VISCHER

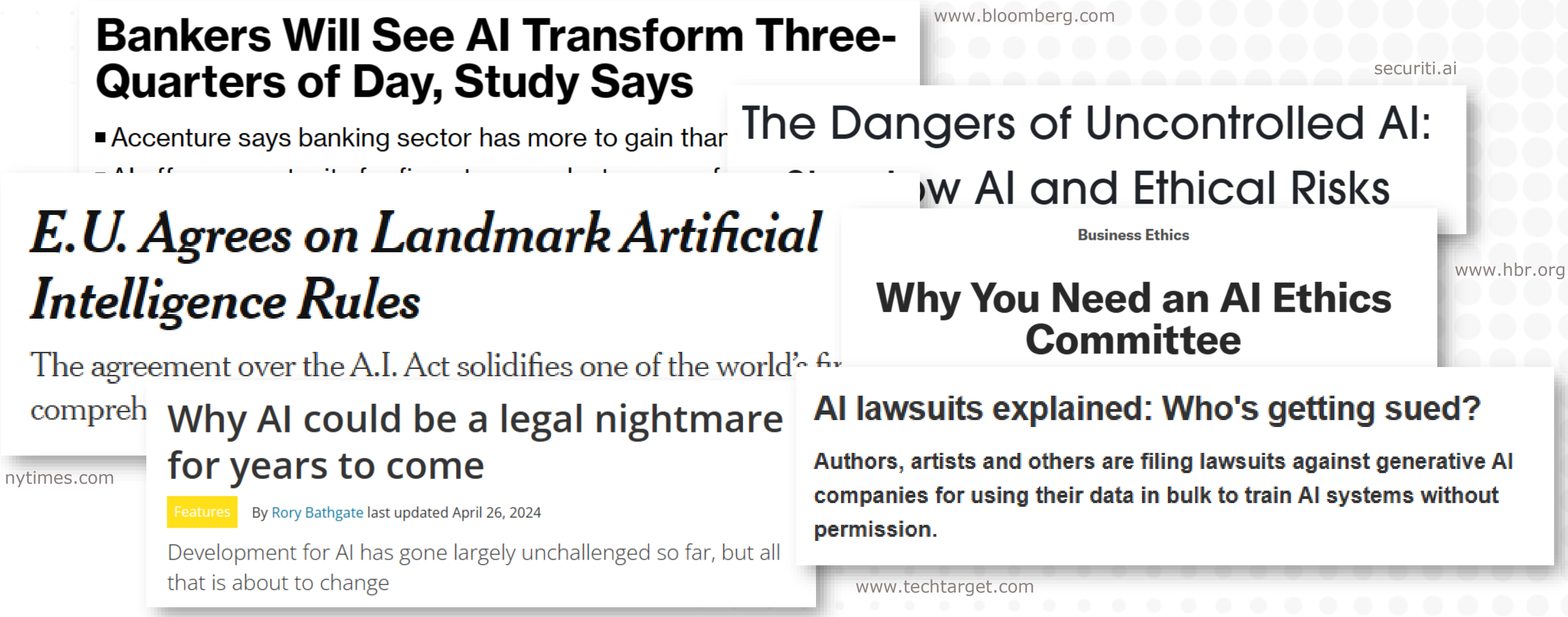
Artificial Intelligence.

How Swiss banks should deal with it from a legal and governance point of view

David Rosenthal, Partner, VISCHER Ltd.

June 6, 2024

We all know the headlines …



www.bloomberg.com

Bankers Will See AI Transform Three-Quarters of Day, Study Says

- Accenture says banking sector has more to gain thar

securiti.ai

The Dangers of Uncontrolled AI:

ow AI and Ethical Risks

E.U. Agrees on Landmark Artificial Intelligence Rules

The agreement over the A.I. Act solidifies one of the world's fi

compreh

nytimes.com

Business Ethics

Why You Need an AI Ethics Committee

www.hbr.org

Why AI could be a legal nightmare for years to come

Features By Rory Bathgate last updated April 26, 2024

Development for AI has gone largely unchallenged so far, but all that is about to change

www.itpro.com

AI lawsuits explained: Who's getting sued?

