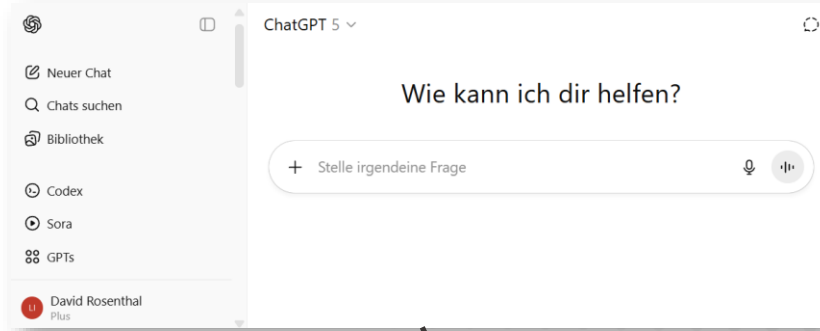
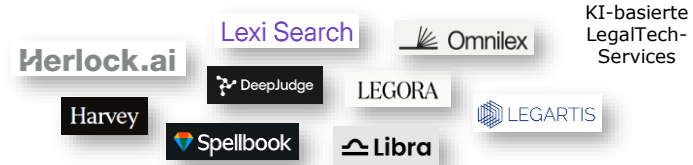


VISCHER

KI in der Anwaltskanzlei. Wie die Hürden meistern?

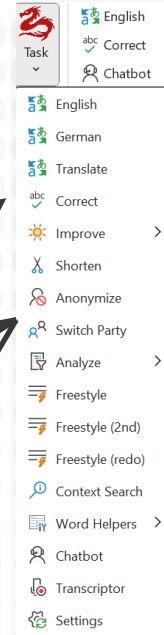
David Rosenthal, Partner, VISCHER AG
21. Oktober 2025

Worüber sprechen wir?



Chatbot/KI-Services wie
ChatGPT, Copilot,
Gemini, Perplexity

Lokale KI-Software wie
Red Ink, Open WebUI, Jan,
Copilot, Comet (Perplexity)



LLM = grosse
Sprachmodelle

spontane
Modelle

Modelle, die
"nachdenken"

weitere Funktionen



Kommerziell (USA,
Hosting auch Europa)



Kommerziell
(USA, Hosting auch Europa)

