

VISCHER

The EU's AI Act from a technological and regulatory perspective.

The Swiss private sector view

David Rosenthal, VISCHER AG
May 29, 2024

Legal AI issues – the context

Checklist: 18 Key AI Compliance Issues.

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

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

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?
- 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 "fair use" rules permit it?
- Do we avoid generating content that resembles pre-existing content of third parties?

EU AI Act (not yet in force)

- 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?

Author: David Rosenthal (david.rosenthal@vischer.com). All rights reserved. For information purposes only (focused on European law). 16.5.24. Updates: vischerlink.com/ai-compliance-short

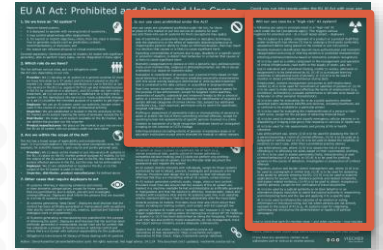


AI Act only one issue of many, and a less important one from a Swiss point of view

vischerlink.com/ai-compliance-short

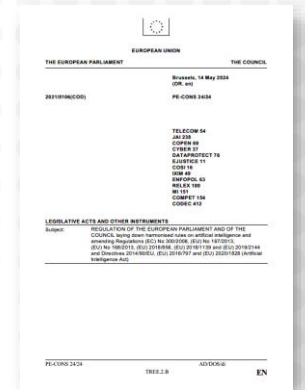
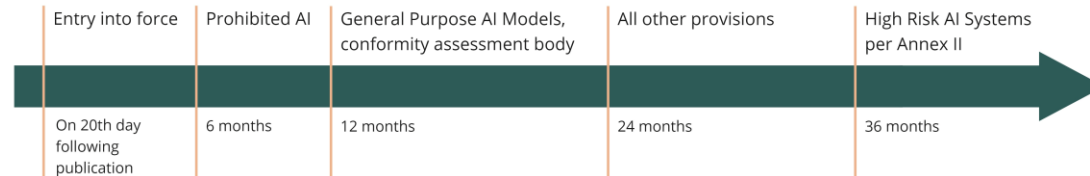
What it's all about

- 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

Timeline EU AI Act

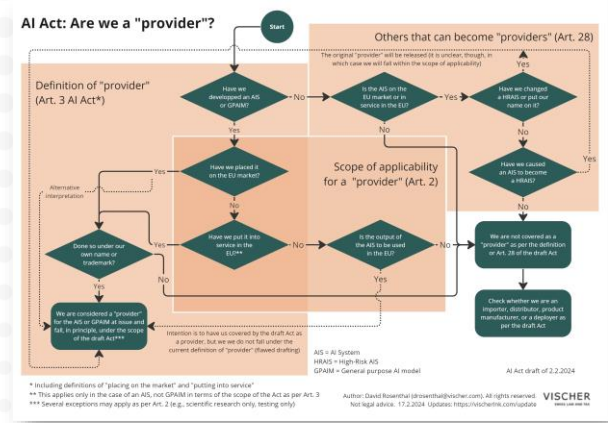
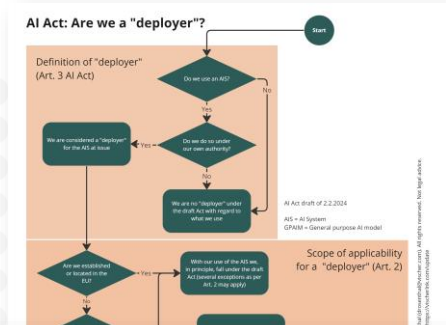


To whom it applies

trained instead of only rule based

- **AI system:** "machine-based system designed to operate with varying levels of autonomy ..."
- **Deployer:** "using an AI system under its authority"
 - If in the EU *or*
 - If AI output is used in the EU 
- **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" 
 - A deployer who makes changes to an AI system
- **Other roles:** Importer, Distributor, Product Manufacturer, EU Representative

vischerlnk.com/ai-act-uc



Various open questions remain

- **What is "developing" an AI system?**
 - Building your own model?
 - Fine-tuning an existing model?
 - Programming the orchestrator?
 - Providing information for a "Retrieval Augmented Generation"?
 - Creating a "custom GPT"?
 - Defining the system prompt?
 - Parameterizing a chatbot for the website?
 - Installing an open source LLM with a given Python script, but slightly customized?
 - Commissioning a provider to provide a chatbot for your website?

