

Aktuelle Themen des Datenschutz- und KI-Rechts. Was in diesen Bereichen derzeit in der Schweiz bewegt

David Rosenthal, VISCHER AG
9. Februar 2026

Überblick

- Auskunftsrecht
- Data Breaches
- Risikobeurteilungen
- Nutzung von KI im Unternehmen
- KI-Regulierung in der Schweiz
- Das wäre auch ein Thema:
 - Cookies und Online-Werbung – Diskussionen auch in der Schweiz
 - Digital Omnibus – EU Daten- und Digital-Recht etwas erleichtern
 - Training von KI mit Benutzerdaten – LinkedIn, Meta & Co.

Auskunftsrecht

- **Schwerpunkt in der Praxis**
 - Nr. 1: Bewerber und arbeitsrechtliche Streitigkeiten
 - Nr. 2: Betrieb von bekannten Websites
- **Themen**
 - Anwendbarkeit der DSGVO auf Schweizer Unternehmen
 - Identifikation der betroffenen Personen
 - "Gib mir alles" ... und die damit verbundene Strafbarkeit
 - Missbräuchliche Auskunftsgesuche
 - "... das Auskunftsgesuch offensichtlich unbegründet ist, namentlich wenn es einen datenschutzwidrigen Zweck verfolgt, oder offensichtlich querulatorisch ist." (Art. 26 Abs. 1 Bst. c DSG)

Ein besonders dreister Fall ...

"... am heutigen **15.01.2026** habe ich Ihr Internetangebot unter ... besucht. Wie im beigefügten Screenshot zweifelsfrei dokumentiert ist, weist Ihr Webauftritt einen erheblichen Mangel in der Umsetzung der Datenschutzbestimmungen auf. ... Durch diesen unbefugten Kontrollverlust über meine personenbezogenen Daten ist mir ein immaterieller Schaden entstanden. ...

Ich fordere Sie hiermit auf:

- **Schadensersatz:** Zahlen Sie zur Abgeltung des entstandenen Schadens einen Betrag in Höhe von **40,00 EUR**.
- **Auskunft:** Erteilen Sie mir vollumfängliche Auskunft über die bereits verarbeiteten Daten sowie alle Empfänger, an welche meine Daten ohne meine Zustimmung übermittelt wurden.

Aufgrund der eindeutigen technischen Beweislage habe ich mir für den Zahlungseingang eine kurze Ausschlussfrist bis zum **22.01.2026** notiert. ... Sollte der Betrag nicht fristgerecht eingehen, werde ich den Vorgang der zuständigen Aufsichtsbehörde (EDÖB) melden. Gemäß meinen internen Richtlinien weise ich darauf hin, dass ich den Anspruch bei einer erneuten Nichtzahlung erhöhen werde. Nur bei fristgerechter Zahlung betrachte ich die Angelegenheit als erledigt. ..."



Data Breaches

Vorgaben

- Data Breach $\approx$ Bruch von Schutzmassnahmen führt zur planwidrigen Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität von Personendaten
- Bei hohem Risiko für Betroffene: Dem EDÖB melden
- Falls zu ihrem Schutz nötig: Betroffene informieren

Themen

- Wann liegt ein hohes Risiko vor? Meldung auch ohne ein solches?
- Information der betroffenen Personen
- Medienberichterstattung, Öffentlichkeitsgesetz
- Meldepflicht nach ISG, Meldepflicht nach DSGVO

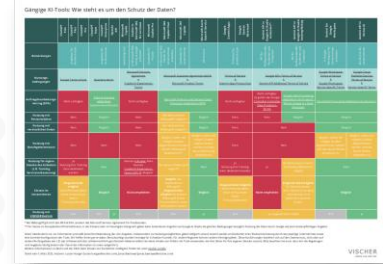
vud.ch/breach

Ideales Einsatzgebiet für KI

vud.ch/dsfa,
ausgefüllt mit Red Ink

Nutzung von KI im Unternehmen

- **Thema:** KI auch mit streng vertraulichen Daten nutzen
 - Kein Thema: Angst, dass Daten für Trainings genutzt werden
- **Angebotslage nicht transparent**
 - US-Tech-Anbieter vs. nationale Anbieter vs. Self-hosting
 - Hürde #1: Vertragliche und technische Massnahmen erforderlich
 - Hürde #2: Leistungsfähigkeit der verfügbaren Modelle
- **Herausforderungen**
 - Benutzer sind enttäuscht, "AI Slop"
 - "Shadow AI" als Sicherheitsrisiko
 - "KI-Agenten" als systemisches Sicherheitsrisiko



vischerlnk.com/ki-tools-0325

Providerliste auf
<https://redink.ai>



Berufsgeheimnis-Zusatz
vischerlnk.com/3IuUQLO

Wenn menschliche Aufsicht umgangen wird ...