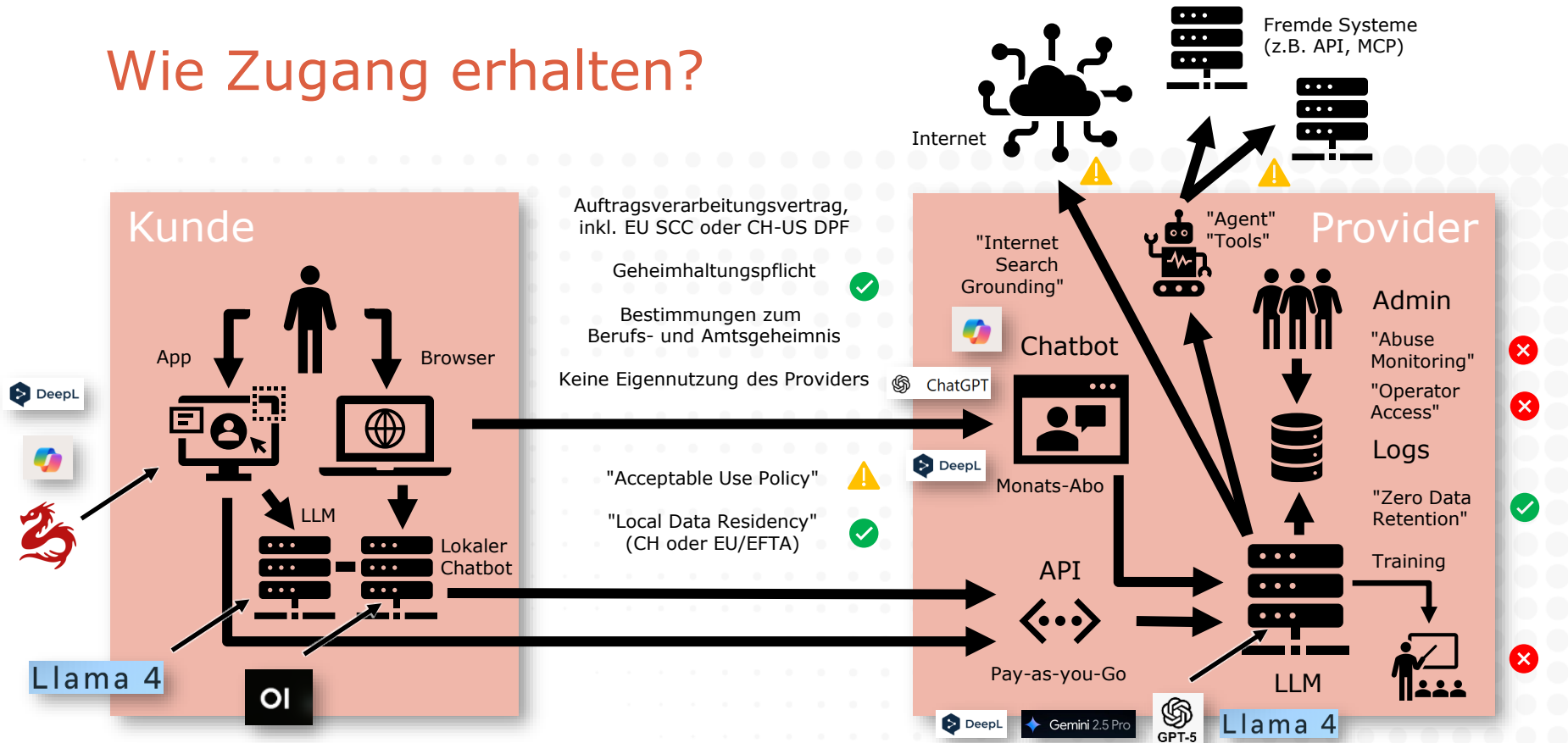


Open-Source
(China, USA; Hosting überall)



Open-Source
(Schweiz)

Wie Zugang erhalten?



Was braucht es rechtlich?

Achtung: Consumer-Versionen der KI-Services sind günstiger, aber nicht genügend für das Berufsgeheimnis und Personendaten

- **Passender Providervertrag**

- "Auftragsverarbeitungsvertrag" (AVV, DPA) (= DSGVO-Basispflicht)
- Regelungen zum Schutz von Berufs- und Geschäftsgeheimnissen
- *Zero Data Retention* (keine Speicherung von In- und Outputs)
- *Local Data Residency* (Speicher- und Bearbeitungsort garantiert)
- Keine Verwendung der In- und Outputs für Zwecke des Providers (z.B. Training, Abuse Monitoring), grundsätzlich kein Datenzugriff
- Angemessene, überprüfte Datensicherheit

- **Passende Konfiguration**

- Insb. Geo wählen (Schweiz oder "sicheres" EU-Land; sonst braucht es die sog. EU SCC), kein Zwischenspeichern (Caching), Admin-Zugriff sperren, autom. Internet-Suche deaktivieren

Endpoint = <https://europe-west4-aiplatform.googleapis.com/v1/p>

↗ = Rechenzentrum in Eemshaven, Holland

Berufsgeheimnis in der Cloud?

- **Vorgaben** beim Einsatz insb. **ausländischer Provider**
 - Einhaltung der Geheimhaltung seitens des Providers, auch wenn dieser im Ausland ist (vertragliche Verpflichtung)
 - Angemessene Informationssicherheit, keine Zweckentfremdung
 - Kein Grund zur Annahme, dass es via Provider zu ausländischem Behördenzugriff kommt (Stichwort "US CLOUD Act")
- **Massnahmen** insb. gegen ausländische Behördenzugriffe
 - Europäische Gegenpartei, Datenhaltung in der Schweiz, vom Kunden kontrollierte Verschlüsselung, manueller Providerzugriff beschränken (Stichwort "Customer Lockbox"), Verpflichtung zur Einhaltung des Berufsgeheimnisses, Defend-your-data-Klausel, Schutzmassnahmen für Personendaten auf alle Inhalte ausweiten und Einschränkung der Bearbeitung für eigene Providerzwecke

Prüfung Lawful Access Risiko
mit "Methode Rosenthal"
vischerlnk.com/flara
vischerlnk.com/flaraafa



vischerlnk.com/4ck2J0L

Ermöglichen
Abwehr von
Behörden-Zugriff
z.B. unter dem
US CLOUD Act

Cloud-Nutzung rechtmässig ohne Waiver möglich

Art. 37 Datensicherheit

Anwältinnen und Anwälte stellen sicher, dass digitale Daten, die dem Berufsgeheimnis unterstehen, so aufbewahrt und für den digitalen Zugriff bereitgestellt werden, dass sie nach dem Stand der Technik vor unerlaubtem Zugriff Dritter geschützt sind.

