

# VISCHER

KI-Tools.

Womit darf im Unternehmen gearbeitet werden?

David Rosenthal, Jonas Baeriswyl, VISCHER AG  
17. März 2026

---

## Zunächst einmal dies ...

### **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."

Nutzt ein Angreifer die eigene Anthropic API zur Exfiltration von Daten, wird der Angriff nicht bemerkt

## Nach wie vor viele Sicherheitsrisiken

Sources: Varonis.com, Wired.com, Radware.com, Layerxsecurity.com, Thehackernews.com

### EchoLeak in Microsoft Copilot: V it Means for AI Security

MATT BURGESS

SECURITY AUG 6, 2025 9:00 AM

A critical vulnerability in Micro  
AI agents and why a data-cent

ShadowLeak: A Zero-

### Hackers Hijacked Google's Gemini AI With a Poisoned

### Take Over a



Lexi Cr

### Researchers Reveal Reprompt Attack Allowing Single- Click Data Exfiltration From Microsoft Copilot

### Come

by Ravie Lakshmanan Jan 15, 2026

### Can Turn Perplexity's Comet AI Browser Against You

laor U.

shown how AI can be hacked to create real-world  
havoc, allowing them to turn off lights, open smart  
shutters, and more.

## Rechtliche Grundlagen (Standardfall)



\* Foreign Lawful Access Risk Assessment

## 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.

## 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 Berufseigennutzen selbst unterstehen und dieses strikte einzuhalten haben. Anwältinnen und Anwälte stellen im Übrigen die Einhaltung der Berufsregeln, insbesondere des Berufseigennutzes, sicher.

• Swiss Banking

- Swiss Banking

Die Speicherung und sonstige Bearbeitung von Informationen unterstehen, kann beim Betreiber von entsprechenden Anwendungen (Applikationen) für die Mandatspflicht sichergestellt ist, dass die Datensicherheit gemäss dem Zugang zu den Informationen nur unter Wahrung des Berufsgeheimnisses möglich ist. Das wird bei ausserhalb der Cloudlösungen mit Datenspeicherung und -bearbeitung und im Vereinigten Königreich vermutet.

## Cloud-Leitfaden

## Schweizer Standesregeln der Rechtsanwälte (SSR)

Cloud-Leitfaden der  
Schweizerischen  
Bankiervereinigung

November 2025  
Leitfaden der SBVg  
3. Auflage

Es darf kein Grund zur Annahme bestehen, dass es zu einem ausländischen Behördenzugriff kommt

