, and do we have a legal basis insofar required?
- Do we have measures in place if the AI produces wrong or otherwise improper data about them?
- When an AI makes important decisions about them, can they have it reviewed by a person?
- Is our AI protected against misuse, attacks and other security issues, in particular if we allow third parties to use it (e.g., chatbot)?
- Can we honor access and correction requests?
- Have we done a risk assessment (incl. DPIA)?

Contractual Commitments, Secrecy

- Do we comply with our secrecy obligations (e.g., when using providers, data leakage prevention)?
- Do any of our contracts prohibit our intended use case (e.g., NDA that also restricts use of data)?

Third-Party Content Protection

- Do we feed third-party content to AI systems only where our licenses or legal exemptions permit so?
- Do we avoid generating content that resembles pre-existing content of third parties?

EU AI Act (applies on a rolling basis from 2025-2027)

- Do we make sure we are either not subject to the AI Act or what we do is not a prohibited practice and, if possible, also not a "high risk" AI system (and do we otherwise deal with it properly)?
- Where an AI creates deep fakes or interacts with or watches people, are they made aware of this?

Other (also ethical) Aspects

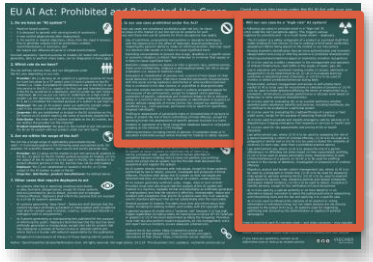
- Do we avoid discrimination when using AI?
- Do humans (really) keep control over the use of AI?
- Does our AI generate output we can justify/explain?
- Do we tell people how we use AI where it may be unexpected and allow them to opt-in or opt-out?
- Do we have adequate testing, monitoring and risk management of AI?

AI Act only one topic of several

vischerlnk.com/ai-compliance-short

AI Act: What it's all about

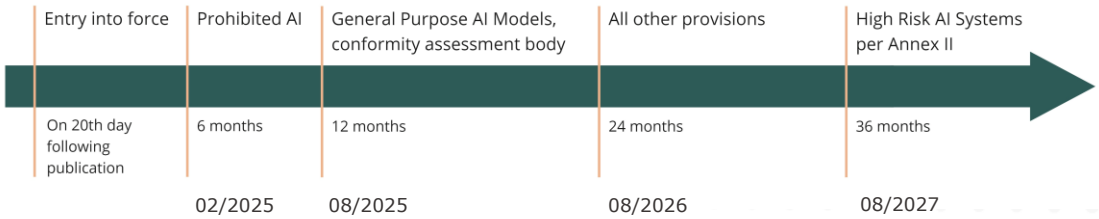
- No general regulation of the use of AI
- Instead: **Product regulation** with a focus on safety
  - Prohibited AI practices
  - Rules for "high-risk" AI systems, general-purpose AI models
  - Individual (transparency) requirements for other AI systems
- **Supplements** existing law (GDPR, DSA, contract law, etc.)



