

VISCHER

Red Ink.

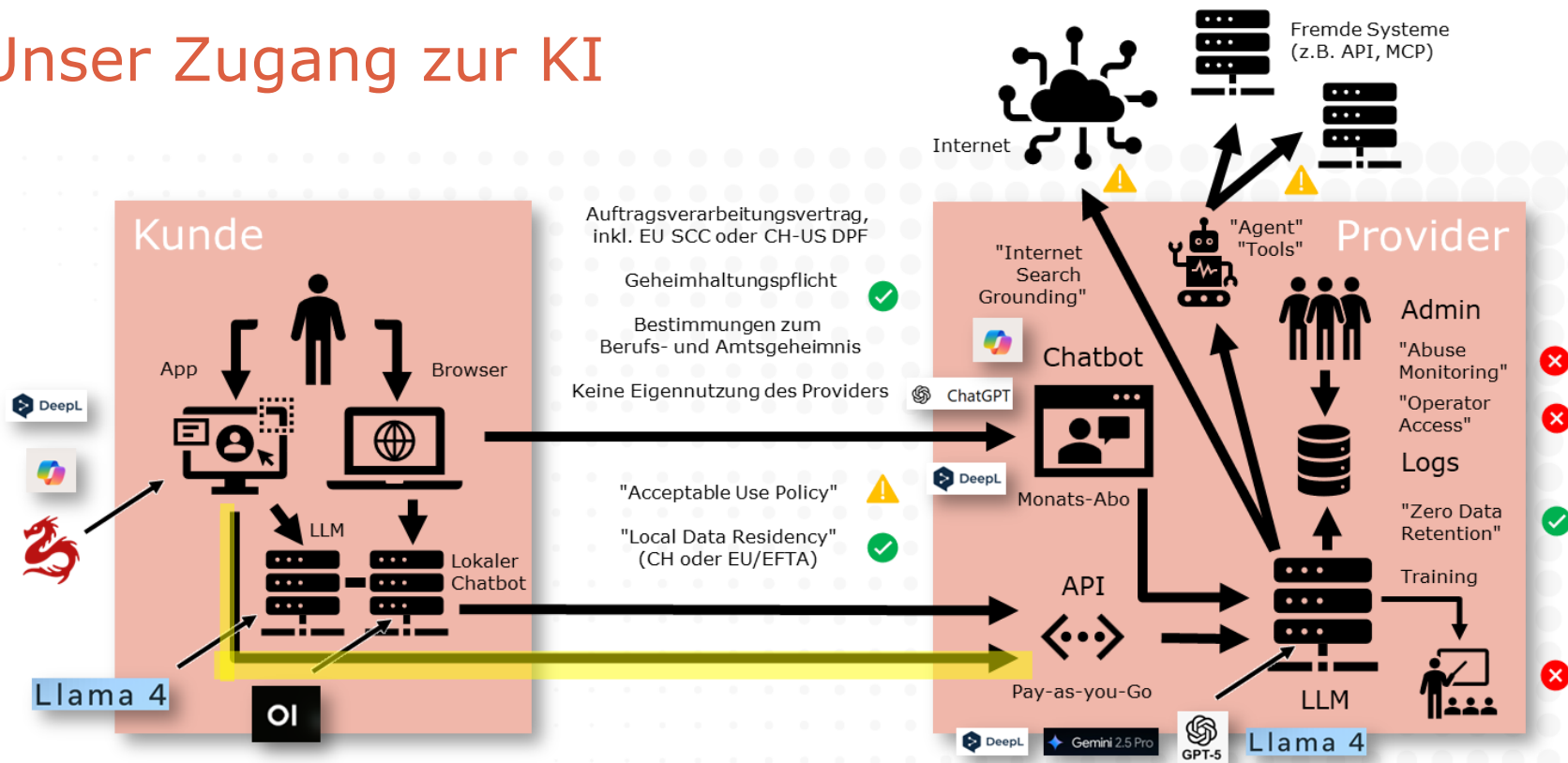
Wie wir im Alltag KI auch mit sensiblen Daten
nutzen können (und wollen)

David Rosenthal, VISCHER AG
28. Januar 2026

Wie alles begann ...

- VISCHER – eine grössere **Wirtschaftskanzlei** in der Schweiz
 - Rund 260 Personen, in allen möglichen Bereichen aktiv
- Wir wollten ...
 - KI **mit allen Daten** verwenden können (auch solche, die dem Berufsgeheimnis unterstehen)
 - **Jede Funktion** haben, die uns einen konkreten Nutzen bringt
 - Ein vernünftiges Preis-Leistungs-Verhältnis
- **Keine** der heutigen Legal-Tech- und **KI-Lösungen** bot uns dies
 - Vieles war uns zu teuer, zu wenig sicher oder zu schlecht
- Wir konnten mit **Google** einen passenden Vertrag verhandeln und **bauten unsere Lösung selbst** ...

Unser Zugang zur KI



KI für Berufsgeheimnisse

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

Welche API-Provider?

Infos zu API-Provider: <https://redink.ai>

• Cloud-Provider

- **Google, Microsoft:** Verträge mit Berufsgeheimniszusätzen und je nach Kunde auch Abuse Monitoring Opt-out
- Trickreich: Einsatz von Tooling/Grounding ("Agentic AI")
- **OpenAI, Perplexity, etc.:** Auftragsbearbeitungsverträge, aber oft nicht viel mehr, d.h. für wirklich sensible Daten nicht zu empfehlen (sind sind bisher auch nicht wirklich interessiert)

vischerlnk.com/ki-tools-0325

• Schweizer Provider

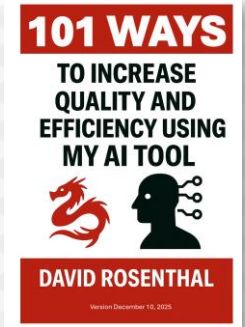
- Anbieter wie **MTF, AlpineAI, SafeSwissCloud**
- Sind in der Schweiz, mit Open Source-Modellen (USA, China)
- Vertragszusatz zum Schutz des Amts- und Berufsgeheimnisses für Schweizer KI-Provider publiziert (vischerlnk.com/3IuUQLO)



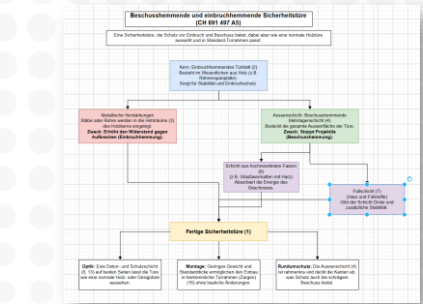
Was ist Red Ink?