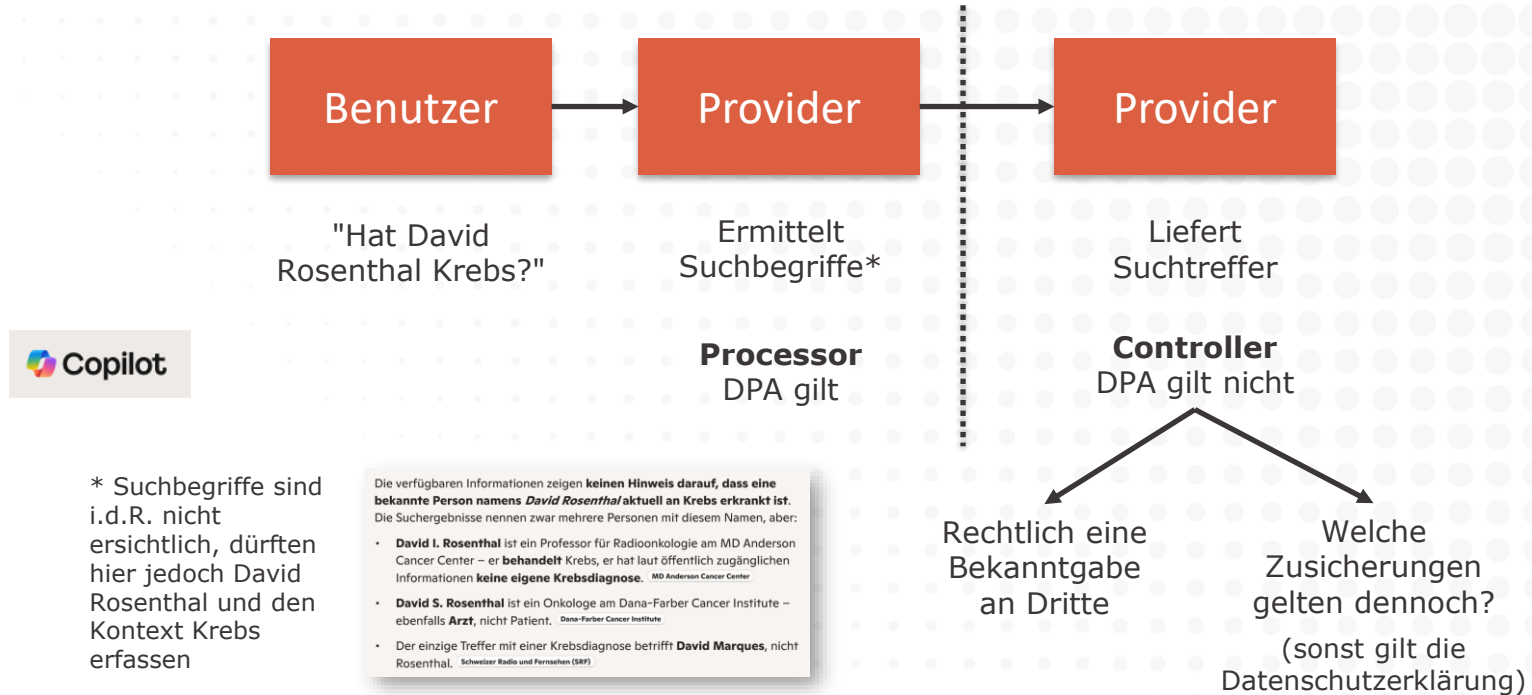
- Die Berechnung des Risikos eines ausländischen "Lawful Access" erscheint nach Ansicht der Staatsanwaltschaft grundsätzlich ein geeignetes Kriterium, um die Vertretbarkeit der Auslagerung auch vor einem strafrechtlichen Hintergrund zu beurteilen. Eine Überprüfung des Ergebnisses im konkreten Fall ist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

vischerlnk.com/4ck2J0L

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

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

# Rechtliche Grundlagen (Sonderfall)



# Microsoft 365 Copilot / 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 re [Product Terms](#) [more](#)

## 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 used for any other purpose.
- Query Data is not used for any other purpose.
- Query Data is not used for any other purpose.
- Query Data is not used for any other purpose.

## Bing

When Bing is optionally available through an Online Service, as disclosed in the product documentation, use of Bing by end users is governed by the Microsoft Services Agreement (<https://www.microsoft.com/servicesagreement/>), the Microsoft Privacy Statement (<https://privacy.microsoft.com/privacystatement>), the Microsoft Bing Maps and Embedded Maps Service Terms of Use (<https://www.bingmapsportal.com/terms/EndUserTerms>), except that noncommercial use limitations in those terms do not apply to Products available for a fee through Microsoft volume license. The Data Protection Addendum does not apply to use of Bing function

Bing

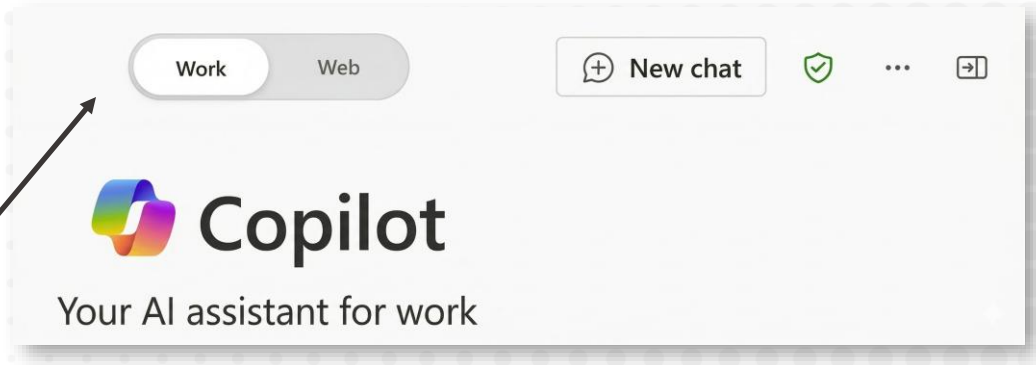
The Data Protection Addendum does not apply to Bing Search Services or to any use of Bing within a Product. For any component of a Product that is powered by Bing, as disclosed in the product documentation, the Microsoft Privacy Statement (<https://privacy.microsoft.com/privacystatement>) applies.