vischerlnk.com/ai-act-uc

Text: vischerlnk.com/ai-act

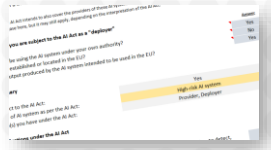
Timeline EU AI Act



AI Act: To whom it applies

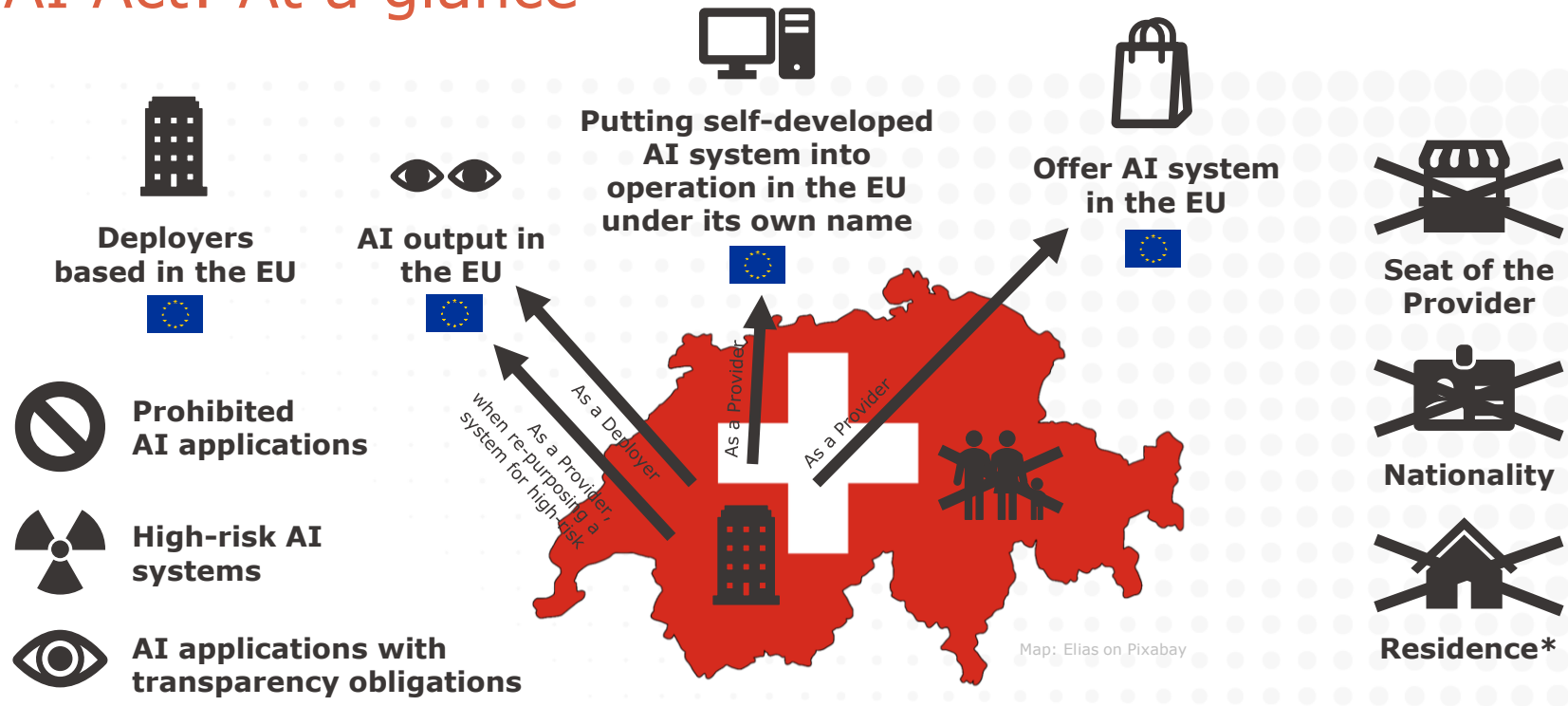
Detailed essay on the EU AI Act:
vischerlnk.com/3ZkPOYh

- **Deployer:** "using an AI system under its authority"
  - If established in the EU *or*
  - If AI output is used in the EU (as intended)
- **Provider:** "develops an AI system ... and places them on the [EU] market or puts the system into service [in the EU] under its own name or trademark"
  - Joint development? Engage provider + "powered by..."
  - Also who re-purposes a system for a high risk use case (Art. 25)
- **Other roles:** Importer, Distributor, Product Manufacturer, EU representative



See AI Act Check at
vischerlnk.com/gaira

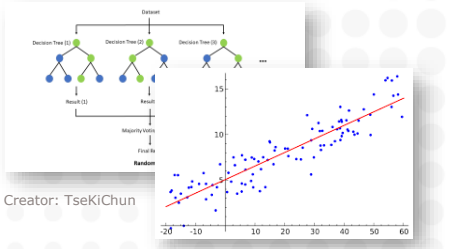
AI Act: At a glance



* Place of a person is relevant for the assertion of rights

AI Act: What is "AI", after all?