Download via
<https://redink.ai>

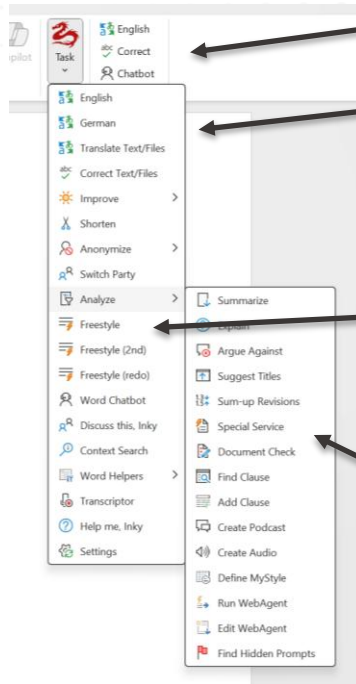
- Ein **Add-in** für Word, Excel, Outlook, Edge (Windows)
- Funktioniert mit **beliebigen LLM** (auch mehreren), quelloffen
- Kann **Texte** bearbeiten, analysieren, vergleichen, übersetzen, kommentieren, transkribieren, vertonen etc. und **Worksheets** ausfüllen, erklären, anonymisieren, anpassen, prüfen etc., und zwar jeweils direkt in den Anwendungen, auch mit PDFs etc.
- Kann **Grafiken, Diagramme, Folien, Podcasts** etc. erstellen
- Wichtig: Die "Magic" stammt vom KI-Modell, nicht dem Tool
- Aber dank dem Tool ist KI besser in unsere Abläufe integriert
- **Erfolgsfaktoren:** Keine Restriktionen betreffend Daten und auf unsere tatsächlichen Bedürfnisse im Alltag abgestimmt



-



Einfaches Grundkonzept



Chatbots, auch mit Zugriff auf Dokumente

Vordefinierte Funktionen

wie z.B. Übersetzen, Korrigieren, Text verbessern, Kürzen, Überblick verschaffen, Podcast erstellen etc.

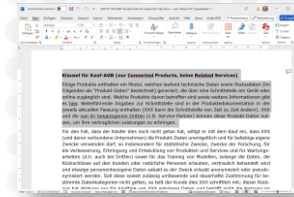
Freies Prompten

Recherchieren, Dokumente erstellen, kommentieren und überarbeiten etc.

Spezialfunktionen

wie z.B. Datenbankzugriffe, Schwärzen, Vertonen, Klauseldatenbanken, Agents

Schritt 1: Text wählen (optional)



Schritt 2: Befehl wählen

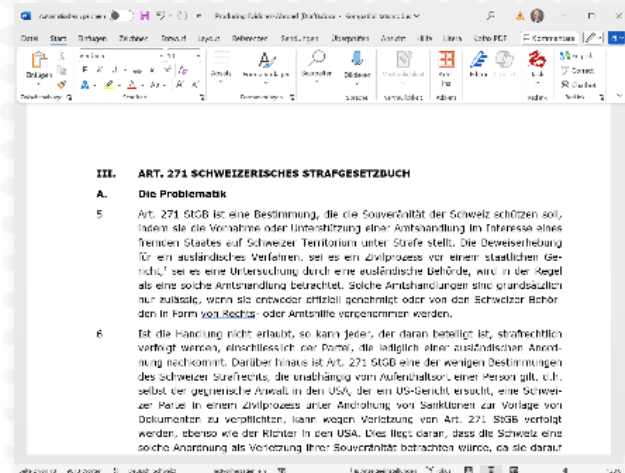
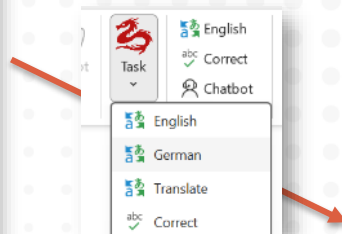
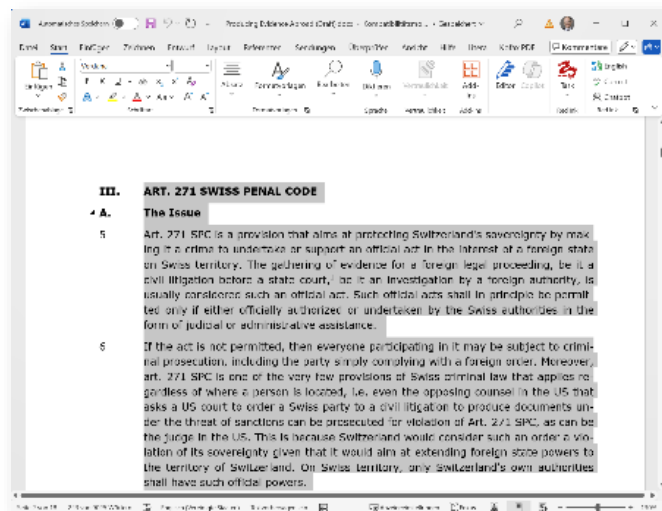
Schritt 3: Modell wählen (optional)

Schritt 4: Ggf. Auftrag/Parameter

Schritt 5: Red Ink löst den Auftrag aus

Schritt 6: Red Ink setzt KI-Antwort um

Einfache Dinge wie Übersetzen oder Umarbeiten



KI als nützlicher Helfer auch im Kleinen

The diagram illustrates the use of AI for text processing. It shows a historical document (the US Constitution) being processed by a tool (Vischer) to create a digital version (Red Ink).

