VISCHER

The Legal Basis for Offering and Using AI.

What do we have, what is to come

David Rosenthal, Partner, VISCHER AG

February 11, 2025

Let's start with a reality check

- **AI** is not new
  - Any system that has also been "trained" is AI (legally speaking)
  - AI is already widely used, e.g., OCR, face-login, translation, AML
  - New: "general purpose" AI, increased capabilities and availability
- **Most laws relevant for AI** are not new, either
  - Data protection, protecting business and professional secrets
  - Copyright law
  - Contract law
  - Competition law
- Nor are **reputational issues, fear** and **uncertainty** whenever there is disruptive use of technology we are not used to …

Example: The Swiss Data Protection Act already regulates automated decision making

www.jusletter.ch

David Rosenthal / Livio Veraldi

Das Training von KI-Sprachmodellen mit fremden Inhalten und Daten aus rechtlicher Sicht

Grosse Sprachmodelle benötigen für ihr Training umfangreiches Sprachmaterial. Viel davon stammt aus dem Internet. Diese Daten können jedoch Personendaten und geistiges Eigentum Dritter enthalten. Unter welchen Voraussetzungen ist deren Nutzung für Trainingszwecke zulässig? Zur Beantwortung dieser Frage analysieren wir zunächst Zweck und Funktionsweise des Trainings grosser Sprachmodelle. Anschliessend betrachten wir die relevanten Trainingsdatenquellen aus rechtlicher Perspektive. Schliesslich erläutern wir den Umgang mit diesen Quellen nach Schweizer Urheber-, Datenschutz-, Lauterkeits- und Vertragsrecht. Wir behandeln zudem «Crawler-Verbote» und die Haftung von Anbietern.

Beitragsart: Beiträge
Rechtsgebiete: Informatik und Recht, Urheberrecht, Datenschutz, Wettbewerbsrecht

Zitiervorschlag: David Rosenthal / Livio Veraldi, Das Training von KI-Sprachmodellen mit fremden Inhalten und Daten aus rechtlicher Sicht, in: Jusletter [illegible]