More questions

- **Passing on AI services within the group?**
 - Swiss parent company purchases an AI solution and passes it on to group companies (also) in the EU
 - Even if the product is already on the market in the EU, the parent company can be a "distributor" (there are counterarguments ...)
- **Passing on AI functionality to customers**
 - Example: A bank providing its business customers with an AI-supported analysis of their portfolios via its online access generally becomes a provider
 - The business customer who uses the AI functionality under their authority (i.e. control) usually becomes a "deployer", even if they are not even aware that AI is involved

→ BTW: FINMA requires compliance with EU AI Act, where applicable

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

→ Not where used only for safety or health purposes

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 use cases** (only some are private sector)
 - AI for biometric emotion recognition or categorisation
 - AI as a safety component for critical infrastructure
 - AI for assessments in the educational sector
 - AI for the assessment of applicants and employees or decisions concerning them in detail (e.g. allocation of tasks at work)
 - AI to manage access to key public services and healthcare or emergency services
 - AI for assessing creditworthiness and pricing re some insurances

Biometric authentication is not covered

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

But not the "Robo-Doc" → medical device

Most important obligations

- 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 obligations
- 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**

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

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

Examples of application in Switzerland

Case	Provider	Deployer
A company in Switzerland provides employees with ChatGPT or Copilot. They use it to create emails, presentations, blogs, summaries and translations and to generate images. Use also in the EU.	No	Yes
A company in Switzerland has developed its own chat tool based on an LLM and uses it internally to create emails, presentations, blog posts, summaries, translations and other texts and to generate images. It is planned that people in the EU will also receive the AI-generated content (e.g. as emails or texts on the website).	(Yes)	Yes
A company in Switzerland uses ChatGPT or Copilot to analyse documents from applicants for jobs in Switzerland for any problems. The results remain internal. The applicants also come from the EU.	No	No
A company in Switzerland provides a self-created chatbot on its website to answer general enquiries about the company. The website (with the chatbot) is also aimed at people in the EU.	Yes	Yes
A company in Switzerland uses the product or service of a third party to realise the chatbot on its website. The company's content is made available to the chatbot in the form of a database (RAG). The company does not disclose that the chatbot has been created by a third and who that third party is.	(No)	Yes
The company states on the website that the chatbot is being provided by a name third party provider.	No	Yes
A company in Switzerland uses an LLM locally to transcribe texts that are also intended for the EU. It transfers the Python script unchanged from a free template on the Internet to its own computer.	No	Yes
A company in Switzerland uses a service from a US service provider that is also offered to customers in the EU to generate avatars for training videos.	No	Yes

AI Act Checker (free, open source)

vischerlnk.com/gaira

Is your application subject to the EU AI Act?
Version 14.5.2024

Instructions: 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 lets 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 once in force, AI Act high-risk AI system, core obligations (mainly concerning transparency) apply. The most important obligations are shown at the end of this page.

Company: Bank ABC
Department: Health Management
Application owner: Peter Parker
Status and date of risk assessment: 4

Name of application: 5
Step 4: Summary

Scope of assessment includes: 6
Scope of assessment does not include: 6

Step 1: The AI System or AI model

101 Do you make use of an automated component based on input at least partially auto? 7
102 Could your application be qualified as doing AI? 7

Subject to the AI Act:
Type of AI system as per the AI Act:
Role(s) you have under the AI Act:

103 Could your application be qualified as doing AI? 0

104 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

105 Are you creating an AI model that displays significant generality and is capable of comprehensively 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

Assess	Comment
2.01 Will you have developed (yourself or through a third party) the AI system or model, partially or fully?	Yes
2.02 Will you be the first one placing the AI system or the general-purpose AI model on the EU market?	No
2.03 Will you be the first one putting the AI system into service by yourself or by someone else in the EU?	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 market?	No
2.06 Will you make substantial modifications to a high-risk AI system that is already on the EU market?	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 fixed in the AI system as 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
2.08 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: Under the AI Act, it is also your provider of those AI systems when the supplier is intended to be used in the EU. However, the AI Act has been drafted in a way 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"

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

Yes

High-risk AI system

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:

Ensure adequate AI literacy within the organisation.

Other obligations:

Ensure adequate AI literacy within the organisation.

Some final remarks

- **Many buzzwords and issues, but few real solutions**
 - Most provider obligations are either high-level or unrealistic
 - Example 1: "Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose." (from Art. 10)
 - Example 2: AI-generated text shall have watermarks to show that it has been artificially generated, but technology for effectively and reliably doing so does not exist
- **Burden for SME that wish to provide AI products**
 - The Brussels effect – AI products have to comply with the AI Act
 - Big business for audit firms ahead

VISCHER

vischerlnk.com/3TKWj2e

Thank you for your attention!

Questions: david.rosenthal@vischer.com

Zürich

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

www.vischer.com

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



More on the topic:
vischer.com/ai