Authors, artists and others are filing lawsuits against generative AI companies for using their data in bulk to train AI systems without permission.

www.techtarget.com

Reality Check I

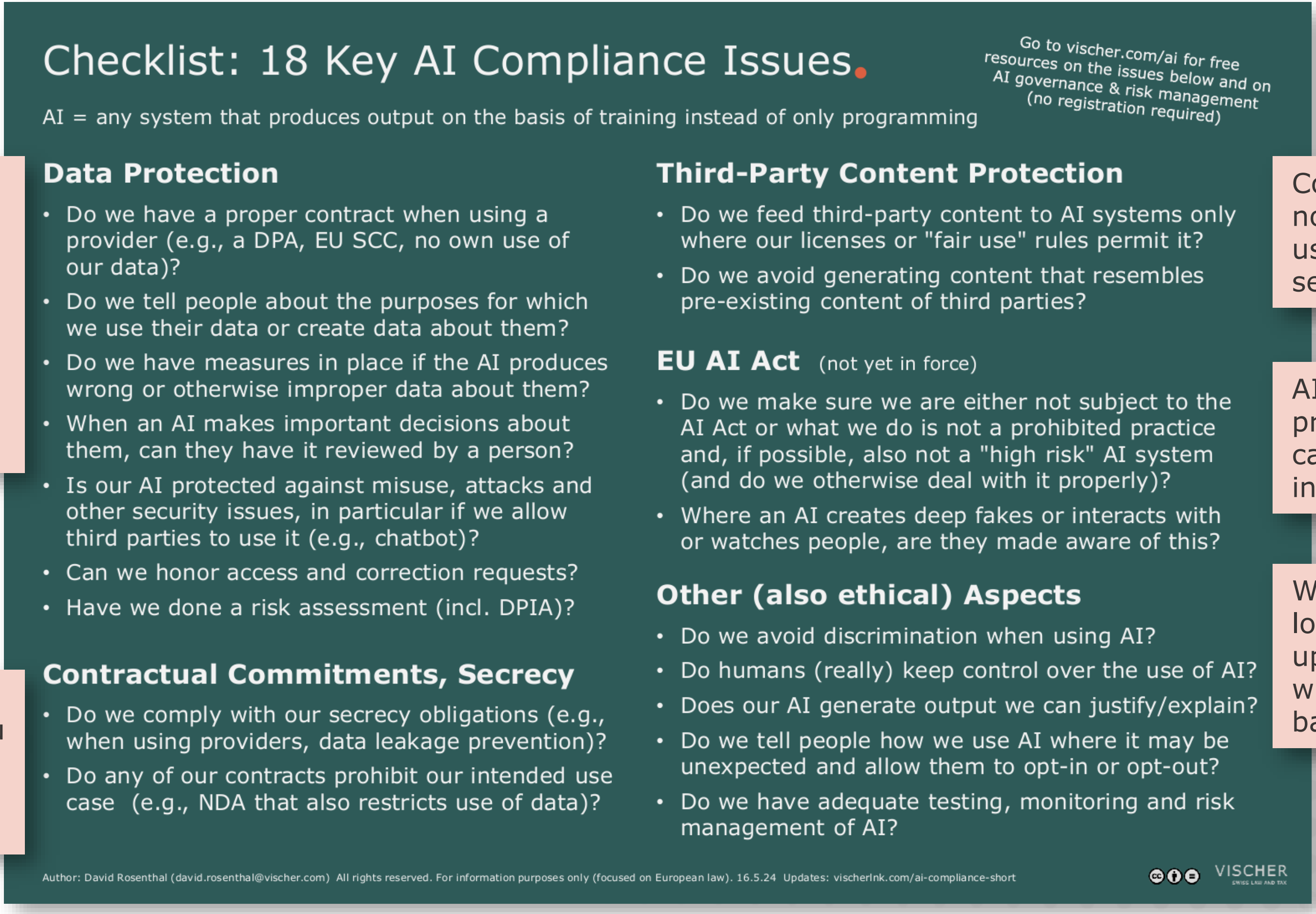
- **AI** is not new
  - Any system that has also been "trained" is AI (legally speaking)
  - AI already widely in use, e.g., OCR, face-login, translation, AML
  - New: "general purpose" AI, increased capabilities and availability
- **AI compliance issues** are not new, either
  - Governing providers, protection of CID, secondary use of data, detecting errors, protecting reputation, risk-based decisions
  - New: More SaaS, uncertainty in applying existing rules, new use cases and balancing of interest issues, regulatory activism
- AI will "disappear", as it becomes **ubiquitous** (like the net)
  - But we need to get AI literate and do our home-work