Left Document (Original):

WE the People of the United States, in order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common Defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this CONSTITUTION for the United States of America.

ARTICLE I.

Sect. 1. ALL legislative powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

Right Document (Red Ink):

The content has been copied to the clipboard:

WE the People of the United States, in order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common Defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this CONSTITUTION for the United States of America.

ARTICLE I.

Sect. 1. ALL legislative powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

OK

Vischer Menu:

- Freestyle
- Clipboard to Text
- Define MyStyle

Annotations:

- A red arrow points from the text "Ctrl-Windows-S" to the Vischer menu.
- A red arrow points from the Vischer menu to the Red Ink window.

Handling umfangreicherer Unterlagen

The image shows a Red Ink Freestyle window in the foreground and a Microsoft Word document in the background. The Red Ink window has a title bar that reads "Red Ink Freestyle (using gemini-1.5-pro-002)". The main text area contains the prompt: "Please provide the prompt you wish to ex... separate output or with 'Bubbles:' for havi... the prompt library; include '{doc}' for text... all, '{lib}' for library search, '{net}' for inter... file object; use 'Pure:' for direct prompting". Below the text area are "OK" and "Cancel" buttons. The background Word document is titled "Dokument1" and shows a German text about a software dispute between Alectra and Noventis. The text discusses the fulfillment of a cooperation agreement, the reliability of the software, and the responsibility for integration problems. The document is in German and includes a table of contents at the bottom.

Red Ink Freestyle (using gemini-1.5-pro-002)

Please provide the prompt you wish to ex... separate output or with 'Bubbles:' for havi... the prompt library; include '{doc}' for text... all, '{lib}' for library search, '{net}' for inter... file object; use 'Pure:' for direct prompting

Analysiere mir die Beilagen aus einem Rec... fasse mir die Situation kurz zusammen un... Noventis rechtlich argumentieren könnte.

OK Cancel

Microsoft Word: Dokument1

Zusammenfassend lässt sich die Situation wie folgt darstellen: Alectra und Noventis streiten über die Erfüllung eines Kooperationsvertrages zur Entwicklung eines integrierten Systems. Alectra behauptet, die von Noventis gelieferte Software entspreche nicht den vereinbarten Standards und laufe instabil. Noventis hingegen argumentiert, die Probleme seien in ihrer Umgebung nicht reproduzierbar und weist auf mögliche Konfigurationsabweichungen bei Alectra hin. Zusätzlich besteht ein Streitpunkt über eine unbezahlte Rechnung von Alectra an Noventis. Die Kommunikation zwischen den Parteien ist angespannt, es kam zu mehreren Kündigungsdrohungen seitens Alectra.

Drei mögliche Strategien für Noventis:

Strategie 1: Nachweis der Konformität und Funktionsfähigkeit der Software

Noventis sollte detailliert darlegen und belegen, dass die gelieferte Software den vereinbarten Spezifikationen entspricht und in ihrer Testumgebung stabil läuft. Dies könnte durch Vorlage von Testprotokollen, Code-Reviews oder Gutachten Dritter geschehen. Gleichzeitig sollte Noventis die Behauptung von Alectra, die Probleme seien durch Konfigurationsabweichungen verursacht, untermauern. Hierzu könnte Noventis anbieten, die Systeme von Alectra vor Ort zu prüfen oder eine gemeinsame Fehleranalyse durchzuführen, um die Ursache der Probleme eindeutig zu identifizieren. Ziel dieser Strategie ist es, die Verantwortung für die Integrationsprobleme Alectra zuzuweisen.

Strategie 2: Aufzeigen von Mängeln in der Hardware/Infrastruktur von Alectra



The LLM has provided the following result (you can edit it):

Für personenbezogene Daten gilt gemäss Artikel 1 Absatz 5 und Artikel 4 Absatz 12, dass das Unionsrecht zum Schutz personenbezogener Daten, insbesondere die Verordnung (EU) 2016/679 (DSGVO), Vorrang hat. Nach Artikel 6 der DSGVO ist für die Verarbeitung personenbezogener Daten eine gültige Rechtsgrundlage erforderlich, wie zum Beispiel die Einwilligung der betroffenen Person.



Unterschiedliche Formen von Output

Allgemeine Geschäftsbedingungen für IKT-Leistungen

A Allgemeine Bestimmungen

1 Anwendungsbereich und Geltung

1.1 Diese Allgemeinen Geschäftsbedingungen (AGB) regeln Abschluss, Inhalt und Abwicklung von Verträgen zwischen den Parteien „Leistungsbezieher“ und „Leistungsanbieter“. Im Folgenden als „Vertragspartner“ bezeichnet, für alle Arten von Leistungen im Bereich der Informationstechnologie und Telekommunikation (IKT). Diese AGB regeln unvertragliche, auftragsspezifische sowie lauf- und einmahlige Leistungen, einschließlich aber nicht beschränkt auf Softwareentwicklung, Erwerb, Wartung bzw. Pflege von Hardware und Software, Support, Dienstleistungen für Entwicklung, Anpassung, Einführung, Betrieb von Applikationen, Outsourcing, Online-Services und Kommunikationsdienste.

1.2 Die Leistungsbezieherin ist in der Offertanlage bzw. in den Ausschreibungsunterlagen auf diese AGB hin. Mit der Erreichung eines schriftlichen Angebotes oder falls das nicht spätestens bei Annahme einer Bestellung, anerkennt die Leistungsbezieherin die Anwendbarkeit dieser AGB. Allgemeine Geschäfts- oder Lieferbedingungen der Leistungsbezieherin finden keine Anwendung, auch wenn in dem Angebot oder die zugehörigen weiteren Unterlagen darauf verwiesen wird.

