

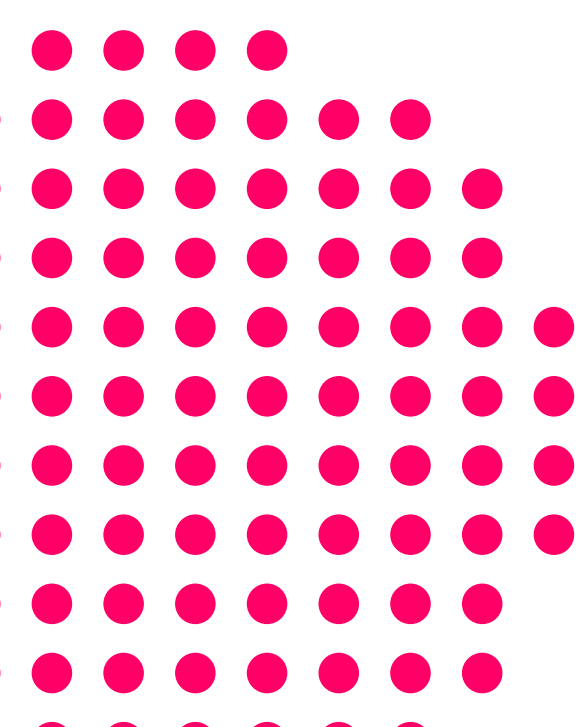
The logo for KIPROOF features a stylized icon on the left, composed of a thick horizontal bar and a chevron-like shape above it. To the right of the icon, the word "KIPROOF" is written in a bold, uppercase, sans-serif font. The letter "i" is lowercase and includes a dot.

KIPROOF

KI sicher nutzen

Agenda

- 1 Ausgangssituation
- 2 Herausforderungen
- 3 Lösung & USP
- 4 Datenschutz & Tool Insights
 - 4.1 Datenschutz
 - 4.2 Tool Insights



1 Der blinde Fleck der IT-Sicherheit

Unternehmen haben 2024 einen Schaden von 266,6 Milliarden EUR durch Cyberangriffe erlitten*

Unternehmen legen höchsten Wert auf Schutz vor Cybersecurity-Angriffen...

...um dann gleichzeitig unkontrollierte Datenabflüsse über KI-Modelle zu riskieren.



2 Herausforderungen

Unternehmen müssen drei Herausforderungen bei der KI-Nutzung meistern



Kontrolle & Schutz

- **Volle Kontrolle** über Zugriffe & Verarbeitung sicherstellen.
- **Haftung & Audits** absichern.
- **Wissen & IP** schützen.



Datenrisiken & Schatten-IT

- **40%** der Mitarbeitenden nutzen **private KI-Tools**.
- **Keine Transparenz** über Datenflüsse.
- **Risiko** sensibler Datenlecks.

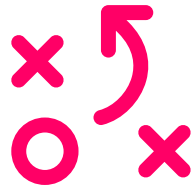


Regulatorische Anforderungen

- **EU AI Act**: High-Risk & Monitoring.
- **DSGVO**: Nachweispflicht & Accountability.
- **Technische Absicherung** ist Pflicht. (TOMs)

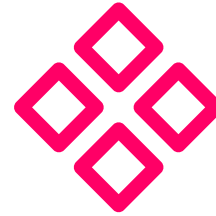
3 Lösung & USP

Wir „enablen“ Sie maßgeschneidert und bereiten Ihnen den Weg für eine sichere KI-Nutzung



Strategie

- Erfassen des Ist-Zustands
- Definieren des Zielbilds
- Identifizieren relevanter Use Cases
- Erarbeiten der KI-Strategie
- Festlegen von Prioritäten & Roadmap



Einführung/ Umsetzung

- Einrichtung der Plattform
- Anbindung relevanter Systeme & Daten
- Rollen, Rechte & Richtlinien festlegen
- Technische Umsetzung & Tests
- Go-live und Rollout mit Begleitung