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

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

VISCHER

vischerlnk.com/ai-compliance-short



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: vischerlnk.com/ai-compliance-short

VISCHER
SWISS LAW AND TAX

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?

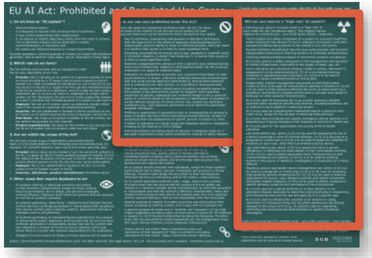
Copyright often no issue when using common sense

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

What regulators love to impose upon you even without a legal basis …

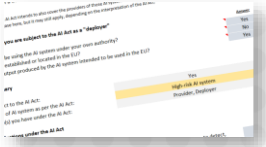
Key takeaways on the EU AI Act

- You as a Swiss bank 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 cases (e.g., AI emotion recognition in the workplace [e.g., call center], manipulation by use of AI)
  - 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

vischerlnk.com/ai-act-uc



AI Act intends to also cover the providers of these AI syst… the interpretation of the AI Act
…ase 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? Yes
…established or located in the EU? No
…utput produced by the AI system intended to be used in the EU? Yes

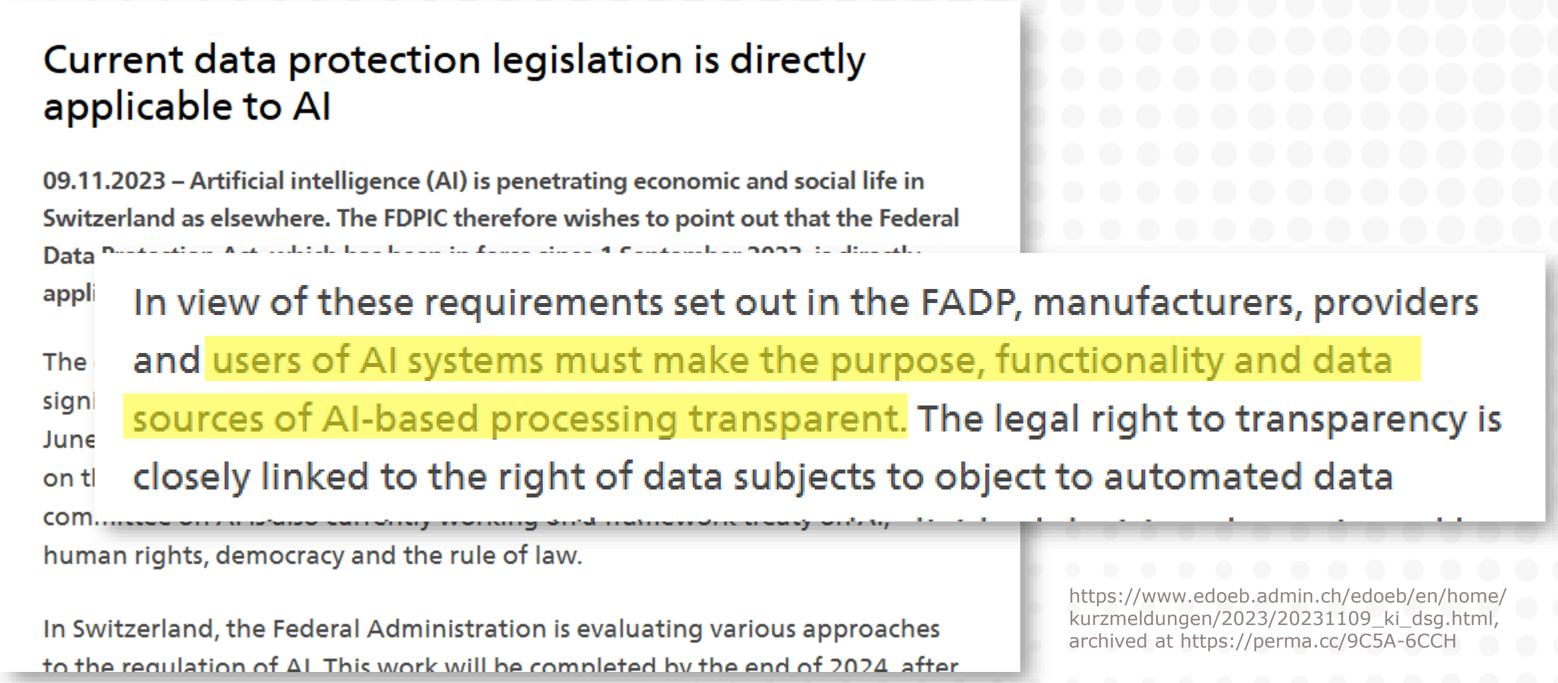
…ary

…ct to the AI Act: Yes
…of AI system as per the AI Act: High-risk AI system
…(s) you have under the AI Act: Provider, Deployer

…tions under the AI Act

See AI Act Check at
vischerlnk.com/gaira

FDPIC Expectations re AI



Current data protection legislation is directly applicable to AI

09.11.2023 – Artificial intelligence (AI) is penetrating economic and social life in Switzerland as elsewhere. The FDPIC therefore wishes to point out that the Federal Data Protection Act, which has been in force since 1 September 2023, is directly appli

The

signi

June

on th

com

human rights, democracy and the rule of law.

In Switzerland, the Federal Administration is evaluating various approaches to the regulation of AI. This work will be completed by the end of 2024, after