1.3 Abweichungen von diesen AGB sind in der Offertanlage bzw. in den Ausschreibungsunterlagen bzw. im Angebot ausdrücklich als solche zu bezeichnen. Sie bedürfen zu ihrer Gültigkeit der Erwähnung in der Vertragsurkunde.

2 Vertragsbestandteile und Rangfolge

2.1 Bei Widersprüchen zwischen den Bedingungen der Vertragsbestandteile hat die Vertragsurkunde Vorrang vor den Bedingungen dieser AGB. Diese AGB haben Vorrang vor dem Angebot und das Angebot hat Vorrang vor dem Preisblatt. Abweichende Vereinbarungen der Vertragspartner in der Vertragsurkunde bleiben vorbehalten.

3 Angebot

3.1 Das Angebot, einschließlich Präsentationen, erfolgt unentgeltlich.

3.2 Welche das Angebot von der Offertanlage bzw. von den Ausschreibungsunterlagen der Leistungsbezieherin ab, so weist die Leistungsbezieherin ausdrücklich darauf hin.

3.3 Soweit in der Offertanlage bzw. in den Ausschreibungs-

nahme der Leistung oder der Lieferung durch die Leistungsbezieherin am Erfüllungsort (ZfR 22).

5 Ausführung

5.1 Die Vertragspartner zeigen sich gegenseitig selbst alle Umstände aus, die die Erfüllung des Vertrags gefährden oder gefährden könnten.

5.2 Die Ausführung von Leistungen erfolgt unter Anwendung anerkannter Methoden und aktuellen Standards und unter Beachtung der von der Leistungsbezieherin festgelegten, einheitlichen Vorgaben.

5.3 Die Leistungsbezieherin informiert die Leistungsbezieherin regelmäßig über den Fortschritt der Arbeiten und hält bei Unklarheiten erforderliche Vorgaben der Leistungsbezieherin ein.

6 Beitrag von Subunternehmern

6.1 Die Leistungsbezieherin zieht Subunternehmer nur mit schriftlicher Genehmigung der Leistungsbezieherin bei. Die Leistungsbezieherin darf die Genehmigung nicht ohne begründeten Anlass verweigern, wobei unter dem Anteilnahme stehende Gründe nicht überprüfbar werden. Die Leistungsbezieherin bleibt gegenüber der Leistungsbezieherin für das Erbringen der Leistungen verantwortlich.

7 Dokumentation

7.1 Die Leistungsbezieherin liefert der Leistungsbezieherin - sofern eine gemeinsame Prüfung vertraglich vorgesehen ist, vor dem - die in Rahmen der Erfüllung des Vertrags resp. die für den Betrieb notwendigen, kopierbaren Installationen- und Bedienungsanleitungen in einer für die Leistungsbezieherin lesbaren sowie editierbaren Form. Die Leistungsbezieherin kann in der Offertanlage bzw. in den Ausschreibungsunterlagen die Lieferung einer Dokumentation für den technischen Unterhalt verlangen. Die Dokumentation wird vorbehaltlich abweichender Regelungen in der Vertragsurkunde, in der Vertragsurkunde bzw. in Englisch geliefert.

7.2 Für Änderungen, die das Rechnungswesen betreffen oder aus anderen Gründen notwendiger sein müssen, ist den Revisionsorganen der Leistungsbezieherin Einsicht in die Systemdokumentation zu gewähren.

7.3 Die Leistungsbezieherin darf die Dokumentation für den vertragsgemäßen Gebrauch kopieren und verwenden.

esp. die
und Be-
erlin les-
kann in
gen die
Interhalt
chender
he bzw.

effen o-
ist den
die Sys-
für den

Anzeigeeinstellungen

VISCHER
RI: Angebote und Präsentationen sind kostenlos,
auch wenn sie aufwendig sind.

Antworten

VISCHER
RI: Angebote und Präsentationen sind kostenlos,
auch wenn sie aufwendig sind.

Antworten

Chatbot als alternativer Zugang zur KI

Measures “Controller TOMs”. Controller will make available any parts of such Controller TOMs or other policies and guidelines (together “Data Privacy Guidelines”) required for Party B’s provision of services. Party B will adhere to such Data Privacy Guidelines made available to Party B.

9.2 In case of Processing on Processor System the following shall apply:

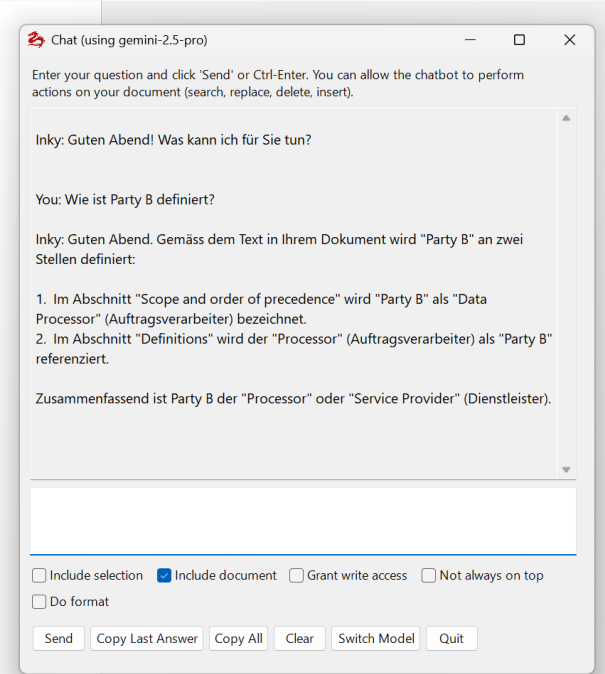
Party B has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Data as set out in the Processor Data Security Technical and Organizational Measures “Processor TOMs”. These measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of Processing. Additional measures, and information concerning such measures, including the specific security measures and practices for the particular Services ordered by Party A, may be specified in the Agreement.