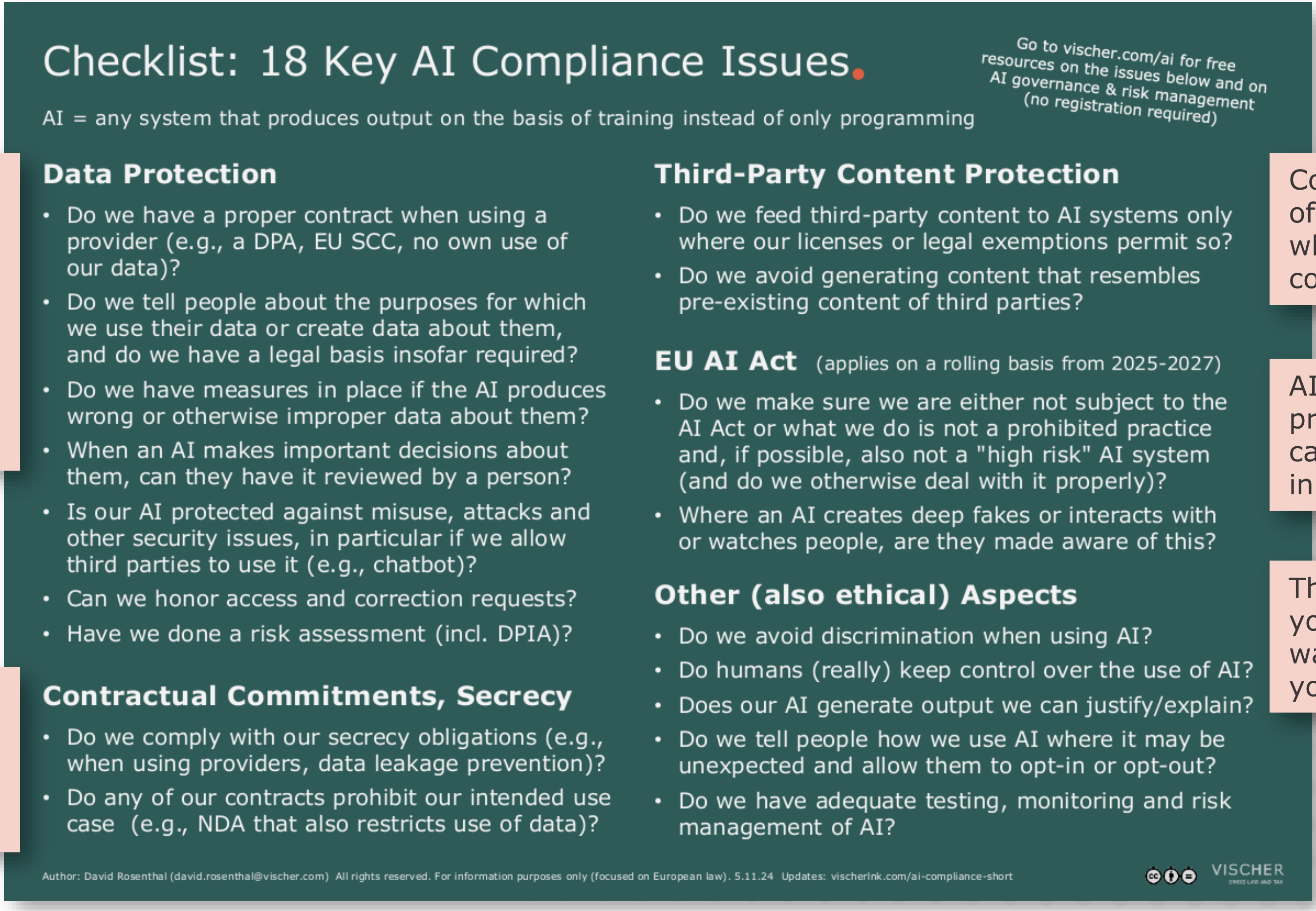
ISSN 1424-7410, [illegible], Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

https://vischerlnk.com/3WTLjlz

vischerlnk.com/ai-compliance-short

The usual stuff when dealing with personal data – make sure you keep control, in particular when using third parties

This is critical – to whom do you disclose highly confidential customer data?



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?

Author: David Rosenthal (david.rosenthal@vischer.com) All rights reserved. For information purposes only (focused on European law). 5.11.24 Updates: vischerlnk.com/ai-compliance-short

VISCHER
SWISS LAW AND TAX

Copyright is often no issue when using common sense

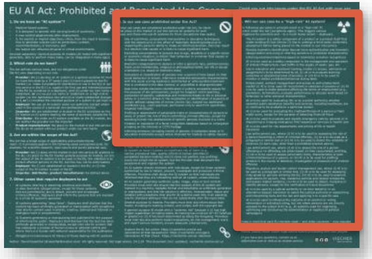
AI Act is about product safety; can also apply in Switzerland

The questions you may also want to ask yourself …

VISCHER

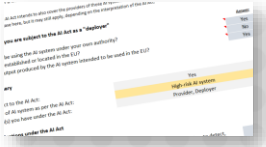
What is really new: The EU AI Act

- As a Swiss company you will be subject to the AI Act if …
  - You **develop** AI products and services for use in the EU
  - You use AI where the **output** is intended for use in the EU
  - But not if your AI **runs** in the EU or **affects** people in the EU
- Under the AI Act, you will have special restrictions if …
  - You have a **prohibited** AI use case (e.g., AI emotion recognition in the workplace, classifying certain aspects based on biometrics)
  - You have a **high-risk** AI use case (e.g., AI assessments of own employees and in education, AI creditworthiness assessments)
- Beyond that, there are very limited **transparency** obligations
  - E.g., emotion recognition, watermarking, deep fakes



EU AI Act: Prohibited a

vischerlnk.com/ai-act-uc



AI Act intends to also cover the providers of these AI syst…
are here, but it may still apply, depending on the interpretation of the AI Act.

you are subject to the AI Act as a "deployer"

be using the AI system under your own authority?
established or located in the EU?
utput produced by the AI system intended to be used in the EU?

