Partner White Paper zur sicheren KI-Nutzung

Ein zusätzlicher Mehrwert für Ihre Kunden. Ein pragmatischer Zusatzbaustein für Ihr Portfolio.

Sichere KI-Nutzung für Organisationen mit sensiblen Daten

Wenn Sie Kunden mit sensiblen Daten betreuen, ist sichere KI-Nutzung sehr wahrscheinlich bereits heute ein Thema in Ihrem Umfeld. Nicht zwingend als offizielles Projekt, aber oft bereits als praktische Realität im Arbeitsalltag.

Für viele Organisationen stellt sich damit eine zentrale Frage: Wie lässt sich die Nutzung externer KI-Systeme ergänzend zu bestehenden Lösungen wie Microsoft Copilot so gestalten, dass Produktivität, Vertraulichkeit und Nachvollziehbarkeit sinnvoll zusammenfinden?

Genau daraus entsteht für IT-Partner ein relevantes neues Thema.

Promptspace.ch unterstützt Sie dabei, Ihren Kunden eine kontrollierte und praxistaugliche Nutzung externer KI-Systeme zu ermöglichen, ohne deren bestehende Arbeitsweise grundlegend zu verändern. **PromptSpaceGuard** bildet dabei die browserbasierte Schutzschicht: Sensible Inhalte werden lokal erkannt und je nach Regelwerk blockiert oder pseudonymisiert, bevor sie das Unternehmen verlassen. Im Hintergrund werden die für Governance, Nachvollziehbarkeit und Administration relevanten Metadaten bereitgestellt.

So entsteht für Ihre Kunden ein realistischer Weg, um produktive KI-Nutzung besser mit Vertraulichkeit, Kontrolle und Nachvollziehbarkeit zu verbinden, und für Sie als IT-Partner ein Zusatzbaustein, der sich sinnvoll in bestehende Kundenbeziehungen und Leistungen einfügt.

Ausgangslage

Mit der zunehmenden Nutzung generativer KI im Arbeitsalltag entsteht bei vielen Organisationen mit sensiblen Daten ein neues Spannungsfeld. Einerseits möchten Mitarbeitende KI-Tools produktiv nutzen. Andererseits dürfen vertrauliche Inhalte nicht unkontrolliert an externe Systeme übermittelt werden.

Aktuelle Daten (KPMG, Netskope, Brynjolfsson, Forbes) aus 2025/2026 belegen diese Thematik:

- **48 %** der Mitarbeitenden nutzen KI entgegen den Richtlinien im Verborgenen.
- **22 %** der Uploads enthalten dabei hochsensible Daten wie Namen oder Beträge.
- **34 %** an Produktivität gehen durch Einschränkungen der Nutzung verloren.

Für IT-Partner ist das relevant, weil dieses Thema bei vielen Kunden bereits operativ vorhanden ist, auch wenn es noch nicht als offizielles Projekt geführt wird.

Problem

Viele Kunden möchten heute vom Effizienzpotenzial generativer KI-Modelle profitieren. Gleichzeitig stehen sie vor einem Spannungsfeld, das sich in der Praxis oft nur schwer auflösen lässt: Produktivitätswunsch, Vertraulichkeitsanforderungen und fehlende kontrollierte Nutzung.

Die Einführung von Microsoft Copilot ist für viele Organisationen ein wichtiger Schritt, löst diese Herausforderung jedoch nicht. Denn die tatsächliche Nutzung im Arbeitsalltag bleibt meistens breiter: Mitarbeitende greifen zusätzlich auf andere KI-Tools zurück, weil diese im Browser direkt verfügbar sind, bereits vertraut wirken oder für bestimmte Aufgaben als qualitativ besser, schneller oder einfacher wahrgenommen werden. So entsteht die Lücke zwischen offizieller Freigabe und realem Verhalten.