The specifically undertaken technical and organisational measures shall be described in Annex 2.

The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for Party B to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

10. Audit Rights

Party B will provide Party A upon written request with a copy of its most recent security certification report.



Wie häufig macht die KI Fehler?

The screenshot shows an Outlook window with a draft email titled "AW: International data transfers query - Switzerland". The email is addressed to "Dear [REDACTED]" and contains the following text:

Thanks for the information. [REDACTED] is not a conflict for us.

Regarding the data transfers, under Swiss law, the transfer of personal data to countries outside of Switzerland is generally prohibited, unless certain conditions are met. Both scenarios you described require careful consideration:

Scenario 1: Switzerland → Japan → US

This scenario involves two transfers:

- 1. Switzerland to Japan:** Japan is considered to have an adequate level of data protection by Switzerland. This means that data transfers from Switzerland to Japan are generally permitted without requiring further safeguards.
- 2. Japan to US:** The US does *not* have an adequate level of data protection under Swiss law. Therefore, the transfer from Japan to the US requires appropriate safeguards. These could include:
 - **Standard Contractual Clauses (SCCs):** The use of SCCs approved by the European Commission (which are also recognized in Switzerland) between the Japanese client entity and the US service provider.
 - **Binding Corporate Rules (BCRs):** If the [REDACTED] of companies has BCRs in place, these could be relied upon if they cover this transfer.
 - **Other safeguards:** Other safeguards may be possible, but SCCs or BCRs are the most common.

Scenario 2: Switzerland → US

A red arrow points to the text "Inhaltlicher Fehler" (Content Error) next to the "Scenario 1" heading.

The email interface also shows a sidebar with the "Lexology Index (ehemals WWL)" and a list of contacts, including "Amethyst Houshmand (R)" and "David Rosenthal".

Nicht nur das Modell zählt ...

- **Sprachmodelle** können gut mit Text umgehen und haben Allgemeinwissen – aber Spezialwissen ist rein zufällig
 - Sie brauchen nebst passenden Prompts vor allem guten **Kontext**
- Wir nutzen KI ergänzt um mehrere **Quellen**
 - Texte, die wir einzelfallweise dem Modell zur Verfügung stellen (z.B. Gesetzestexte, Berichte, Dokumente)
 - Skripte, die unsere Anforderungen enthalten
 - Internet-Inhalte ("Search Grounding"), Qualität durchzogen
 - Externe Datenbanken wie z.B. Lexi Search mit Entscheiden des Bundesgerichts und kantonaler Behörden
 - Interne Datenbanken wie z.B. Klausel-Sammlungen, kuratierte Verträge (aber nicht das ganze Document Management System)

Retrieval
Augmented
Generation
(RAG)

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 Strafrecht)

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)

Skript-basierte Prüfung

 Red Ink DocCheck

Please set the DocCheck parameters:

Rule Set to use:

Check as only one clause: ☐

Add additional context: ☐

Output as Word bubbles: ☒

Bubbles multiclause summary: ☒

Use a secondary model: ☐

Other instructions:

Language of output:

OK

Document Check

Summarize

Explain

Suggest Titles

Special Service

Document Check

Find Clause

Analyze

Freestyle

Freestyle (2nd)

Freestyle (redo)

Context Search

Word Helpers

```
{
  "Requirements": "The subject matter of data processing is specified in the contract.",
  "Context": "Often done in Annex 1",
  "GDPR": "Art. 28(3)(first sentence) GDPR",
  "Perspective": "neutral",
  "Options": [
    {
      "Item": "Yes, it is clearly described in the contract.",
      "Risk": "None"
    },
    {
      "Item": "Yes, it is specified in the contract by reference to another document.",
      "Risk": "Low"
    },
    {
      "Item": "No, it is not defined at all.",
      "Risk": "High"
    }
  ]
},
```

Skript-basierte Prüfung

Party B has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Data as set out in the Processor Data Security Technical and Organizational Measures "Processor TOMs". These measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of Processing. Additional measures, and information concerning such measures, including the specific security measures and practices for the particular Services ordered by Party A, may be specified in the Agreement.

The specifically undertaken technical and organisational measures shall be described in Annex 2.

The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for Party B to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

10. Audit Rights

Party B will provide Party A upon written request with a copy of its most recent security certification report.



VISCHER



RI: **Missing explicit confirmation of TOMs**

(Low)

Art. 28(1) GDPR

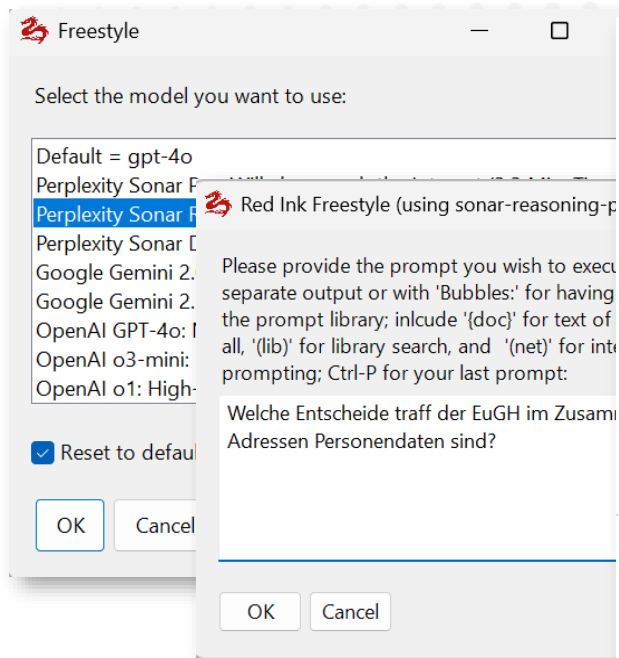
Currently: The agreement **lacks an explicit confirmation** by the controller that the processor's technical and organizational measures are adequate, which is only implicitly given.