Answer:
Yes
No
Yes

ary

ct to the AI Act:
of AI system as per the AI Act:
(s) you have under the AI Act:

Yes
High-risk AI system
Provider, Deployer

…ations under the AI Act

See AI Act Check at
vischerlnk.com/gaira

Some buzzwords …

Distinguish what is legally required and what may be good to do

- Example 1: **"Any use of AI has to be transparent"**
  - Instead: Do people have to expect that AI will be used in that way without special notice? Is it necessary for assessing risks?

→ See our blog and sample "AI Declaration" at vischerlnk.com/3KuXeiN

- Example 2: **"AI should never discriminate people."**
  - Switzerland: We have no law generally prohibiting discrimination
- Example 3: **"Any AI result should be explainable"**
  - We can explain the principle, but often not the specific results
  - Instead: Can we justify AI decisions with our own human mind?
- Example 4: **"AI should not take decisions"**
  - Instead: Oversight and responsibility needs to remain human

What we see with all sobriety …

- **Initial reaction**
  - AI needs to (and can) be regulated to get it under control
  - Using AI in an "ethical" manner is key
  - Some rush in regulating without fully understanding the effects
- **Meanwhile …**
  - We take a more nuanced view; existing law handles unwanted effects already well (→ Federal Council to provide its report)
  - "Ethical AI" has been replaced by "Responsible AI" and often downgraded to what is necessary for compliance & reputation
  - We start to understand that broad regulations such as the EU AI Act may not be as good as intended; we should rather focus on very specific areas of regulation and enforce existing laws …

TIME
THE STRANGE NEW WORLD OF THE
INTERNET
Battles on the frontiers of cyberspace

July 25, 1994 (time.com, Cover: James Porto)

Der Chief LOL Officer

Laut lachen – gesund arbeiten

deepseek

Some recommendations

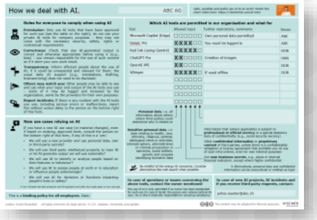
- For those **offering** AI products
  - Understand the impact of the GDPR, the EU AI Act and copyright law on your product offerings, avoid "high risk" AI Systems
  - Document your efforts in training & testing your products, know the components you rely on, and be able to answer questions
  - Have your supply chain under control
  - Be ready to take certain risks
- For those **using** AI products
  - Have proper governance for the AI stuff your staff wants to use, including an inventory and a proper risk management
  - Challenge your providers, and do your compliance homework
  - Have your staff become AI literate, including management

Check out your GenAI project for risks.

1. Is your application likely to involve high risks for the company?

2. How are you dealing with the typical risks of generative AI?

vischerlnk.com/ai-riskcheck



How we deal with AI.

ABC AG

Rules for everyone to comply when using AI

Which AI tools are permitted in our organisation and what for

vischerlnk.com/ai-policy-short

What is to come

- **Switzerland to position itself**
  - The Federal Council's report is expected tomorrow
  - My expectation: Only limited, specific changes to existing law
  - Use law to give Switzerland a competitive advantage?
- **More heavy regulation on the part of the EU**
  - Not limited to AI, but also concerning other digital topics, such as cybersecurity and online services
  - Increasing compliance costs, big business for audit firms and advisors, and the de-facto global standard
- **Supervisory authorities get active, courts start ruling**
  - Examples: FINMA, pending court decision on inventions by AI

"The Blue Wall"

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance

https://www.kaizenner.eu/post/digital-factsheet-vol-3

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

For in-depth materials on the topic visit us at vischer.com/ai

www.vischer.com