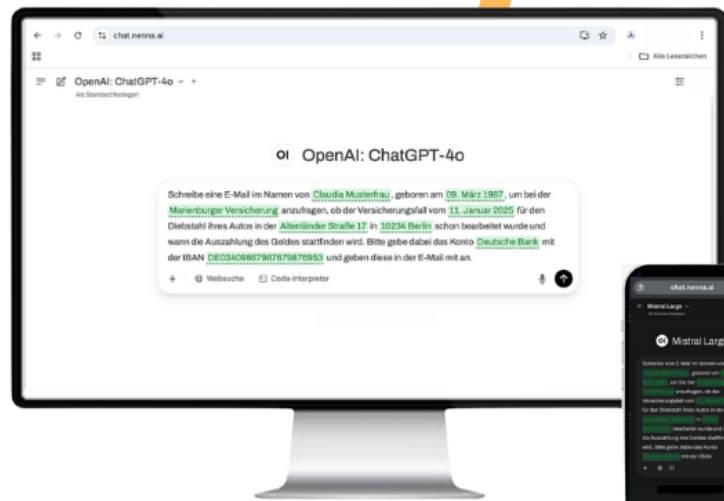
Schulung

- Teams & Führungskräfte trainieren
- Effektiv prompten lernen
- Prompt-Library & Systemprompts aufbauen
- Anwendung an realen Use Cases
- Sicherer Umgang im Arbeitsalltag

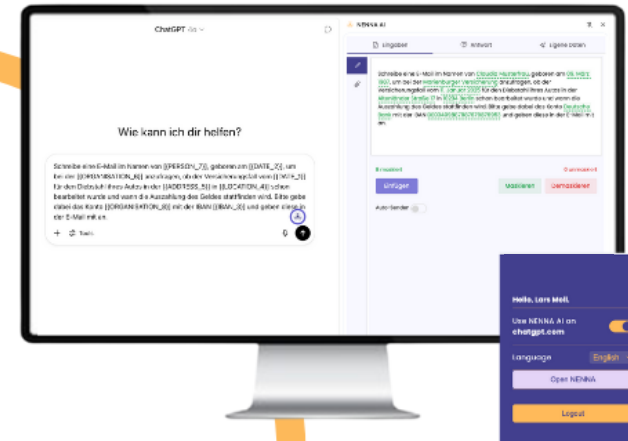
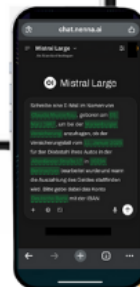
4 Tool Insights & Datenschutz

3 Möglichkeiten der datensicheren KI-Infrastruktur für Ihr Unternehmen

Eigene KI-Oberfläche mit integriertem Datenschutz



360°
KI-Schutz



KI-Datenschutz für
über 300 Tools im
Browser



API-Anbindung für
Prozessautomatisierung

4.1 Datenschutz

3 Möglichkeiten der datensicheren KI-Infrastruktur für Ihr Unternehmen.

1

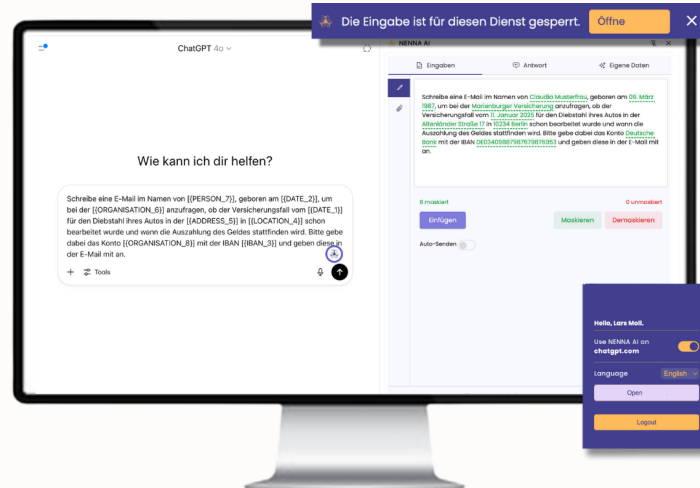
Eigene KI-Oberfläche mit integriertem Datenschutz