Art. 38 Outsourcing

Die Beauftragung Dritter mit der Erbringung von digitalen oder persönlichen Hilfsdienstleistungen für die Berufsausübung (Outsourcing) ist zulässig. Drittanbieter solcher Hilfsdienstleistungen sind darauf hinzuweisen, dass sie als Hilfspersonen gemäss Art. 321 StGB dem Berufsgeheimnis selbst unterstehen und dieses strikte einzuhalten haben. Anwältinnen und Anwälte stellen im Übrigen die Einhaltung der Berufsregeln, insbesondere des Berufsgeheimnisses, durch die sorgfältige Auswahl und Instruktion des Dienstleistungserbringers sowie durch ausreichende vertragliche Regelung sicher.

Die Speicherung und sonstige Bearbeitung von Daten, die dem Berufsgeheimnis unterstehen, kann beim Betreiber von entsprechenden Infrastrukturen oder Anwendungen (Applikationen) für die Mandatsführung erfolgen, wenn und solange sichergestellt ist, dass die Datensicherheit gemäss Artikel 37 gewährleistet und der Zugang zu den Informationen nur unter Wahrung der Bestimmungen zum Schutz des Berufsgeheimnisses möglich ist. **Das wird bei ausreichend erfahrenen Anbietern von Cloudlösungen mit Datenspeicherung und -bearbeitung im Inland, in der EU, der EFTA und im Vereinigten Königreich vermutet.**

Schweizer Ständesregeln (SSR)

Kriterium 1	Kriterium 2	Kriterium 3	Kriterium 4	Kriterium 5
1. Land in Betracht, von dem es geht:	2. Bewertung des Risikos des Informationsverlusts	3. Bewertung des Risikos des Informationsverlusts	4. Bewertung des Risikos des Informationsverlusts	5. Bewertung des Risikos des Informationsverlusts
a) Bewertung des Risikos des Informationsverlusts	b) Bewertung des Risikos des Informationsverlusts	c) Bewertung des Risikos des Informationsverlusts	d) Bewertung des Risikos des Informationsverlusts	e) Bewertung des Risikos des Informationsverlusts
100	100	100	100	100
100	100	100	100	100

- Die Berechnung des Risikos eines ausländischen "Lawful Access" erscheint nach Ansicht der Staatsanwaltschaft grundsätzlich ein geeignetes Kriterium, um die Vertretbarkeit der Auslagerung auch vor einem strafrechtlichen Hintergrund zu beurteilen. Eine Überprüfung des Ergebnisses im konkreten Fall ist der Staatsanwaltschaft indes nicht möglich, da dieses letztlich von den Einschätzungen der einzelnen Berechnungsfaktoren abhängt. Diese können von aussen nicht überprüft werden.

Beurteilung der Wahrscheinlichkeit eines Foreign Lawful Access mit der "Methode Rosenthal"

vischerlnk.com/flara

vischerlnk.com/flarafaq

vischerlnk.com/3HAvCVB (zur Lage betr. Trump)

Cloud-KI-Provider für Anwaltskanzleien

- **Google** (Gemini, weitere Modelle via Vertex API)
 - Vertrag mit Berufsgeheimniszusatz; Opt-out vom Abuse Monitoring auch für "Kleine" möglich; EU/EFTA; ZDR
- **Microsoft** (Copilot, Azure OpenAI Services, GPT-Modelle)
 - Vertrag mit Berufsgeheimniszusatz, EU/EFTA, kein Opt-out vom Abuse Monitoring bei API-Zugang für Kanzleien, nicht konform geregeltes Search Grounding, fehlende Klarheit bei "Copilot"
- **OpenAI** (ChatGPT, GPT-Modelle)
 - ADV, aber kein Berufsgeheimniszusatz (OpenAI scheint nicht interessiert), Daten gehen vermutlich in die USA, inzwischen keine dauerhafte Speicherung der Outputs mehr (betr. Europa)
- **Perplexity** – ungenügender Vertrag, Daten gehen in die USA

The table compares various AI tools (Google Gemini, Microsoft Copilot, OpenAI GPT, etc.) across several criteria: Data protection, Search Grounding, Abuse Monitoring, and others. It uses a color-coded system (green for good, red for bad, yellow for mixed) to indicate the quality of each tool's performance in these areas.