- They have **no clear** understanding of what AI is
  - Is it a copying machine since OCR is based on a neural network?
- As per the EU **AI Act** "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and 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"
  - The only practically relevant element is **"autonomy"**
  - In simple terms: An IT system that has been **trained** on how to decide, not only using programmed logic …
  - But to which applications in your company does this apply?



Creator: TseKiChun

AI Act: Prohibited practices – private sector view

- **Some use cases**
  - AI subliminally, deliberately manipulating or deceiving a person to significantly influence their behaviour (so that they can no longer make correct decisions) or to exploit the weaknesses of vulnerable people, which can lead to significant harm to them
  - AI to categorise people according to their race, political, religious or secular views, sexual orientation or sex life based on biometric characteristics
  - Social scoring or profiling using AI leads to unfavourable treatment in areas that have nothing to do with the data used or that is unjustified or disproportionate
  - AI to predict whether a person will commit an offence, with exceptions
  - Emotion recognition in the workplace/in educational institutions

→ Common and legitimate practices, e.g. in the area of advertising, which comply with the law, should not be covered

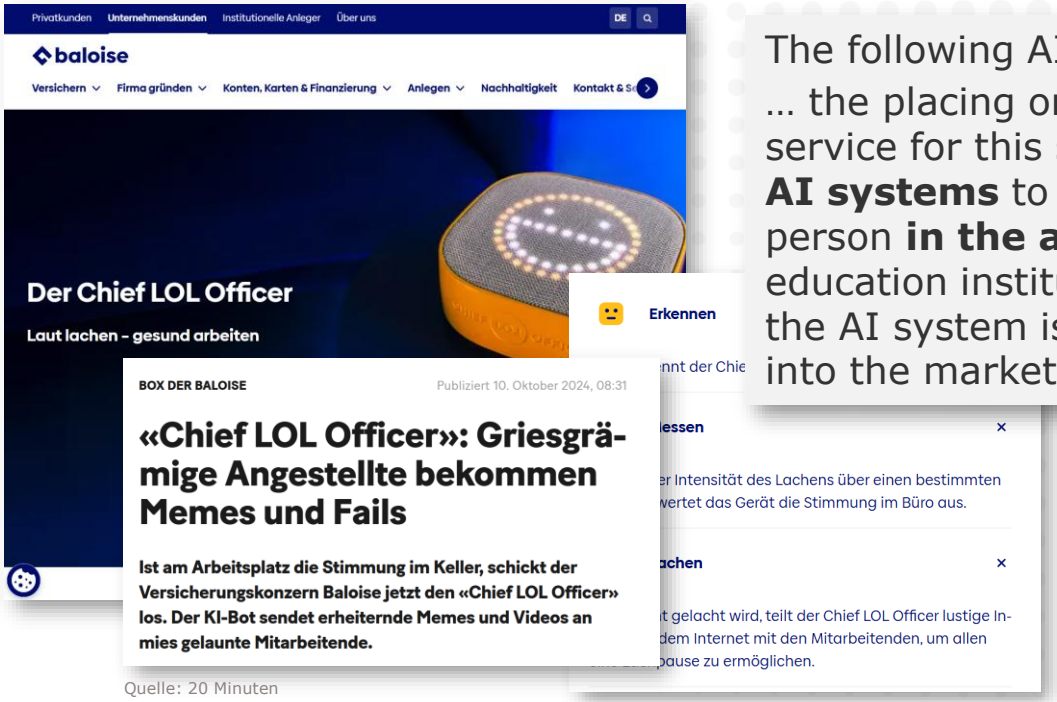
→ This is about correlating race or "inner" aspects with external appearance

→ Use of data for "a specific purpose" not in scope?