- ✓ Eigener KI-Zugang und Nutzeroberfläche für alle Mitarbeitenden
- ✓ Eigener, integrierter und echter Datenschutz
- ✓ Schattennutzung wird deutlich reduziert
- ✓ Mit allen Smartphones kompatibel

2

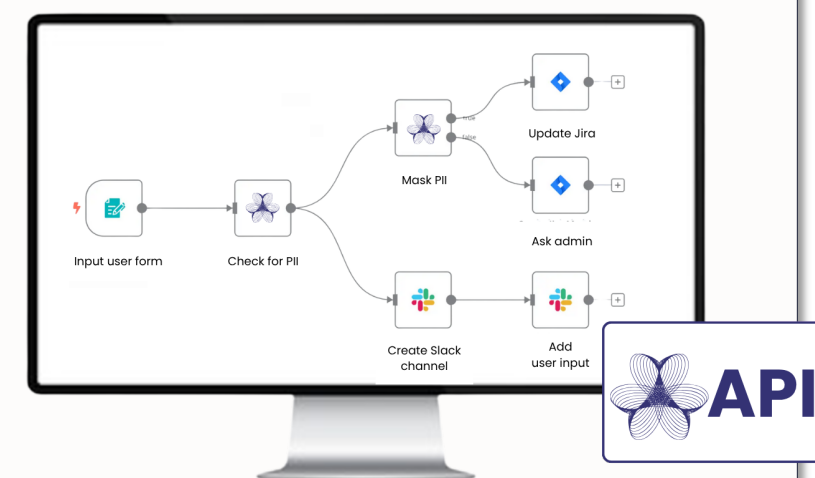
Im Browser KI-Datenschutz für alle KI-Tools



- ✓ Eingabe über Maske im Browser
- ✓ Geschützter Zugriff auf über 300 KI-Tools
- ✓ Schattennutzung wird deutlich reduziert
- ✓ Datenschutz
- ✓ sichere und transparente Nutzung von allen KI-Tools im Unternehmen.