Fehlt dafür eine praxistaugliche Antwort, entstehen meist drei unerwünschte Zustände: KI wird informell genutzt, KI wird pauschal eingeschränkt oder Mitarbeitende weichen auf Grauzonenlösungen aus. Gerade bei Organisationen mit sensiblen Daten reicht es deshalb oft nicht, das Thema allein über Richtlinien, Awareness oder spätere Zielarchitekturen zu adressieren.

Hinzu kommt, dass Anforderungen an Transparenz, Dokumentation und verantwortbare KI-Nutzung an Gewicht gewinnen. Gleichzeitig steigt die Sensibilität für Drittstaaten- und Zugriffsrisiken, wenn vertrauliche Inhalte ungeschützt an externe KI-Anbieter übermittelt werden. Wer dieses Thema heute nicht aktiv angeht, überlässt es im Zweifel dem informellen Verhalten einzelner Mitarbeitender.

Lösung

PromptSpaceGuard setzt genau an dieser Stelle an. Die Lösung arbeitet als lokale Schutzschicht im Browser. Inhalte und Dokumente werden vor der Übermittlung an externe KI-Systeme geprüft und je nach Regelwerk pseudonymisiert. Nur die freigegebene und entsprechend verarbeitete Anfrage wird an das jeweilige KI-System weitergegeben. Im Hintergrund werden die für Betrieb, Konfiguration und Audit relevanten Metadaten bereitgestellt, ohne dass der Inhalt des Prompts gespeichert werden muss.

Für IT-Partner ist dieser Aufbau besonders relevant, weil sich PromptSpaceGuard als ergänzender Baustein in bestehende Kundenumgebungen einfügt, ohne die gewohnten KI-Oberflächen der Endkunden grundlegend zu verändern.

Nutzen für Ihre Kunden

Unser Ansatz schützt sensible Daten und ist modellagnostisch einsetzbar. So können gängige KI-Modelle genutzt werden, ohne ein ressourcenintensives IT-Projekt auszulösen.

- **Sicherheit:** Ihre Kunden schaffen die Voraussetzungen für einen sicheren Umgang mit KI, minimieren Schatten-KI und reduzieren das Risiko von Datenabflüssen.
- **Produktivität:** Ihre Kunden heben das Produktivitätspotenzial ihrer Mitarbeitenden und schaffen die Grundlage für eine kontrollierte KI-Nutzung im Alltag.
- **Technologie:** Mitarbeitende können in ihren gewohnten LLM-Umgebungen arbeiten und vom technologischen Fortschritt der jeweiligen Modelle profitieren.

Nutzen für Sie als IT-Partner

Promptspace hilft Ihnen, ein bei Ihren Kunden bereits vorhandenes Thema aktiv aufzugreifen und zusätzlichen Mehrwert zu schaffen, ohne neue Produkte oder Delivery-Strukturen aufzubauen.

- **Kundenmehrwert:** Promptspace ist besonders interessant bei Kunden, die sich bereits mit ChatGPT, Microsoft Copilot, Vertraulichkeit, Shadow-AI, kontrollierter KI-Nutzung oder regulatorischen Anforderungen wie dem EU AI Act und dem US CLOUD Act auseinandersetzen.
- **Portfolio-Ergänzung:** Promptspace ergänzt bestehende Leistungen in den Bereichen Cloud, Security, Modern Workplace und Managed Services, statt sie zu ersetzen.
- **Begrenzter Aufwand:** Wir begleiten die Einführung eng und persönlich.
- **Wirtschaftliches Potenzial:** Bei erfolgreicher Vermittlung profitieren Sie von einem attraktiven Referral-Bonus. Zusätzlicher Aufwand für Produktbetrieb oder Support entsteht für Ihr Team nicht.

Zusammenarbeit

Die Zusammenarbeit ist bewusst einfach aufgebaut. Sie bleiben gegenüber Ihren Kunden der vertraute Ansprechpartner, während Promptspace Einführung, Onboarding und Betrieb übernimmt.