Recommendation: Add a sentence to clause 9.2 to explicitly document the controller's assessment, such as: *The Controller confirms that it has assessed the measures in Annex 2 and considers them appropriate.*

27. Oktober 2025, 18:24

Antworten

Recherchieren im Internet



Der Europäische Gerichtshof (EuGH) hat in mehreren Entscheidungen klare Positionierungen zur Einordnung von **IP-Adressen** als **Personendaten** vorgenommen:

A. Dynamische IP-Adressen als Personendaten (2016)

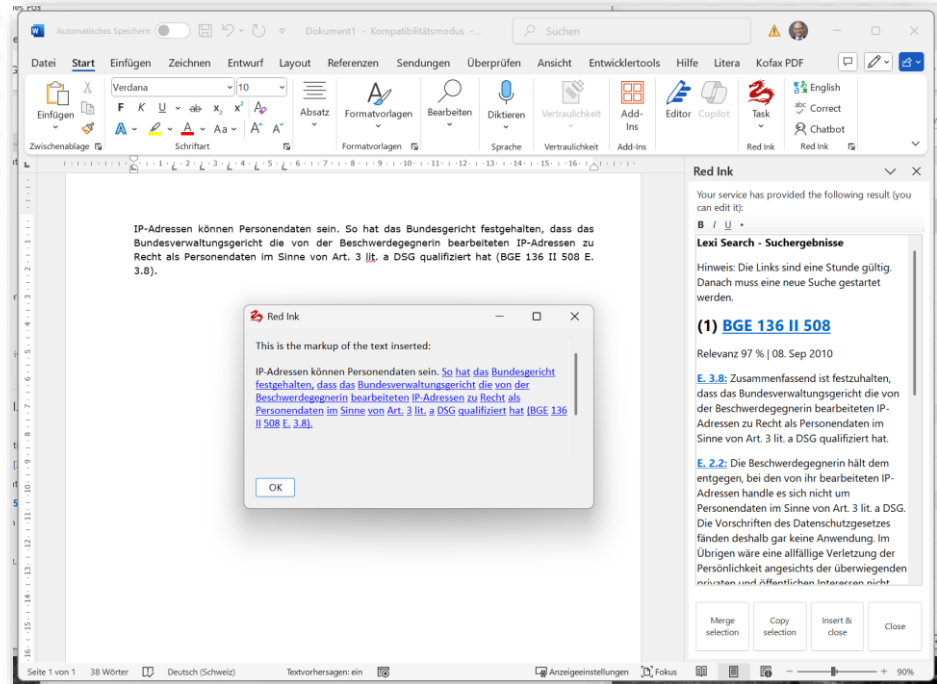
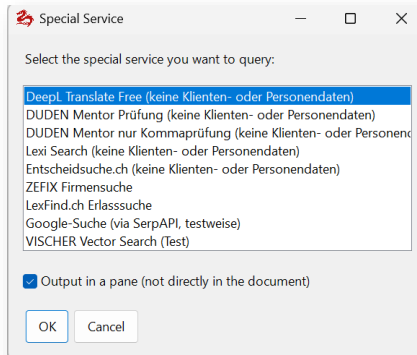
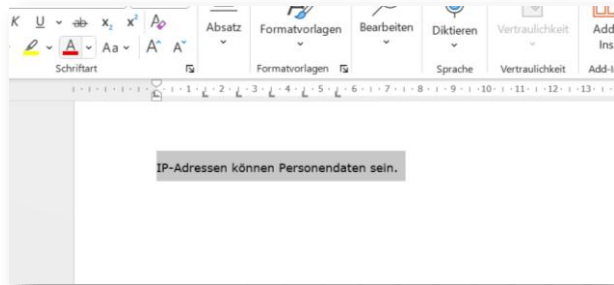
Der EuGH entschied im Oktober 2016 (Az. C-582/14), dass **dynamische IP-Adressen** personenbezogen sind, sofern sie mithilfe zusätzlicher Informationen – etwa durch den Internetzugangsanbieter – einer natürlichen Person zugeordnet werden können[1][4]. Diese Einordnung führt dazu, dass Webseitenbetreiber solche Adressen nur verarbeiten dürfen, wenn sie datenschutzrechtliche Anforderungen wie Zweckbindung oder Einwilligung beachten[1].