Contagious Claude Code bug Anthropic ignored promptly spreads to Cowork

Office workers without AI experience warned to watch for prompt injection attacks - good luck with that

 [Brandon Vigliarolo](#)

Thu 15 Jan 2026 // 19:15 UTC

Anthropic's tendency to wave off prompt-injection risks is rearing its head in the company's new Cowork productivity AI, which suffers from a Files API exfiltration attack chain first disclosed last October and acknowledged but not fixed by Anthropic.

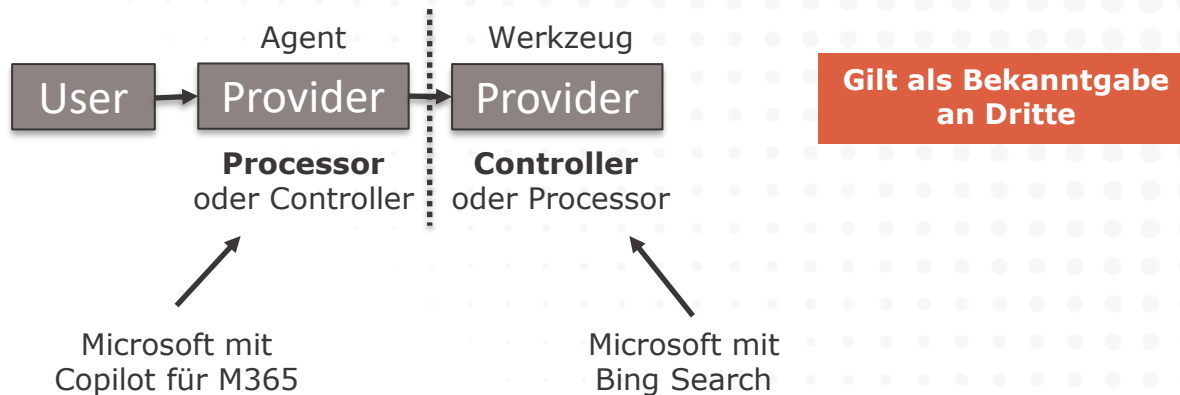
Source: [TheRegister.com](#)

"In order to trigger the attack, all a potential victim needs to do is connect Cowork to a local folder containing sensitive information, upload a document containing a hidden prompt injection, and voilà - when Cowork analyzes those files, the injected prompt triggers."

If an attacker uses its own Anthropic API to exfiltrate, the attack is not detected ...

... und Provider zu "Verantwortlichen" werden

- Wer die wesentlichen datenschutzrechtlichen **Parameter** (wer erhält wo was wann und wie) einer Bearbeitung (mit) **festlegt**
 - Betreiber von KI-Agenten, die entsprechenden Einfluss haben
 - Dritte, die Anfragen mit Daten von KI-Agenten verarbeiten



Copilot für M365 / Bing

Note: The web search queries generated by Copilot and sent to Bing are subject to the [Microsoft Services Agreement](#) between each user and Microsoft, together with the [Microsoft Privacy Statement](#). In the event of conflict with respect to the use of Bing with Microsoft 365 Copilot and Microsoft 365 Copilot Chat, the [Product Terms](#) supersede the Microsoft Services Agreement and the Microsoft Privacy Statement. [Learn more](#)

Bing

The Data Protection Addendum does not apply to Bing Search Services or to any use of Bing within a Product. For any component of a Product that is powered by Bing, as disclosed in the product documentation, the Microsoft <https://privacy.microsoft.com/privacystatement>

Query Data

If permitted by Customer, users may elect to use web query functionality optionally available through Bing as a connected service subject to the "Bing" terms of use set forth in the [Universal Terms for Online Services](#). Notwithstanding the foregoing, any terms applicable to the web query functionality, queries, or other data (including any **Personal Data**) ("Query Data") sent from Entra ID-authenticated use of Microsoft 365 Copilot and Microsoft 365 Copilot Chat to Bing are subject to the following terms:

- Microsoft has no rights in Query Data other than as needed to provide the services,
- Query Data is not used to improve Bing,
- Query Data is not used to create advertising profiles or track user behavior,
- Query Data is not shared with advertisers or otherwise beyond Microsoft and its contracted suppliers who are subject to terms no less protective than these provisions,
- Query Data is not used to train generative AI foundation models, and
- Query Data is treated as Customer confidential information and protected by appropriate technical and organizational measures.