3

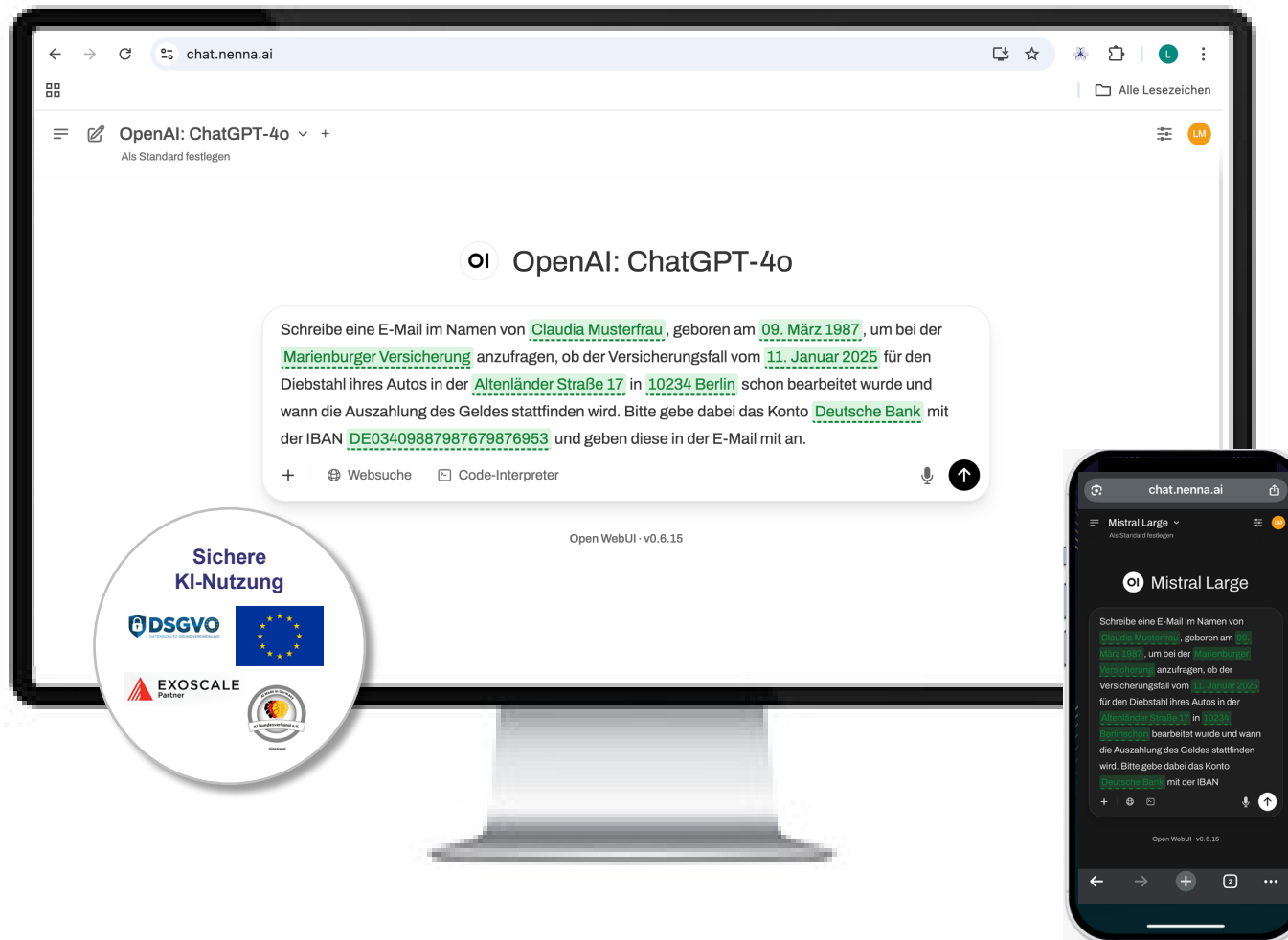
Technische Schnittstelle zur Integration in bestehende Software



- ✓ Privacy-Schutz aller internen AI Cases
- ✓ Wir bringen Datenschutz in unternehmenseigene KI-Prozesse und Agentic-Use-Cases durch die API und ermöglichen damit den DSGVO und EU-AI-Act kompatiblen Einsatz.

4.1 Datenschutz

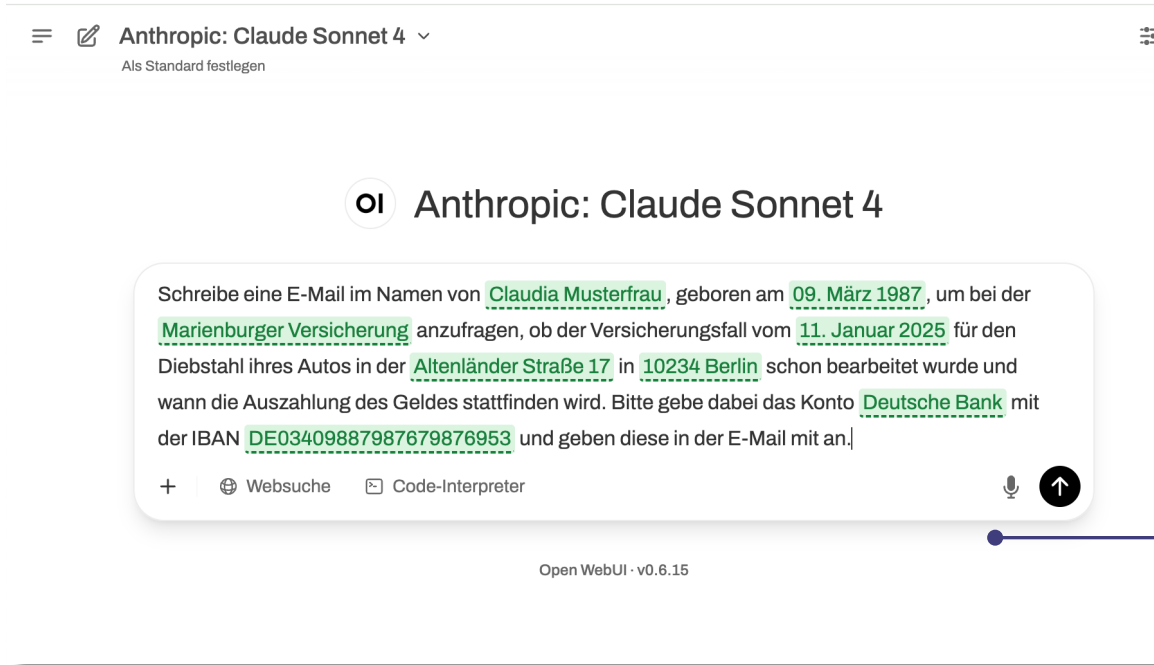
Alle KI Use-Cases auf einer Plattform – Datensicher in der Verarbeitung
Sicherheit + Unabhängigkeit + Wirtschaftlichkeit in einer KI-Lösung vereint