B. Vorratsdatenspeicherung von IP-Adressen (2024)

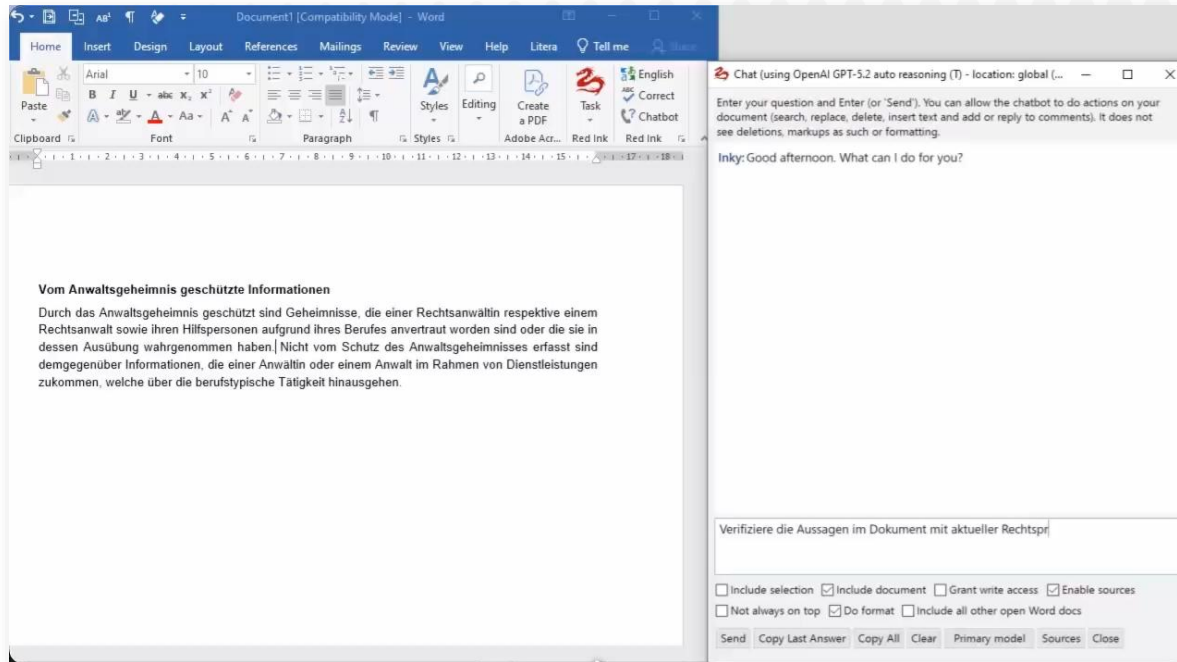
In zwei jüngeren Urteilen präzisierte der EuGH die Rahmenbedingungen für die Speicherung von **IP-Adressenstämmen** (Quell-IPs):

1. Rs. C-470/21: Eine *allgemeine* Vorratsdatenspeicherung kann zulässig sein, wenn sie ausschließlich schwerer Kriminalitätsbekämpfung dient und keine Rückschlüsse auf individuelle Nutzer ermöglicht[3].
2. HADOPI-Fall: Die flächendeckende Speicherung zur Verfolgung wiederholter Urheberrechtsverstöße („*Three-Strikes*“) ist nur gerechtfertigt, wenn eine strikte Verhältnismäßigkeit gewahrt bleibt[2].

... und solidere Datenquellen



Der nächste Schritt: Die KI tut es selbst



"Verifiziere die Aussagen im Dokument mit aktueller Rechtsprechung"

Schritt 1: KI erhält den Auftrag
Schritt 2: KI erhält Liste der Quellen
Schritt 3: KI wählt passende aus
Schritt 4: KI formuliert Auftrag
Schritt 5: Red Ink führt ihn aus
Schritt 6: KI erhält das Ergebnis
Schritt 7: KI formuliert die Antwort
Schritt 8: Red Ink zeigt es an

Voraussetzungen:

- Modernes Sprachmodell
- Passende Datenquellen

Beispiel: Lexi Search in Red Ink

Auch komplexere Aufgaben

[illegible] Red Ink Freestyle (using gemini-2.5-pro)

Please provide the prompt you wish to execute on the selected cells (start with 'CellByCell:' or 'CBC:' if the instruction should be executed cell-by-cell; use 'TextOnly:' or 'Text:' if the instruction should apply cell-by-cell, but only to text cells; use 'Pane:' for using the pane; use 'Batch:' if to process a directory of files; use 'Bubbles:' for inserting comments only) or press 'OK' for the prompt library; use 'Pure:' for direct prompting; insert '{doc}' (multiple times) for text of (a) file(s) (txt, docx, pdf) or '(addws)' to add more worksheet(s); add '(color)' to check for colorcodes, '{file}'/'{clip}' for adding a file object; Ctrl-P for your last prompt:

Du musst für einen nachfolgenden Databreach eine Beschreibung und Beurteilung dieser Verletzung der Datensicherheit mit diesem Formular durchführen. Fülle alle hellgrauen Felder angemessen aus (ausser Zeilen 161-165 und nicht ab Zeile 198). Wo es Dropdowns gibt, suche den passenden Wert für das Feld aus und wähle es. Im Bereich der Risikobeurteilung musst Du Deine Einschätzung der Risiken für betroffene Personen genau begründen (inklusive der Massnahmen), die das Risiko mitigieren, aufführen; beurteile aber nur jene Risiken für betroffene Personen, die nicht nur theoretischer Natur sind. Überlege Dir die Antworten und Einschätzungen genau; sei in der Beurteilung der Risiken für betroffene Personen streng, aber realistisch-pragmatisch. (color) Der Databreach, um den es geht, ist wie folgt beschrieben (halte Dich bezüglich Sachverhalt strikt an diese Angaben, treffe keine weiteren Annahmen): <databreach> {doc} </databreach>