In view of these requirements set out in the FADP, manufacturers, providers and users of AI systems must make the purpose, functionality and data sources of AI-based processing transparent. The legal right to transparency is closely linked to the right of data subjects to object to automated data

https://www.edoeb.admin.ch/edoeb/en/home/kurzmeldungen/2023/20231109_ki_dsg.html, archived at https://perma.cc/9C5A-6CCH

FINMA Expectations re AI

1. Clear **roles** and **responsibilities** and **risk management** processes must be defined and implemented. The responsibility for **decisions cannot be delegated** to AI or third parties. Everyone involved must have sufficient expertise in AI.
2. When developing, training, and using AI, institutions need to ensure that the results are sufficiently **accurate**, **robust**, and **reliable**. Both the data and the models as well as the results need to be open to critical questioning.
3. Institutions must ensure that the results of an application are **explainable** and use of the application is **transparent**, in accordance with the recipient, relevance and process integration.
4. Institutions must avoid unjustified **discrimination**.

finma

FINMA Risk Monitor 2023

https://vischerlnk.com/3wAXidy

These expectations raise interesting questions about their legal basis and implementation

Reality Check II

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

- Example 1: **Being transparent when using AI**
  - Make any use of DeepL, text recognition, ChatGPT 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: **Non-discrimination by AI**
  - We have no law that generally prohibits discrimination in the private sector in Switzerland (e.g., when granting credit)
- Example 3: **Explainability of AI results**
  - We can explain the principle, but often not the specific results
  - Instead: Can we justify AI decisions with our own human mind?
  - FINMA's fear: Decisions that are no longer verifiable ex-post