→ Not e.g. fraud analysis of transactions, AML or DLP

→ Not where used only for safety or health purposes or not based on biometrics

Example: Chief LOL Officer



Quelle: 20 Minuten

The following AI practices shall be **prohibited**:

… the placing on the market, the putting into service for this specific purpose, or the **use of AI systems** to **infer emotions** of a natural person **in the areas of workplace** and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

The people responsible for legal reviewing new apps apparently knew nothing about it …

AI Act: High-risk AI systems – private sector view

- **Safety components** of **products** that already today require conformity assessments by third parties (according to a list)
  - E.g. medical devices, toys, radios, elevators
- List of **further AI use cases** (only some are private sector)
  - Biometric emotion recognition, categorisation, remote ident.
  - A safety component for (certain) critical infrastructure
  - For assessments in the educational sector
  - For assessments of applicants and employees or decisions concerning them in detail (e.g. allocation of tasks, pot. DLP)
  - To manage access to key public services and healthcare or emergency services
  - For assessing creditworthiness or pricing re some insurances

Biometric authentication is not covered

E.g., sentiment analysis based on voice, but not based on text

E.g., an image search feature that relies on face recognition, but not on metadata

But not the "Robo-Doc" → medical device

AI Act: Most important obligations

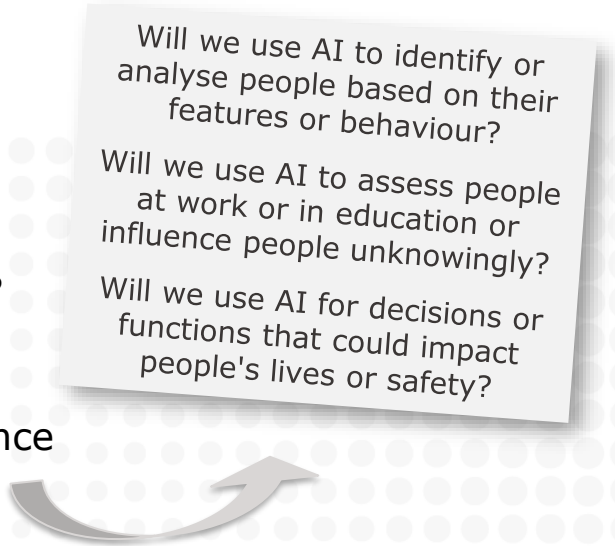
No general rules on how to use AI apart from the obligation to promote "AI literacy"

- Obligations for **high-risk AI systems** (selection)
  - **Provider:** Risk and quality management, data quality, conformity assessments, registration, EU representative, instructions, documentation, incident monitoring incl. reporting obligations
  - **Deployer:** Compliance with instructions, suitable input, human monitoring, reporting obligations, transparency, assessing impact
- Obligations for **other AI systems**
  - **Provider:** Reference to interaction with AI, watermarking
  - **Deployer:** Notice about biometric emotion recognition, deep fakes and AI-generated and automatically published content of public interest must be recognisable as such
- Further rules exist for **general-purpose AI models**

Check each use case to determine the role of the organisation and whether it is within the scope of the AI Act