**Manche Organisationen untersagen darum Personendaten bei der Web-Suche**

## Microsoft 365 Copilot / Bing

Konfiguration  
regelmässig kontrollieren:

Wurde die Web-Suche automatisch  
wieder aktiviert?



je nach Konfiguration sind Web-Zugriffe  
auch im Work-Modus möglich

# Microsoft Azure – Grounding mit Bing Search

## Grounding with Bing Search

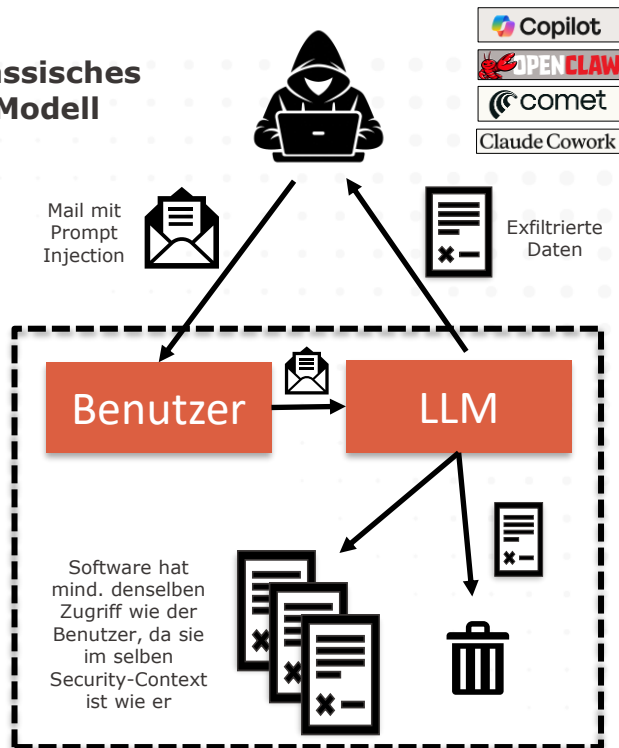
When Customer uses Grounding with Bing Search and/or Grounding with Bing Custom Search (including use of Web Knowledge Source), Customer's use will be of a **First-Party Consumption Service** governed by the terms at <https://www.microsoft.com/bing/apis/grounding-legal-enterprise>.