Ausserhalb einer Auftragsbearbeitung
(die hier gerade nicht vorliegen soll) ist
eine Bekanntgabe von Personendaten
an Dritte oft unzulässig

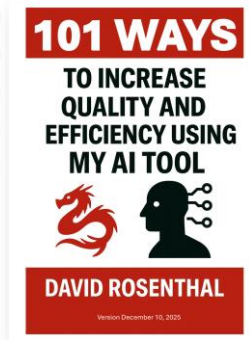
KI im Recruitment

- **Typischer Use Case**
 - KI prüft Bewerber und (a) macht Vorschlag oder (b) sortiert aus
- **Datenschutzrechtliche Themen**
 - Transparenz: Muss auch Fall (a) offengelegt werden?
 - Verhältnismässigkeit: Was ist Bewerbern zuzumuten?
 - Automatisierte Einzelentscheide: Auch im Fall (a)? Alle anhören?
- **EU AI Act** (gilt in diesem Bereich bald)
 - Grundsätzlich eine Hoch-Risiko-Anwendung → Deployer-Pflichten
 - Also: Anweisungen befolgen und deren Einhaltung überwachen, menschliche Aufsicht sichern, Qualität und Relevanz der Inputs gewährleisten, betroffene Personen informieren, DSFA

Empfehlungen

Start small, grow tall

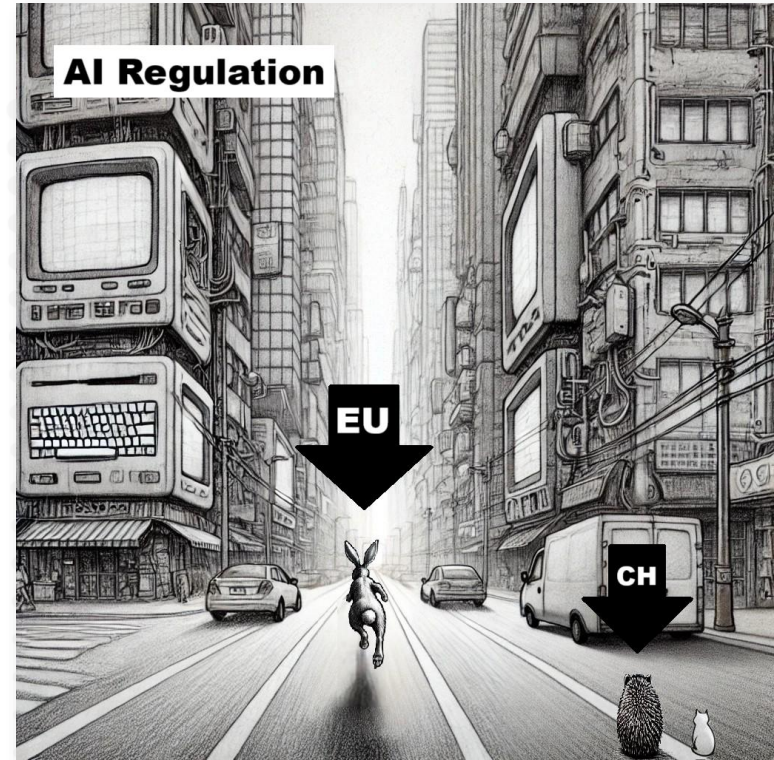
- **KI zugänglich machen**
 - Jeder sollte KI nutzen können, und zwar mit leistungsfähigen Werkzeugen und für alle Daten
 - So wird "Shadow AI" zurückgebunden
- **KI risikobasiert regeln**
 - KI-Weisung, die nach Risiken unterscheidet
 - Wir raten vom Logging der Prompts ab, wo es nicht zwingend ist
 - Basis-Infrastruktur (mit Basis-Use-Cases) freigeben; so muss bei neuen Use Cases nicht mehr jedes Mal von vorne geprüft werden
- **KI-Skills schulen – Ziel ist Kontrolle, nicht Aufsicht**
 - No-Skilling, De-Skilling und Automation Bias entgegenwirken