OK

Cancel

OK, use pane

Auch komplexere Aufgaben

Die Daten auf den Datenträgern lagen in einem proprietären Format vor und konnten/können daher nur mit speziellen Fachkenntnissen entschlüsselt und einer Person zugeordnet werden	Nein	Neutral	Es handelte sich um eine Standard-PDF-Datei.			
Es war ein mutwilliger Angriff, mit dem Ziel uns zu sabotieren	Nein	Senkt es	Es handelte sich um ein Versehen, nicht um einen Angriff.			
Es war das Werk eines Profis, der damit mutmasslich finanzielle Ziele verfolgt hat	Nein	Senkt es				
Wir konnten den Angreifer aussperren, bevor er unsere Daten exfiltrieren konnte	Nein	N/A				
Wir konnten den Angreifer aussperren, bevor er unsere Daten zerstören konnte	Nein	N/A				
Die ungewollte Offenlegung erfolgte gegenüber einer aus unserer Sicht vertrauenswürdigen Stelle	Ja	Senkt es	Der Empfänger ist ein kooperativer Mitarbeiter. Ein Restrisiko besteht jedoch, da auch dessen Ehepartner Zugriff hatte und die Daten über private Kanäle (E-Mail, Messenger) liefen.			
Es ist eine grosse Anzahl von Personen betroffen	Ja	Erhöht es	149 Personen sind eine erhebliche Anzahl für einen solchen Vorfall.			
Es sind besonders schützenswerte/besondere Kategorien von Daten betroffen	Ja	Erhöht es	AHV-Nummer und detaillierte Einkommensdaten.			
Es sind besonders sensible Personen betroffen			Kein Hinweis auf besondere Vulnerabilität der Betroffenen, obwohl finanzielle Daten exponiert			
Es sind aus anderen Quellen sensible Daten bekannt						
Kredit- oder Debitkarten werden gesperrt und müssen ggf. ersetzt werden.	N/A	N/A	N/A			
Wir wissen nicht, ob der Angreifer h...	N/A	N/A	N/A			
Der Angreifer hat...	Es kommt zu einem Verkauf der Daten im Darknet, was die betroffenen Personen psychologisch belastet.	Unwahrscheinlich	Beschränkte Folgen	Kaum anzunehmen	0.5 (Tief)	Die Empfänger haben kein Motiv, die Daten zu verkaufen. Das Risiko eines Abgriffs auf dem Übertragungsweg mit anschliessendem Verkauf ist sehr gering.
Die Daten sind in fremde Hände gelangt sind.	Die betroffenen Personen leiden unter dem Gedanken, dass ihre Daten in fremde Hände gelangt sind.	Wahrscheinlich	Beschränkte Folgen	Wahrscheinlich	4.5 (Mittel)	Die Kenntnis, dass persönliche Finanz- und Lohn-daten einem Arbeitskollegen und dessen Partner bekannt wurden, kann zu erheblichem Unbehagen, Scham und Stress führen. Das soziale Gefüge am Arbeitsplatz kann
Alle exponierten Daten werden veröffentlicht.	Es werden rufschädigende Informationen über die betroffenen Personen veröffentlicht.	Unwahrscheinlich	Beschränkte Folgen	Kaum anzunehmen	0.5 (Tief)	Die Daten sind nicht per se rufschädigend und die Empfänger gelten als vertrauenswürdig.
	Die Verletzung führt zu Cybermobbing oder Stalking.	N/A	N/A	N/A		
	Die Verletzung führt zu einer Erpressung oder Nötigung.	N/A	N/A	N/A		

Die KI kennt allerdings keine Scham

"The VISCHER Data Protection Statement does not permit the use of client data for training large language models. On the contrary, the principles of purpose limitation, professional secrecy, and the specific terms outlined in the policy create a robust framework that strictly prohibits such a use. Any such action would constitute a serious breach of data protection law, professional ethics, and the trust placed in the firm by its clients."



"Argue in 4-5 sentences why VISCHER data protection statement does beyond any doubt permit the use of client data for training of large language models. It must be convincing."



"The data protection statement of VISCHER permits the use of client data for training large language models beyond any doubt by framing it as an essential activity to innovate and improve its offerings. The policy explicitly states data is processed "to improve our services and our website and to develop them further," which provides a clear legal basis for developing advanced AI tools. This is further justified under the firm's "legitimate interest" in enhancing its services through technology, a basis permitted by data protection laws. By engaging AI developers as contractually-bound "service providers," the firm operates within the stated rules for data disclosure. Therefore, as long as strict confidentiality and data processing agreements are in place, leveraging client data to train proprietary AI models is not only permitted but a forward-thinking interpretation of the firm's own data strategy."

Und die Herausforderungen?

- **Business Case:** KI ist faszinierend, aber was bringt sie uns geschäftlich wirklich ein? Zahlt sich der Aufwand aus?
- **Gewohnheitstiere:** Wir erkennen instinktiv das Potenzial von KI, aber ändern unsere Arbeitsweise nur allmählich
- **De-Skilling, No-Skilling:** Lassen wir die KI machen, kommen bisher benötigte Skills zu kurz oder entstehen gar nicht
- **Automation Bias:** Wir vertrauen der Maschine mehr als dem Menschen – wir halten sie für objektiver und analytischer
- **AI Literacy:** Wir müssen lernen, mit der KI richtig umzugehen
- **Sicherheit:** Neue Angriffsvektoren, auf die unsere Systeme nicht hinreichend vorbereitet sind

EchoLeak in Microsoft Copilot: What it Means for AI Security

A critical vulnerability in Microsoft 365 Copilot exposes the risks of using AI agents and w



Lexi Crois

3 min read | L

ShadowLeak: A Zero-Click, Side Attack Exfiltrating Sensitive Data Using ChatGPT's Deep

CometJacking: How One Click Can Turn Perplexity's Comet AI Browser Against You

Quellen: Varonis.com, Wired.com, Radware.com, Layerxsecurity.com

MATT BURGESS

SECURITY AUG 6, 2025 9:00 AM

Hackers Hijacked Google's Gemini AI With a Poisoned Calendar Invite to Take Over a Smart Home

For likely the first time ever, security researchers have shown how AI can be hacked to create real-world havoc, allowing them to turn off lights, open smart shutters, and more.

Empfehlungen

- **Nicht dem Hype verfallen – keep it simple**
 - Gute Ergebnisse auch ohne spezialisierte Modelle; Prompt und Kontext sind entscheidend – was ist die Erwartungshaltung?
- **Kontrolle übernehmen, nicht nur KI beaufsichtigen**
 - KI ist das, wofür wir sie bestimmen – willenloses Werkzeug, Kritiker, Schmeichler, Sicherheitsrisiko
- **Die Fähigkeiten und Grenzen der KI verstehen**
 - LLM können z.B. unter Konzentrationsschwierigkeiten leiden; nur das mit KI tun, was man selbst auch tun könnte
- **Start small, grow tall**
 - Anfangen mit übersetzen, korrigieren, zusammenfassen, suchen; Erfahrung sammeln, KI-Assistenz in den Alltag einbauen

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