vischerlnk.com/ki-tools-0325

Wir nutzen **Google** mit Berufsgeheimnisdaten und **OpenAI** und **Perplexity** ohne (für Research/Deep Research) jeweils mit unserem Tool Red Ink und Open WebUI

Details wie Sie zu einem Vertrag mit Google oder Microsoft kommen in Kürze auf vischer.com/redink

Schweizer KI-Provider für Anwaltskanzleien

- **Schweizer Provider** als Alternative zur KI via "US-Cloud"
 - Vertragszusatz zum Schutz des Berufsgeheimnisses für Schweizer KI-Provider publiziert (vischerInk.com/3IuUQLO) →
 - Diverse Schweizer Provider eingeladen, KI-API-Services für Anwälte mit diesem Vertragszusatz anzubieten (nicht über uns!)
- **Zusagen** bisher von **MTF**, **AlpineAI**, **SafeSwissCloud**
 - Weitere sind angefragt bzw. im Gespräch
 - Details auf vischer.com/redink
- Daten bleiben **in der Schweiz**, der Anbieter ist in der Schweiz, und sie haben lokalen Support und teilweise weitere Angebote
- Die **Open-Source**-Modelle, die sie nutzen, sind etwas weniger leistungsfähig, genügen aber für manche Basisaufgaben



Diese Services können mit Tools wie Red Ink, Open WebUI oder Jan benutzt werden; teils werden auch Chatbot-Services angeboten

Was wir bei uns machen



- **Niederschwellige** Einsatzmöglichkeiten im Alltag waren uns wichtig
 - Gamechanger: Freigabe der KI für alle Daten, Verfügbarkeit für alle
 - Unser Tool gibt uns Zugang zu den besten Modellen auf dem Markt
 - Kosten dank API-Nutzung viel tiefer als Lösungen mit Monatsabo
- KI als ein wichtiges **Werkzeug**, aber nicht als **Ersatz** verstehen
 - Wir produzieren mehr in weniger Zeit oder aber bessere Qualität
 - KI: Schneller, williger Adlatus, der mit Fleiss und Durchschnitt glänzt
- Tools und gute Modelle genügen nicht, **Schulung** und **Übung** sind nötig – wo und wie KI in Abläufen sinnvoll einbauen ("AI Slop")?
- **Aber:** Altbekannte und neue Herausforderungen wegen KI
 - Fehler, "Denkfresser", Ausbildung Nachwuchs, Wandel des Geschäftsmodells



12	It was a wi-fi attack with the aim of sabotaging us	No	N/A	Incident was accidental disclosure.
13	It was the work of a professional who presumably pursued financial goals with it	No	N/A	Incident was due to human error by a backup staff member.
14	We were able to lock out the attacker before he could exfiltrate our data	No	Neutral	Not an external attacker; data was sent out.
15	We were able to lock out the attacker before he could destroy our data	No	Neutral	Not an external attacker; no data destruction occurred.
16	The unintentional disclosure was made to what we consider to be a trustworthy third party	Yes	Reduces it	Recipient co-worker and their spouse. Co-worker was cooperative, deletion supervised. Trustworthiness of spouse assumed via employee.
17	A large number of people are affected	Yes	Increases it	149 co-workers affected.
18	Particularly sensitive/special categories of data is affected	Yes	Increases it	Social Security Identifier, financial data (taxable income, tax paid), marital status.
19	Particularly vulnerable people are affected	Unclear	Neutral	No specific information on vulnerability of affected co-workers beyond general employee status.
20	The data is for other reasons particularly sensitive	Yes	Increases it	Combination of Full name, DOB, SSN, Home address, and financial details poses a high risk for identity fraud.
21	We		Neutral	Incident occurred on 13 April, email sent then. Discovered/reported on 15 April. Duration of exposure known.
22	Th		Reduces it	Spouse forwarded to co-worker. Deletion supervised. Assumed no further intentional distribution by
23	Th		N/A	Not mentioned in the case.
24	Th		N/A	Researcher is misdirected email not system compromise. Email authors security not detailed.