- **Ihr Beitrag:** Sie identifizieren passende Kunden oder Situationen und empfehlen Promptspace bei Bedarf.
- **Unser Beitrag:** Wir übernehmen die weiteren Schritte, insbesondere Einordnung, Einführung, Onboarding und den laufenden Betrieb. Interessierte Kunden können die Lösung unverbindlich testen.

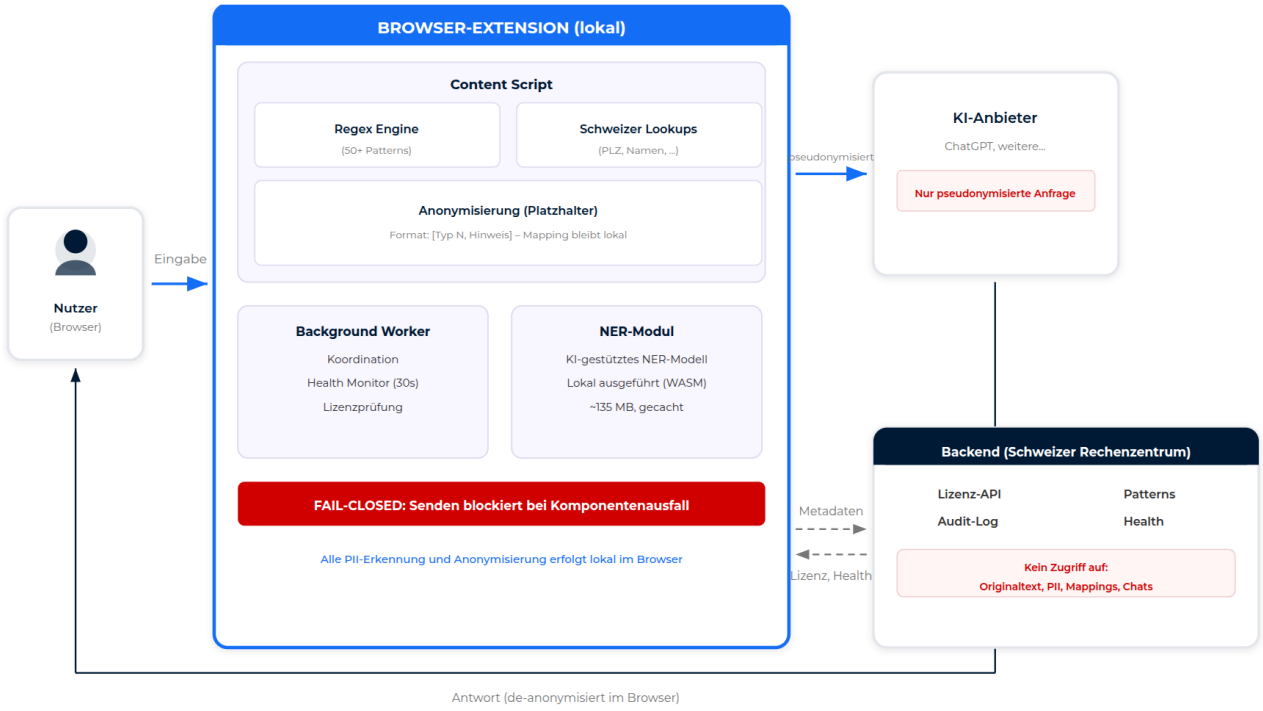
So schaffen Sie für Ihre Kunden einen professionell begleiteten Einstieg in die sichere KI-Nutzung, ohne dafür zusätzliche interne Strukturen aufbauen zu müssen.

Gerne zeigen wir Ihnen in einem kurzen unverbindlichen Austausch, wie sich PromptSpaceGuard sinnvoll in Ihr bestehendes Angebot integrieren lässt.