- Über die Plattform bereitgestellte europäische KI-Modelle nutzen – **Mistral, Llama, Azure OpenAI, Anthropic, uvm.**
- **Prompt Vorlagen und Wissensdatenbanken** anlegen und im Team teilen
- Integration von **On-Prem Modellen** für sehr sensible Unternehmensbereiche
- **Volle Flexibilität** bei der KI-Nutzung: **Datenhoheit**, keine **Blackbox-Mechanik**
- Direkte **Integration** von **KI-Datenschutz** im **Browser** und **Mobil**
- **DSGVO-konform, EU AI ACT ready und 100% EU-Infrastruktur**

4.1 Datenschutz

Maskierung sensibler Inhalte und personenbezogener Daten bei Eingabe in Oberfläche



- ✓ Sensible Daten werden direkt bei der Eingabe maskiert und beim Output automatisch wieder angezeigt
- ✓ Manuell können weitere Inhalte maskiert oder demaskiert werden
- ✓ Auch Spracheingaben werden transkribiert und sensible Daten maskiert

Das KI-Modell sieht **keine persönlichen Daten**:

Mit freundlichen Grüßen

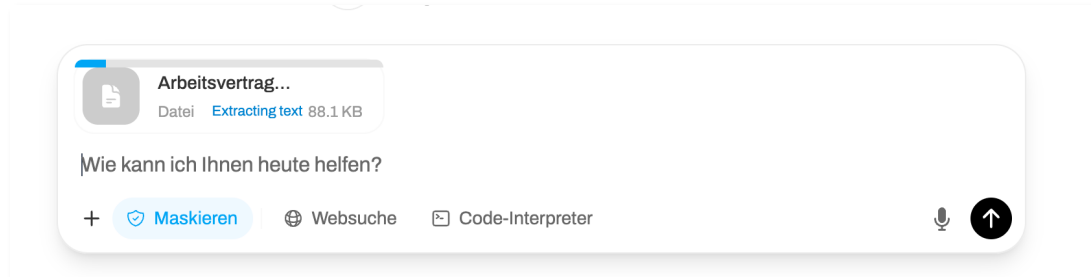
Claudia Musterfrau



PERSON_8 - Wurde maskiert

4.1 Datenschutz

Dokumente sind direkt in der KI-Oberfläche geschützt



Dokumentenmaskierung:

- **On-the-fly-Maskierung:** Dateien werden beim Hochladen maskiert (Persönliche Daten und IP), egal welche KI Sie nutzen
- **Individuelle Anpassung der maskierten Daten:** direkt im Prompting-Prozess können PII an- und abgewählt werden, je nach Use Case
- **Datensicheres Hinterlegen von Wissen:** Zudem können im Wissensbereich maskierte Dokumente hinterlegt und beim Prompten eingesetzt werden
- **Demaskierung beim Output:** Lokal werden die Daten von der Plattform wieder zugeordnet, das jeweilige LLM sieht keine sensiblen Daten