AI Act: How to prepare yourself

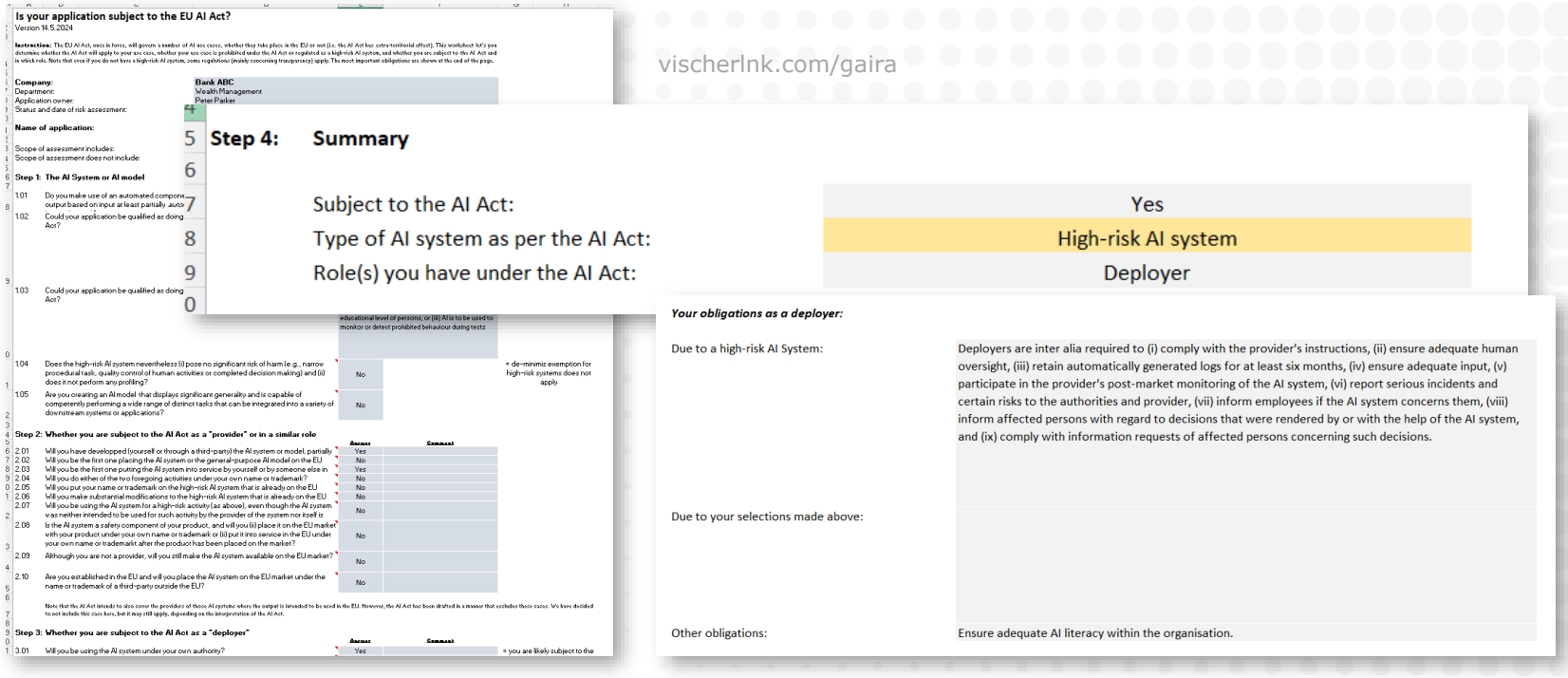
- Create an **inventory** of your AI applications
  - Do not only list tools but also use cases
  - Do you have adequate policies and accountabilities?
- Assess whether the use cases are **"in scope"**
  - Both from a geographical point of view or in substance
  - If they are "high risk", can you avoid this?
- If so, assess which **role(s)** you will have
  - If you are a "provider", can you avoid this?
  - Check out the steps necessary for implementation
- Have your (AI) **supplier contracts** checked/amended



VISCHER

AI Act Checker (free, open source)

vischerlnk.com/gaira



Is your application subject to the EU AI Act?

Version 14.5.2024

Instruction: The EU AI Act, once in force, will govern a number of AI use cases, whether they take place in the EU or not (i.e. the AI Act has extra-territorial effect). This worksheet let's you determine whether the AI Act will apply to your use case, whether your use case is prohibited under the AI Act or regulated as a high-risk AI system, and whether you are subject to the AI Act and in which role. Note that even if you do not have a high-risk AI system, some regulations (mainly concerning transparency) apply. The most important obligations are shown at the end of the page.