Anhang: Funktionsweise & Sicherheit

Systemarchitektur von PromptSpaceGuard

PromptSpaceGuard ist kein eigenes KI-Modell, sondern eine vorgeschaltete Schutzschicht für die kontrollierte Nutzung externer KI-Systeme. Sensible Inhalte werden lokal im Browser erkannt und je nach Regelwerk markiert, blockiert oder pseudonymisiert. An den KI-Anbieter wird nur die freigegebene Anfrage weitergegeben; im Backend verarbeitet Promptspace ausschliesslich die für Betrieb, Lizenzierung, Konfiguration und Audit erforderlichen Metadaten.



Datenfluss

- Mitarbeitende geben Inhalte in unterstützte KI-Oberflächen (z.B. ChatGPT) ein.
- Die Extension prüft Eingaben lokal auf definierte sensible Inhalte.
- Je nach Regelwerk werden Inhalte markiert, blockiert oder pseudonymisiert.
- Nur die freigegebene, verarbeitete Anfrage wird an das KI-Modell weitergegeben.
- Die Antwort wird an den Nutzer zurückgegeben.
- Metadaten werden für Administratoren protokolliert.
- Regeln und individuelle Blacklists können zentral über das Dashboard verwaltet werden.

Welche Daten Promptspace verarbeitet und welche nicht

Zugriff

✓ Technische Betriebsdaten
✓ Anonymisierte Audit-Metadaten
✓ Lizenzkonfiguration
✓ Pattern-Definitionen

Kein Zugriff

✗ Nutzereingaben (Originaltext)
✗ Erkannte PII-Werte
✗ Anonymisierungs-Zuordnungen (Mappings)
✗ KI-Antworten und Chat-Verläufe
✗ Browserdaten und Cookies

Grenzen und Annahmen

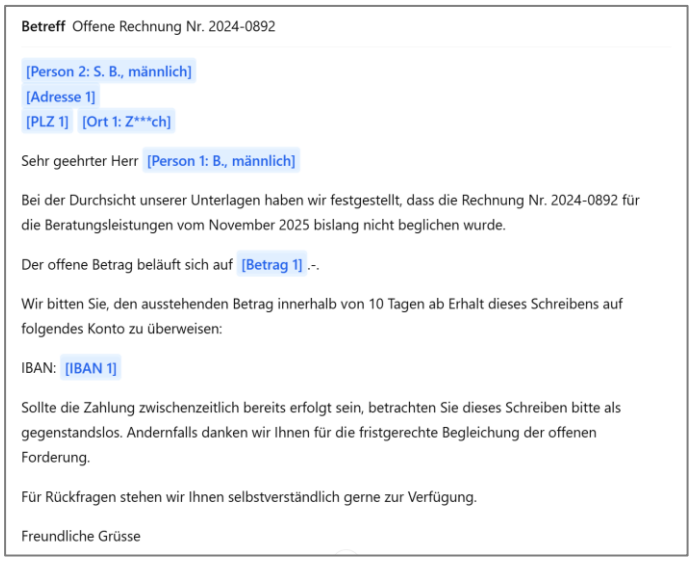
PromptSpaceGuard reduziert Risiken bei der Nutzung externer KI-Systeme erheblich. Seine Wirkung ist am stärksten, wenn technische Schutzmechanismen, organisatorische Vorgaben und Schulung sinnvoll zusammenspielen. Die Wirksamkeit hängt insbesondere davon ab, dass Regeln, Muster und Konfigurationen zum jeweiligen Anwendungsfall passen und die unterstützten Oberflächen korrekt eingebunden sind. Externe KI-Anbieter bleiben eigenständige Dienste mit eigenen Rahmenbedingungen.