Use Case 1: Analysis of CV

vischerlnk.com/ai-provider-check

17. April 2024

VISCHER

CHECKLISTE ZU KI FÜR VERTRÄGE MIT LIEFERANTEN UND PARTNERN

David Rosenthal

Projekt/Anbieter: ________ Bewertet: ________

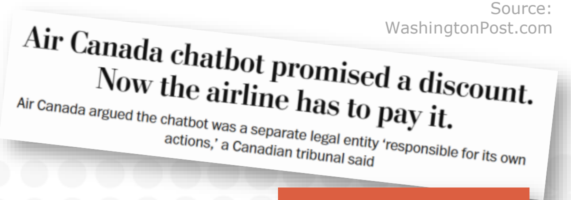
Anforderung (★ = Grundschutz)	Datenschutz	Geheimnispflichten	Urheberrecht	KI-Regulierung	Allgemein	Bewertung des Projekts/Anbieters
Identifizierung von KI [illegible]				✓	✓	☐ OK ☐ NOK ☐ N/A
Auftragsverarbeitungsvereinbarung ★ [illegible]	✓					☐ OK ☐ NOK ☐ N/A
Data Sharing/Joint Controller Agreement [illegible]	✓	✓			✓	☐ OK ☐ NOK ☐ N/A
Beschränkung der Datennutzung durch den Anbieter ★ [illegible]	✓	✓	✓			☐ OK ☐ NOK ☐ N/A

- Analyzing a **CV** of a job candidate using a provider-hosted LLM
- Have we contracted the AI **provider** in a manner that permits the processing of personal data? Will it not re-use our data?
- Are we processing the personal data for the **purpose** for which we collected it?
- Do job candidates have to expect us to do this or do we need to tell them? Is it covered by our **privacy notice**?
- Is it **fair/proportionate** for us to analyze a CV in this manner?
- Is the personal data **accurate** in view of the purpose of processing?
- Is there a relevant automated individual **decision** taken?

Warning: Such use of AI is a "high risk" use case under the AI Act

Use Case 2: Website chatbot

Source: WashingtonPost.com



Air Canada chatbot promised a discount. Now the airline has to pay it.

Air Canada argued the chatbot was a separate legal entity 'responsible for its own actions,' a Canadian tribunal said

Why wouldn't it have to pay? Would it not have to pay for the wrong advice by a call agent?

- How **risky** is the bot's topic, really? Is it ensured that the bot will stick to this topic? How well is it tested?
- Is the chatbot limited to own, **curated data** (so-called RAG)?
- How is the **reliability** of the chatbot's answers communicated to the user? Via a general disclaimer on the website (weaker) or by aligning the chatbot on how to formulate its answers and avoid providing advice/promises for individual cases (stronger)?
- Is **escalation** to a human being planned? Through keywords etc. and confidence thresholds? Via a standard disclaimer?
- What measures are in place to prevent (undesirable) **bias**?
- Is **logging** in place? Are the logs and user feedback evaluated?

AI Governance: Six steps you should take …

- Have a foundation with proper, robust **data management**
- Have the tasks, authority and **responsibilities** (AKV) in relation to AI regulated
- Decide on your AI principles and issue an **AI policy** – and use it to enable users and make them "safe", not only to restrict
- **Train** for safe and responsible use of AI and provide for AI literacy – up to the board
- **Map and track** your use of AI – and assess it (e.g., AI Act, FINMA requirements)
- Include AI in your **risk management** process – but follow a risk-based approach (most use cases will be low or medium risk, but you need to understand the unique AI risks)

→ See our blog on the AI Act and a cheat-sheet at vischerlnk.com/3TKWj2e & vischerlnk.com/ai-act-uc

→ See our blog and our AI risk assessment tool GAIRA (also includes AI Act Check) vischerlnk.com/4bF85CW & vischerlnk.com/gaira

VISCHER

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

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