redink.ai

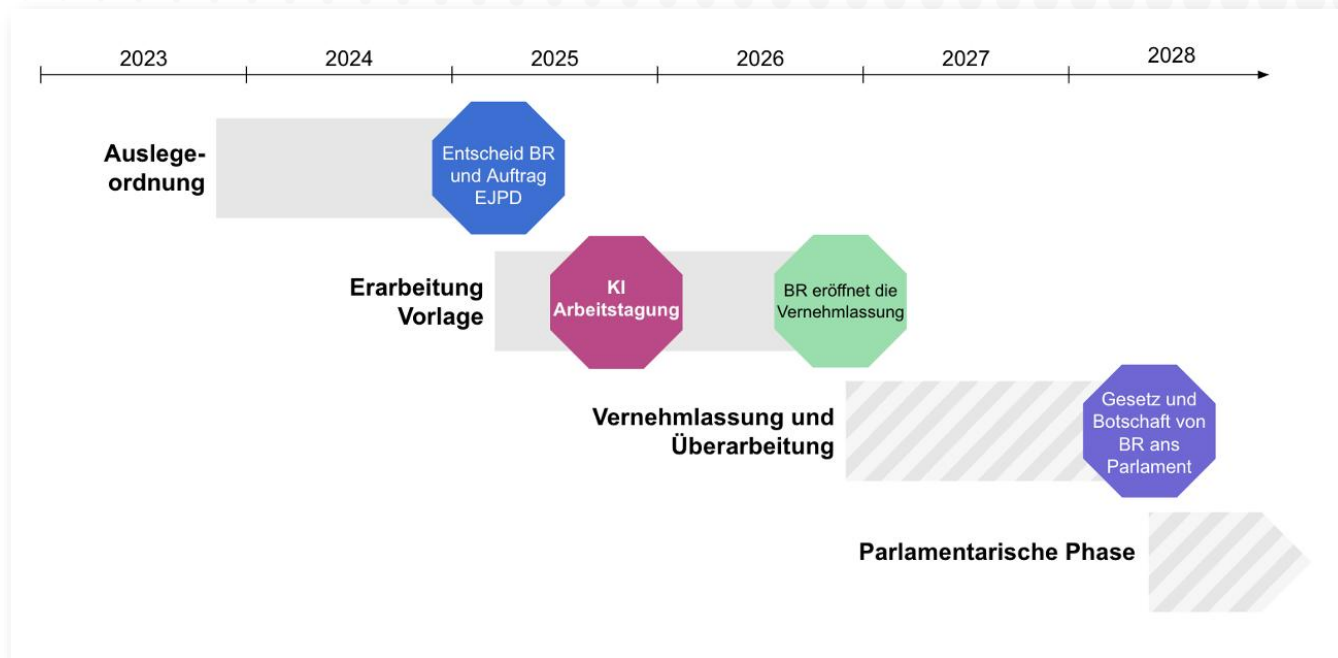
Und die Schweiz?

- **Bund:** Kein Schweizer AI Act, nur die (viel allgemeinere) KI-Konvention des Europarats
 - Beschränkte Gesetzesanpassungen im öffentlichen Sektor erwartet
 - Regelungen für KI-unterstützte Einzelentscheide
 - Pflicht zur Führung eines KI-Inventars
 - Mehr Transparenz
 - "Grundrechte-Folgenabschätzung"
- **Kantone** müssen Vorgehen selbst festlegen



Fahrplan des Bundes

Parallele Projekte in
Spezialbereichen wie etwa dem
Urheberrecht und Finanzmarktrecht



Aus: "Wie lässt sich die KI-Konvention des Europarats ins Schweizer Recht umsetzen?" des Bundesamts für Justiz vom 28. November 2025

Danke für Ihre Aufmerksamkeit!

Fragen: 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

Esplanade Pont-Rouge 9C
Postfach
1200 Genf 26, Schweiz
T +41 58 211 35 00



<https://redink.ai>

KI und Recht:
vischer.com/ki