Company:	**Bank ABC**
Department:	Wealth Management
Application owner:	Peter Parker
Status and date of risk assessment:	
Name of application:	
Scope of assessment includes:	
Scope of assessment does not include:	

Step 1: The AI System or AI model

1.01	Do you make use of an automated component that generates predictions, recommendations, decisions or other output based on input at least partially autonomously?		
1.02	Could your application be qualified as doing Art?		
1.03	Could your application be qualified as doing Act?		
			educational level of persons, or (iii) AI is to be used to monitor or detect prohibited behaviour during tests
1.04	Does the high-risk AI system nevertheless (i) pose no significant risk of harm (e.g., narrow procedural task, quality control of human activities or completed decision making) and (ii) does it not perform any profiling?	No	= de-minimis exemption for high-risk systems does not apply
1.05	Are you creating an AI model that displays significant generality and is capable of competently performing a wide range of distinct tasks that can be integrated into a variety of downstream systems or applications?	No	

Step 2: Whether you are subject to the AI Act as a "provider" or in a similar role

		Answer	Comment
2.01	Will you have developed (yourself or through a third-party) the AI system or model, partially	Yes	
2.02	Will you be the first one placing the AI system or the general-purpose AI model on the EU	No	
2.03	Will you be the first one putting the AI system into service by yourself or by someone else in	Yes	
2.04	Will you do either of the two foregoing activities under your own name or trademark?	No	
2.05	Will you put your name or trademark on the high-risk AI system that is already on the EU	No	
2.06	Will you make substantial modifications to the high-risk AI system that is already on the EU	No	
2.07	Will you be using the AI system for a high-risk activity (as above), even though the AI system was neither intended to be used for such activity by the provider of the system nor itself is	No	
2.08	Is the AI system a safety component of your product, and will you (i) place it on the EU market with your product under your own name or trademark or (ii) put it into service in the EU under your own name or trademark after the product has been placed on the market?	No	
2.09	Although you are not a provider, will you still make the AI system available on the EU market?	No	
2.10	Are you established in the EU and will you place the AI system on the EU market under the name or trademark of a third-party outside the EU?	No	

Note that the AI Act intends to also cover the providers of those AI systems where the output is intended to be used in the EU. However, the AI Act has been drafted in a manner that excludes those cases. We have decided to not include this case here, but it may still apply, depending on the interpretation of the AI Act.

Step 3: Whether you are subject to the AI Act as a "deployer"

		Answer	Comment	
3.01	Will you be using the AI system under your own authority?	Yes		= you are likely subject to the

Step 4: Summary

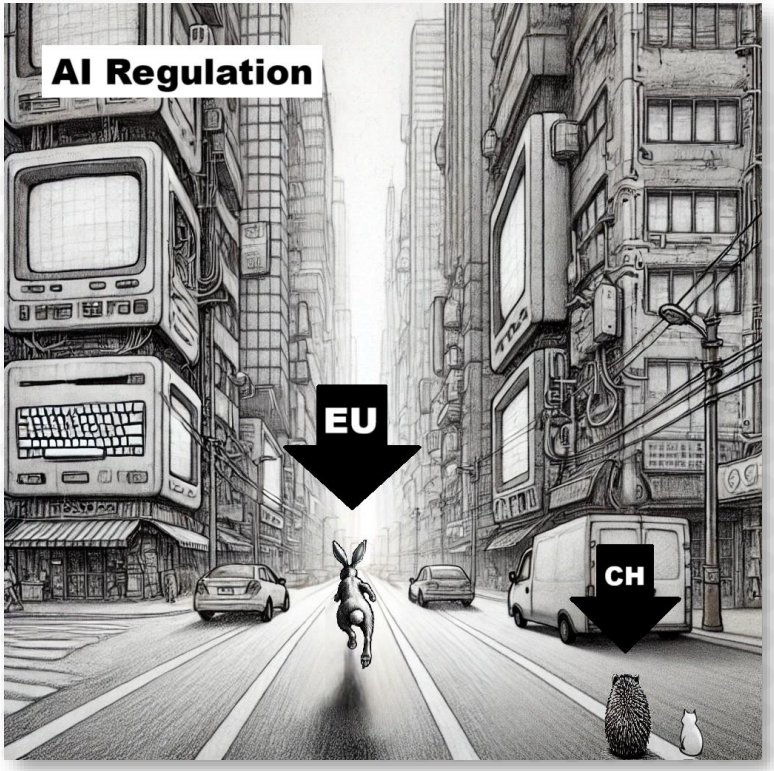
Subject to the AI Act:	Yes
Type of AI system as per the AI Act:	High-risk AI system
Role(s) you have under the AI Act:	Deployer