Zusammenfassend lässt sich aus den Unterlagen folgendes Bild ergeben: **Alectra** und **Noventis** haben einen Kooperationsvertrag zur Entwicklung eines integrierten Systems für die industrielle Fertigungsautomatisierung geschlossen. **Alectra** ist für die Hardware, **Noventis** für die Software zuständig. Es gibt schwerwiegende Probleme bei der Integration der von **Noventis** gelieferten Software. **Alectra** beklagt die Nichteinhaltung der vereinbarten Standards, Instabilität der Schnittstellen und unzureichende Dokumentation. **Noventis** hingegen behauptet, die Probleme seien in ihrer Umgebung nicht reproduzierbar und führt Konfigurationsabweichungen auf Seiten von **Alectra** als mögliche Ursache an. Die Kommunikation zwischen den Parteien ist stark gestört und eskaliert zunehmend. **Alectra** hat den Vertrag fristlos gekündigt und behält sich rechtliche Schritte vor. Zusätzlich gibt es eine offene Zahlungsforderung von **Alectra** an **Noventis**, die **Noventis** bisher nicht beglichen hat.

Drei mögliche Argumentationsstrategien für **Alectra**:

- Fokus auf die Nichterfüllung der vertraglichen Pflichten durch Noventis:** **Alectra** argumentiert, dass **Noventis** die im Vertrag festgelegten Leistungen nicht erbracht hat. Die gelieferte Software ist instabil, entspricht nicht den vereinbarten Standards und ist unzureichend dokumentiert. Die wiederholten Aufforderungen zur Mängelbeseitigung blieben erfolglos. Dies stellt einen erheblichen Vertragsbruch dar, der **Alectra** zur fristlosen Kündigung berechtigt. Die nicht reproduzierbaren Fehler in der Testumgebung von **Noventis** entbinden **Noventis** nicht von der Pflicht, funktionierende Software gemäss den Spezifikationen zu liefern. **Alectra** kann auf Schadenersatz für die entstandenen Kosten und den entgangenen Gewinn klagen.
- Kombination aus technischem Mangel und gestörter Kommunikation:** **Alectra** betont die technischen Mängel der Software und untermauert diese mit den in den Unterlagen dokumentierten Fällen.

21.2 Die Leistungserbringerin übernimmt mit der Lieferung die Verpflichtungen der Leistungsbezügerin aus Einfuhrzertifikaten,

der Datenbearbeitung

der Vertrag nicht anders geregelt, hat die Bearbeitung, welche die Leistungserbringerin im Auftrag der Leistungsbezügerin vornimmt, in der Schweiz und unter dem Schweizer Recht zu erfolgen.

Abtretung, Übertragung und Verpfändung

Die Rechte und Pflichten aus dem Vertragsverhältnis dürfen ohne schriftliche Zustimmung des Vertragspartners nicht abgetreten, übertragen noch verpfändet werden. Die Leistungsbezügerin wird die Zustimmung zur Abtretung und Übertragung von Forderungen durch die Leistungserbringerin in begründeten Fällen verweigern.



VISCHER



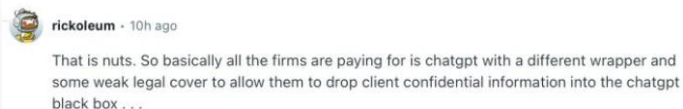
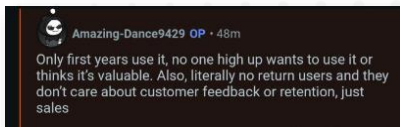
RI: Diese Bestimmung kann für Provider problematisch sein, die ihre Datenverarbeitung im Ausland durchführen oder auf ausländische Subunternehmer angewiesen sind. Die Beschränkung auf die Schweiz kann die Flexibilität und Kosteneffizienz des Providers einschränken.
22. Mai 2025, 23:03