Funktion der Pseudonymisierung

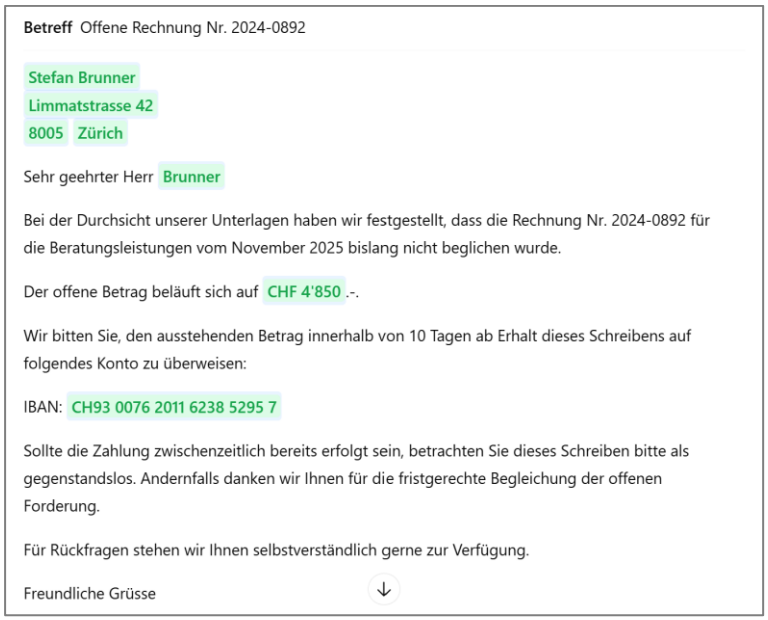
Unsere Lösung PromptSpaceGuard arbeitet als lokale Browser-Erweiterung, wie folgt:

1.1 Erkennung: Sensible Daten (Namen, Orte, E-Mails, Telefonnummern, IBAN, AHV-Nr.) werden direkt im Browser des Mitarbeitenden erkannt.

1.2 Ersetzung und Übermittlung: Sensible Daten werden durch neutrale Platzhalter ersetzt (z. B. [Person A], [Firma B]) und einzig der anonymisierte Text verlässt das Unternehmen.



1.3. Rückübersetzung: Die Antwort der KI wird lokal im Browser wieder mit den Originaldaten angereichert.



Wichtig: Zero-Knowledge, Promptspace.ch oder Dritte haben zu keinem Zeitpunkt Zugriff auf die Dateneingabe. Diese liegen jeweils temporär im Arbeitsspeicher des Nutzers.

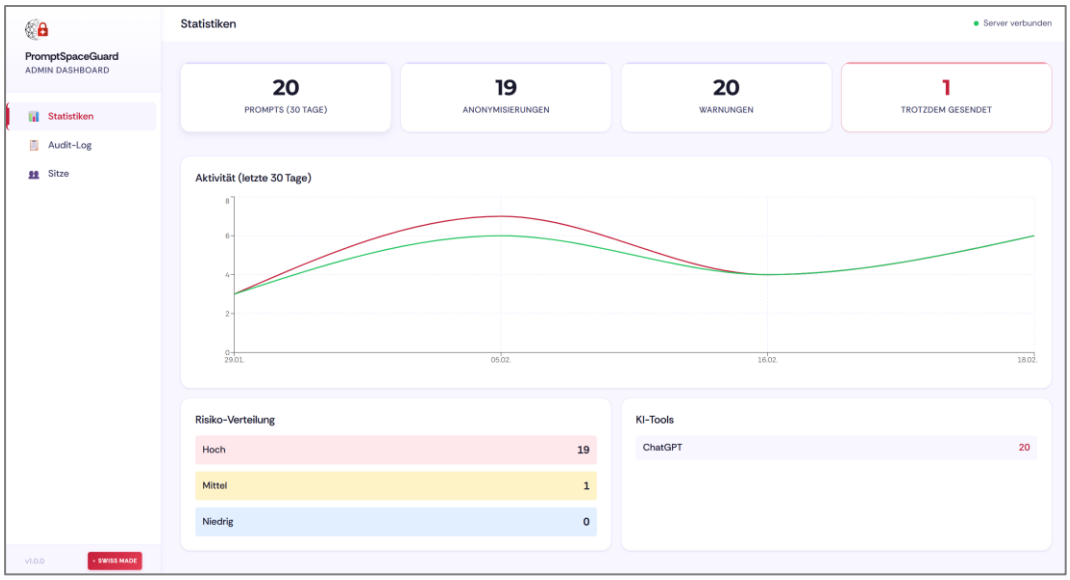
Datenschutz & Compliance (Schweiz & EU)