Your obligations as a deployer:

Due to a high-risk AI System:	Deployers are inter alia required to (i) comply with the provider's instructions, (ii) ensure adequate human oversight, (iii) retain automatically generated logs for at least six months, (iv) ensure adequate input, (v) participate in the provider's post-market monitoring of the AI system, (vi) report serious incidents and certain risks to the authorities and provider, (vii) inform employees if the AI system concerns them, (viii) inform affected persons with regard to decisions that were rendered by or with the help of the AI system, and (ix) comply with information requests of affected persons concerning such decisions.
Due to your selections made above:	
Other obligations:	Ensure adequate AI literacy within the organisation.

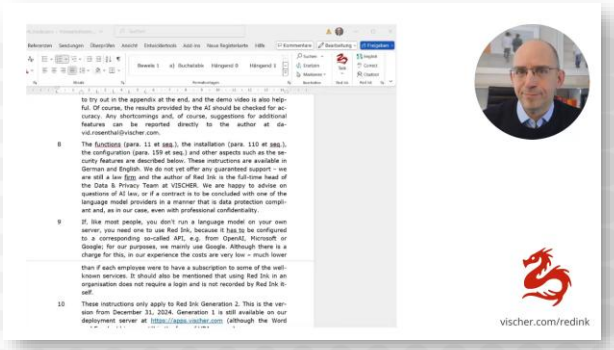
And Switzerland?

- We will not adopt the AI Act, but "only" the (much more generic) AI Convention of the Council of Europe
  - Expect small amendments of Swiss law for the public sector and where "fundamental rights" apply to the private sector (draft by end of 2026)
- Rules on semi-automated decisions
- Obligation to maintain AI inventory
- Additional transparency obligations
- Obligation to assess use cases for their impact on fundamental rights



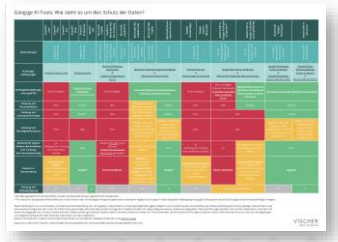
My personal recommendations

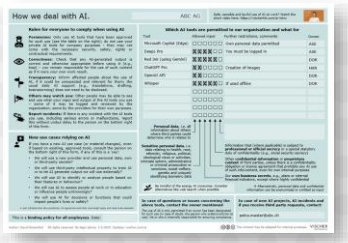
- **Allow** your people use AI in day-to-day work and give them the tools to do so
  - Have a permissive, clear policy
  - Approved tools only (check contracts and costs!)
- **Educate** your people in using AI sensibly
  - This is for most companies the best assurance to get the most out of AI and avoid big issues
- **Understand** your use of AI
  - Assess and understand risks of AI in general and key projects
  - Have an inventory of use cases



https://vischerlnk.com/redinkdemo

https://vischer.com/redink





Tool overview
Sample policy
and much more
vischer.com/ai

VISCHER

Thank you for your attention!

Questions: david.rosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com

vischerlnk.com/3ZkPOYh

More on the topic:
vischer.com/ai