Antworten

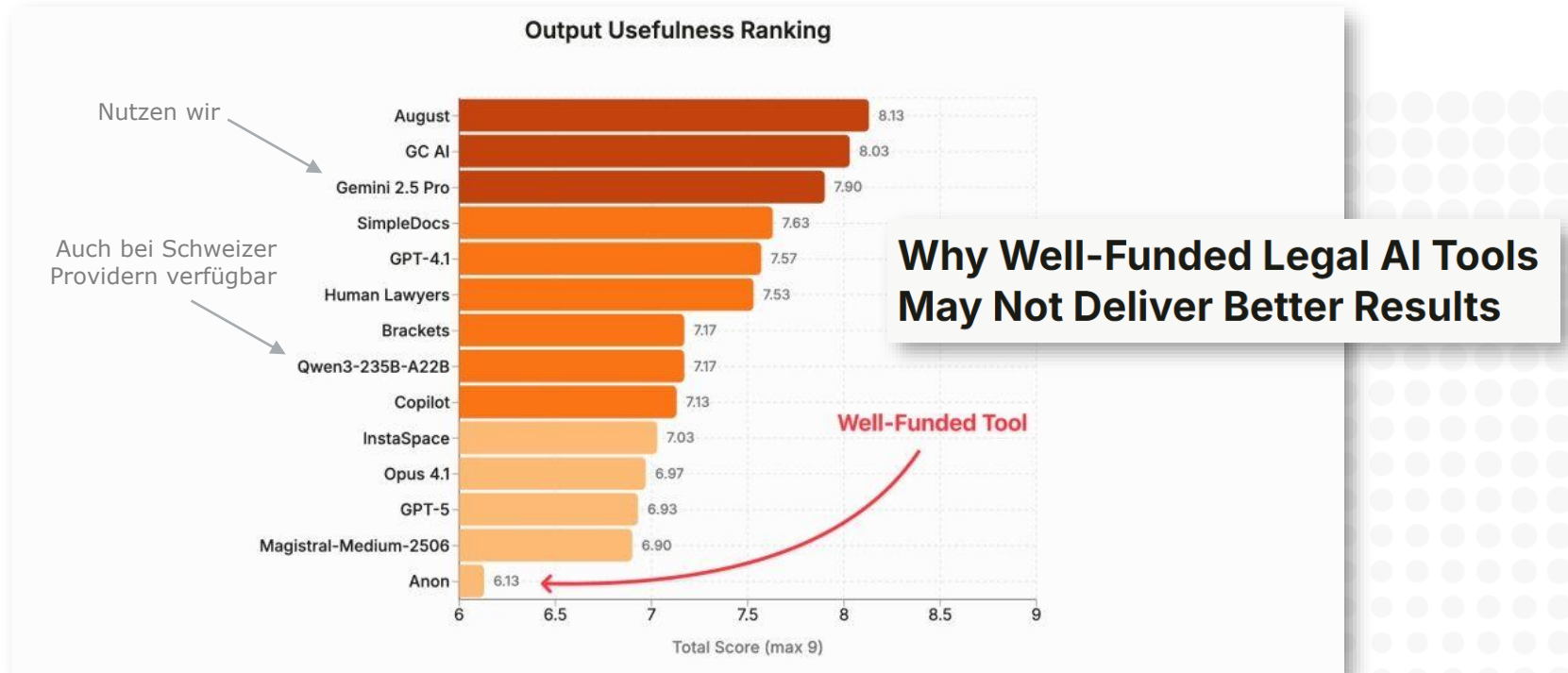
Beispiele mit "Red Ink"

KI-Lösungen speziell für Anwaltskanzleien

- **Kritisch bleiben** – es herrscht Goldgräberstimmung unter den Anbietern
 - Von vielzitierten Produkten wie Harvey, Spellbook etc. halte ich nichts



- Kosten oft ein Vielfaches von "normalen" KI-Lösungen, aber was bieten sie wirklich mehr für uns? Wo sie mehr bieten – lohnt sich das wirklich?
- Manche unseriöse Werbeversprechen im Markt (z.B. KI "ohne Halluzinationen")
- Berufsgeheimnis geschützt? Woher das rechtliche Know-how ("Blackbox")?
- **Prüfen:** KI-basierte Content-Services, Dokumenten-Datenbanken ("RAG")
 - Wir nutzen z.B. LexiSearch als KI-basierter Suchdienst für CH-Rechtsprechung
- **Prüfen:** KI-basierte Dienste für Spezial-Use-Cases (Reviews, Prozessakten)



<https://www.legalbenchmarks.ai/resources/articles/why-well-funded-legal-ai-tools-may-not-deliver-better-results>

Was braucht es zur Strafbarkeit?