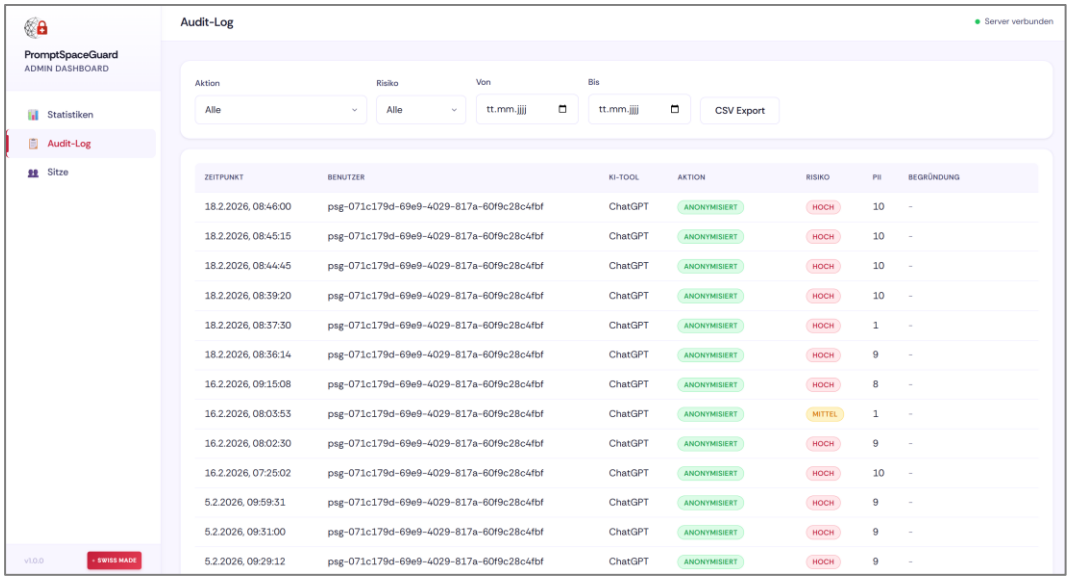
- **Server-Standort:** Administrative Betriebsdaten wie Lizenzen und Audit-Metadaten werden in der Schweiz verarbeitet.
- **Drittstaatenrisiken:** Da sensible Inhalte vor der Übermittlung lokal erkannt und je nach Konfiguration pseudonymisiert werden, wird das Risiko des Zugriffs durch externe Anbieter oder Behörden auf Klartextdaten deutlich reduziert.
- **Datenschutzprinzipien:** Das Verfahren ist auf Datenminimierung, Privacy-by-Design und eine kontrollierte Nutzung externer KI-Systeme ausgelegt.
- **Vertraulichkeit und Berufsgeheimnis:** Da Promptspace keinen Zugriff auf Originaleingaben, erkannte PII-Werte oder lokale Zuordnungen benötigt, kann die Wahrung von Vertraulichkeitspflichten und Berufsgeheimnissen technisch unterstützt werden.

B) Audit-Fähigkeit

Für Compliance-Zwecke wird ein Audit-Log erstellt, das speichert:

- **Wer** hat wann LLMs genutzt?
- **Wie viele** sensible Daten wurden pseudonymisiert?
- **Welche** Art von Daten (z.B. “3x Personenbezug, 1x IBAN”)





Wichtig: Der Inhalt des Prompts wird nicht gespeichert, um die Vertraulichkeit zu wahren.

Weiterführende Informationen zu Datenschutz, Auftragsverarbeitung und Sicherheitsmassnahmen finden Sie in unserem **Trust-Center.** Für eine individuelle Einordnung laden wir Sie gerne zu einem unverbindlichen und vertraulichen **Erstgespräch** ein.