### Section 4. Data collection and privacy

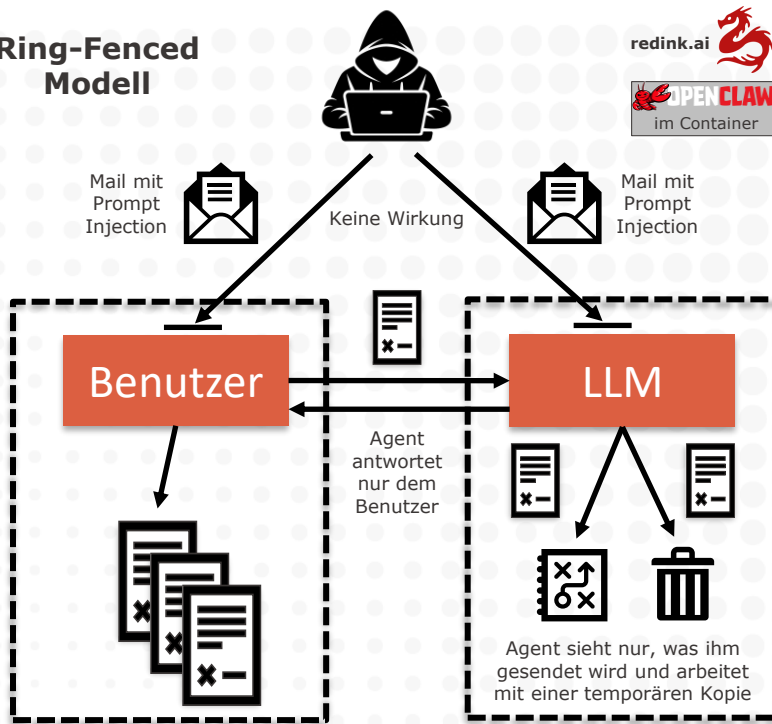
- (a) Microsoft may collect information from Customer or End Users such as, but not limited to, an End User's IP address, requests, time of submissions and the results returned to the End User, in connection with transaction requests to the Services. All access to and use of the Services, including Microsoft's processing of Bing Search Services Data, is subject to the data practices set forth in the then-current Microsoft Privacy Statement, a current copy of which is available at <https://privacy.microsoft.com/en-us/privacystatement>. Customer must prominently include a functional hyperlink to the [Microsoft Privacy Statement](#) in the Customer Solution's End User terms of use. Customer must label the hyperlink Microsoft Privacy Statement.
- (b) Bing Search Services Data and Bing Services Output are not Customer Data, as defined in the Customer Agreement. The Privacy and Security Terms of the Microsoft Product Terms do not apply to the Services. The terms for Microsoft's processing, storage and use of Bing Search Services Data and Output are solely set forth in the Privacy Statement. As between Microsoft and Customer, Microsoft does not claim any ownership rights to the Outputs. Customer acknowledges that the Outputs may contain third-party content and that Microsoft does not assign any rights to the Outputs on behalf of any third party.
- (c) With respect to any personal data subject to the European Union General Data Protection Regulation (GDPR) and that is processed in connection with Customer's use of the Services, Customer understands that Customer and Microsoft are independent data controllers under the GDPR. Customer is independently responsible for its compliance with the GDPR. Microsoft is not Customer's data processor with respect to the Services.
- (d) Customer acknowledges and agrees that the Services are excluded from the Microsoft Products and Services Data Protection Addendum.

## Agenten ...

## Klassisches Modell

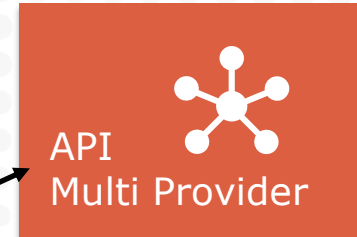


## Ring-Fenced Modell



## Wie Zugang erhalten zu KI?

- **Browser** (typischerweise Chatbot)
  - ChatGPT, Copilot, Claude, OpenWebUI, Red Ink, Google AI Mode, die meisten Legal Tech-Angebote
- **Integration in Office-Anwendung** (via Add-in)
  - Copilot, Red Ink, Google Workspace
- **KI-Browser**
  - Comet, Atlas
- **KI-Desktop-Software**
  - Claude Code, Claude Cowork, OpenClaw, Jan
- **Integriert in Geschäftsanwendung**
  - Salesforce, Slack, Hubspot, etc.



Application Programming  
Interface = direkter  
Zugang zum Modell für  
die Software



Model Context Protocol =  
Verfahren, mit dem eine  
KI-Lösung Datenquellen  
erkunden kann

## KI-Provider in der Cloud

- **Microsoft** (GPT-Modelle, tw. andere; Chatbot, Add-in, API)
  - Modelle in Europa, Vertrag mit Berufsgeheimniszusatz verfügbar
  - Kein Abuse Monitoring bei Copilot; Opt-out bei API nur für wenige
  - Kein ADV bei Search Grounding in Bing; "EU Data Boundary"
- **Google** (Gemini, Anthropic u.a.; Chatbot, Add-in, API)
  - Modelle in Europa, Vertrag mit Berufsgeheimniszusatz verfügbar
  - Abuse Monitoring Opt-out/ZDR bei API für Berufsgeheimnis
  - Search Grounding verschieden geregelt; Data Residency
- **OpenAI** (GPT-Modelle; Chatbot, KI-Browser, API)
  - Geheimhaltungsklausel, aber kein Berufsgeheimniszusatz
  - Local Data Residency und ZDR nur für ausgewählte Kunden und Produkte