- Eine **Gesetzesbestimmung**, die ein Verhalten für strafbar erklärt ("keine Strafe ohne Gesetz")
- Der **objektive Tatbestand** muss erfüllt sein: Voraussetzungen, die im Gesetz stehen
 - Auch Unterlassen (z.B. der nötigen Massnahmen) kann selbst wenn nicht erwähnt strafbar sein, wenn eine (z.B. vertragliche/gesetzliche) Pflicht besteht, das Delikt zu verhindern
- Der **Tralala-Tatbestand** muss erfüllt sein: In der Regel Fahrlässigkeit, ausnahmsweise Vorsatz
 - Aber: Wer eine Tatbestandsverwirklichung zwar nicht wünscht aber damit rechnet und sie in Kauf nimmt, handelt "eventual-vorsätzlich" = vorsätzlich
- Keine **Rechtfertigungsgründe** und **schuldauausschliessende Gründe**
 - **Ethical Hacking**: Rechtfertigender Notstand zur Abwehr einer unmittelbaren Gefahr? Dazu <https://www.ntc.swiss/executive-summary-de-gutachten-strafbarkeit-ehisches-hacking.pdf>
- Normalerweise ist die **natürliche Person** strafbar; **juristische Personen** können u.U. zur Rechenschaft gezogen werden, wenn sich keine verantwortliche Person finden lässt
- **Anstiftung** und **Gehilfenschaft** kann ebenfalls strafbar sein, der Versuch auch

Red Ink
mit GPT5

- Wichtige Korrekturen/Präzisierungen (Schweizer Recht):
- **Subjektiver Tatbestand**: Statt „Tralala-Tatbestand“. Grundsatz: **Vorsatz ist die Regel; Fahrlässigkeit ist nur strafbar, wenn das Gesetz sie ausdrücklich unter Strafe stellt**. Eventualvorsatz zählt als Vorsatz.
 - Unterlassen: Strafbarkeit nur bei rechtlicher Handlungspflicht (Garantenstellung) und Gleichwertigkeit von Tun und Unterlassen (Begehen durch Unterlassen).
- **Rechtswidrigkeit/Schuld**: „Keine Rechtfertigungsgründe und keine schuldauausschliessende Gründe“ (Schweizer Recht)

Copilot KI-generierte Inhalte können fehlerhaft sein

Ja, dein Folieninhalt auf der aktuellen Folie stimmt. Hier sind die wesentlichen Punkte, die du auf deiner Folie "Was braucht es zur Strafbarkeit?" hast:

1. **Gesetzesbestimmung**: Eine Gesetzesbestimmung muss das Verhalten als strafbar erklären.

Welche Voraussetzungen zur Strafbarkeit müssen in der Schweiz erfüllt sein?

3. **Subjektiver Tatbestand**: In der Regel ist Fahrlässigkeit ausreichend, in Ausnahmefällen ist Vorsatz erforderlich. Wer eine Tatbestandsverwirklichung zwar nicht wünscht, aber damit rechnet und sie in Kauf nimmt, handelt "eventual-vorsätzlich", was ebenfalls als vorsätzlich gilt.
4. **Keine Rechtfertigungsgründe**: Es dürfen keine Rechtfertigungsgründe oder schuldauausschliessende Gründe vorliegen.

Copilot KI-generierte Inhalte können fehlerhaft sein

In der Schweiz müssen bestimmte Voraussetzungen erfüllt sein, damit eine Handlung strafbar ist. Diese sind:

1. **Gesetzesbestimmung**: Es muss eine Gesetzesbestimmung geben, die das Verhalten als strafbar erklärt. Dies wird oft als das Prinzip "keine Strafe ohne Gesetz" bezeichnet ¹.
2. **Objektiver Tatbestand**: Der objektive Tatbestand muss erfüllt sein. Das bedeutet, dass die im Gesetz genannten Voraussetzungen gegeben sein müssen. Auch Unterlassen kann strafbar sein, wenn eine vertragliche oder gesetzliche Pflicht besteht, das Delikt zu verhindern ¹.
3. **Subjektiver Tatbestand**: In der Regel ist Fahrlässigkeit ausreichend, in Ausnahmefällen ist Vorsatz erforderlich. Wer eine Tatbestandsverwirklichung zwar nicht wünscht, aber damit rechnet und sie in Kauf nimmt, handelt "eventual-vorsätzlich", was ebenfalls als vorsätzlich

⚠ 3. „Tralala-Tatbestand“ (wohl gemeint: subjektiver Tatbestand)

Vermutlich ist das scherzhaft gemeint und steht für den subjektiven Tatbestand (innere Seite, Vorsatz/Fahrlässigkeit).

✓ Im Kern richtig.

ChatGPT mit GPT5

Es kommt nicht nur auf das Modell, sondern den Prompt und Kontext an (Copilot vs. ChatGPT vs. Red Ink je mit GPT5)

Unter vischer.com/ki finden Sie kostenlose Ressourcen zu diesen Themen sowie zu KI-Governance und Risikomanagement (keine Registrierung erforderlich).

Datenschutz

- Haben wir einen angemessenen Vertrag mit den von uns genutzten Providern (z.B. einen ADV, EU SCC, Verbot der Eigennutznutzung unserer Daten)?
- Haben wir die Leute über die Zwecke informiert, zu denen wir Daten von ihnen bearbeiten oder erzeugen, und haben wir was nötig eine Rechtsgrundlage dafür?
- Haben wir es im Griff, wenn die KI falsche oder anderweitig unzulässige Daten über sie produziert?
- Wenn eine KI wichtige Entscheidungen über sie trifft, können sie diese von einem Menschen prüfen lassen?
- Ist unsere KI vor Missbrauch und Angriffen geschützt und auch sonst sicher, insbesondere, wo wir Dritten die Nutzung erlauben (z.B. Chatbot)?
- Können wir Auskunfts- und Berichtigungsbegehren wie erforderlich umsetzen?
- Haben wir eine Risikobeurteilung für unser Vorhaben (inklusive einer DSFA) durchgeführt?

Vertragspflichten, Geheimhaltung

- Kommen wir unseren Geheimhaltungspflichten nach (z.B. beim Einsatz von Providern, Verhinderung der unerwünschten Preisgabe von Daten)?
- Untersagen unsere Verträge die von uns ins Auge gefasste Anwendung (z.B. NDA, welches die Nutzung von Daten für unsere Zwecke einschränkt)?

Schutz von Inhalten Dritter

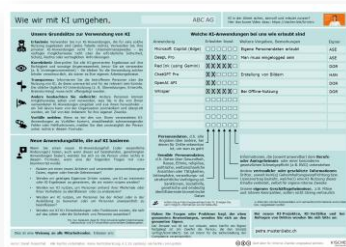
- Füttern wir KI-Systeme nur dann mit Inhalten Dritter, soweit unsere Lizenzen oder die gesetzlichen Schranken des Urheberrechts dies zulassen?
- Vermeiden wir die Erstellung von Inhalten, die bereits bestehenden Inhalten Dritter entsprechen?

EU AI Act (wird rollend von 2025-2027 Anwendung finden)

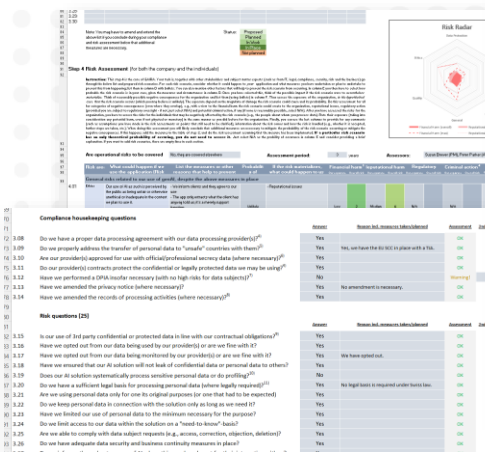
- Ist klar, dass wir entweder nicht unter den EU AI Act fallen oder unser Vorhaben keine verbotene Praktik ist und möglichst auch kein "Hoch-Risiko"-KI-System (und gehen wir ansonsten richtig damit um)?
- Wenn eine KI "Deep Fakes" erstellt oder mit Menschen interagiert oder sie beobachtet, werden sie dann darauf hingewiesen gemacht?

Andere (auch ethische) Aspekte

- Vermeiden wir Diskriminierung beim Einsatz von KI?
- Behält der Mensch (wirklich) die Kontrolle über die KI?
- Können wir unsere KI-Ergebnisse rechtfertigen/erklären?
- Sagen wir es den Leuten, wie wir KI einsetzen, wenn es für sie unerwartet sein könnte, und erlauben wir ihnen gar, sich für oder gegen deren Einsatz zu entscheiden?
- Haben wir ein angemessenes KI-Testing, angemessene Überwachung und ein angemessenes Risikomanagement?



vischerlnk.com/ki-weisung-kurz



[www.wissenschaftlicherLnk.com/ki-risikocheck](http://www.wissenschaftlicherlnk.com/ki-risikocheck)

vischerlnk.com/ki-compliance-kurz & bit.ly/3WNqxeO

Noch mehr gibt es auf vischer.com/ki

vischerlnk.com/qaira

Danke für die 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



youtu.be/RiLa2DkbNTg

Mehr: www.vischer.com/ki
www.rosenthal.ch
vischer.com/redink