## KI-Provider in der Cloud

- **Anthropic** (Claude-Modelle; Chatbot, KI-Desktop-Software, API)
  - ADV und Geheimhaltung
  - Keine direkte Local Data Residency; kein Berufsgeheimniszusatz
- **Perplexity** (div. Modelle; Chatbot, KI-Browser, API)
  - ADV und Geheimhaltung ("Enterprise")
  - Speicherung in den USA, kein Berufsgeheimniszusatz
- **DeepL Pro** (Übersetzung, Schreibhilfe)
  - ADV und Geheimhaltung ("Pro")
  - Kein Berufsgeheimniszusatz
- **Spezialisierte Anbieter** (z.B. LegalTech-Provider)
  - Nutzen meist Cloud-Anbieter; Schutzniveau oft unklar

# KI-Provider in der Schweiz

- **Schweizer Provider** als Alternative zur KI via "US-Cloud"
  - Vertragszusatz zum Schutz des Berufsgeheimnisses für Schweizer KI-Provider publiziert ([vischerlnk.com/3IuUQLO](https://vischerlnk.com/3IuUQLO)) →
  - Zusagen dafür von **MTF, AlpineAI, SafeSwissCloud**; Details auf <https://redink.ai/api-providers/>
  - 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, werden aber immer besser (vor allem die offenen Modelle aus China, wie Qwen 3.5, Kimi K2.5, DeepSeek V3.2)
- **Alternative:** Self-hosted LLM (lokal betriebenes KI-Modell)
  - Realistischerweise CHF 20k plus CHF 500/Monat (z.B. [onprem.ai](https://onprem.ai))



© 2004 Blackwell Publishing Ltd *Journal of Internal Medicine* 255: 103–110

[illegible]

\* Für Nutzer im Europäischen Wirtschaftsraum, in der Schweiz oder im Vereinigten Königreich gelten beim kostenlosen Angebot von Google AI Studio die gleichen Bedingungen bezüglich Nutzung der Daten durch Google wie beim kostenpflichtigen Angebot. Achtung: Es dürfen nur kostenpflichtige Dienste verwendet werden, wenn APIs Clients für Nutzer im Europäischen Wirtschaftsraum, in der Schweiz oder im Vereinigten Königreich verfügbar gemacht werden.

## Was wir bei uns machen



<https://redink.ai>

- **Jeder** darf KI **mit allen Daten** nutzen (Sonderfälle vorbehalten)
  - Google Gemini-Modelle für Berufsgeheimnisdaten, ohne Web-Suche
  - OpenAI-Modelle (via OpenAI), Perplexity für weitere Zwecke (z.B. Recherchen)
  - Anthropic für Softwareentwicklung (aber nicht auf Bürosystemen)
  - DeepL Pro, HeyGen u.a. für Spezial-Anwendungen
- **Red Ink** als KI-Add-in für Word, Excel, Outlook und Edge
  - Zusätzlich: Agent für Aufträge per E-Mail ([inky@vischer.com](mailto:inky@vischer.com))
  - Klassische LegalTech-Lösungen für uns zu teuer, zu beschränkt, zu unsicher
- **Externe Datenquellen** wie z.B. LexiSearch (Red Ink recherchiert selbst)
- **Hohe "Adoption"** (70 Prozent) durch sehr niederschweligen Einstieg

- [illegible]

[vischerlnk.com/ki-weisung-kurz](https://vischerlnk.com/ki-weisung-kurz)

# VISCHER

## Danke für Ihre Aufmerksamkeit!

david.rosenthal@vischer.com, jonas.baeriswyl@vischer.com

### **Zürich**

Schützengasse 1  
Postfach  
8021 Zürich, Schweiz  
T +41 58 211 34 00

[www.vischer.com](http://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

Mehr Informationen:  
[www.vischer.com/ki](http://www.vischer.com/ki)