Arbeitsvertrag Beispiel.pdf

88.1 KB • 119 Extracted Lines ⓘ Formatting may be inconsistent from source.

Arbeitsvertrag

zwischen

Innovara Solutions GmbH

Himmelstraße 789

10115 Berlin

Deutschland

• nachfolgend "Arbeitgeber" genannt -

und

Lena Sommerfeld

Kadiner Straße 11

10245 Berlin

Deutschland

• nachfolgend "Arbeitnehmerin" genannt -

§ 1 Beginn und Dauer des Arbeitsverhältnisses

1. Das Arbeitsverhältnis beginnt am **1. Juni 2024**.
2. Das Arbeitsverhältnis wird auf unbestimmte Zeit geschlossen.

§ 2 Tätigkeit

1. **Die Arbeitnehmerin** wird als Senior Content Marketing Managerin eingestellt.
2. Sie berichtet direkt an den **Leiter der Marketingabteilung**.
3. Die Hauptaufgaben umfassen:
 - o Entwicklung und Umsetzung von Content-Marketing-Strategien
 - o Erstellung und Redaktion von Inhalten für verschiedene Plattformen (Website, Blog, Social Media, Newsletter)
 - o Analyse der Content-Performance und Ableitung von Optimierungsmaßnahmen
 - o Zusammenarbeit mit dem **Design- und Vertriebsteam** zur Sicherstellung eines konsistenten Markenauftritts
 - o Leitung von Projekten und ggf. Führung von Junior-Mitarbeitern

4.1 Datenschutz

Verschiedene Datenschutzlager für Ihre Sicherheit

1

Anthropic: Claude Sonnet 4

Schreibe eine E-Mail im Namen von Claudia Musterfrau, geboren am 09. März 1987, um bei der Marienburger Versicherung anzufragen, ob der Versicherungsfall vom 11. Januar 2025 für den Diebstahl ihres Autos in der Altenländer Straße 17 in 10234 Berlin schon bearbeitet wurde und wann die Auszahlung des Geldes stattfinden wird. Bitte gebe dabei das Konto Deutsche Bank mit der IBAN DE03409887987679876953 und geben diese in der E-Mail mit an.

2

chat.ninna.ai

Anthropic: Claude Sonnet 4

Modell suchen

Alle Extern

Anthropic: Claude Sonnet 4

DeepSeek: R1

Google: Gemini 2.5 Flash

Google: Gemini 2.5 Pro

Google: Gemma 3 27B

Mistral Large

OpenAI: ChatGPT-4o

Temporäre Unterhaltung

3

Anthropic: Claude Sonnet 4

llama3.2:3b

Search a model

llama3.2:3b 3.2B

llama3.2:1b 1.2B

nomic-embed-text:latest 137M

llama3.2:latest 3.2B

llama3.1:latest 8.0B

Arena Model

Temporary Chat

Layer Datenschutz: integrierte Anonymisierung im Frontend für höchsten Datenschutz

Layer für EU-Modelle: Datenresidenz von KI-Modellen in Europa für Souveränität

Layer On-Prem für höchste Sicherheit: Optionaler Betrieb von lokalen, spezifischen Modellen und der gesamten Plattform möglich

Hosting: Exoscale, Datacenter in Frankfurt (u.a. BSI C5, ISO 27001, uvm.)

4.2 Tool Insights

Klare Rollen- und Teamkonfigurationen

Unternehmensinterne Strukturen in der Oberfläche ganz individuell abbilden



Zugangskontrolle ✕

Sichtbarkeit

🔒 **Privat** Öffentlich

Benutzer und Gruppen mit Berechtigung können

Zugangskontrolle ✕

Sichtbarkeit

🔒 Privat ▼

Nur ausgewählte Benutzer und Gruppen mit Berechtigung können darauf zugreifen

Gruppen

✓ Wählen Sie eine Gruppe

test

keine Gruppen mit Zugriff, fügen Sie eine Gruppe hinzu, um Zugriff zu gewähren

ROLLE

ADMINISTRATOR

BENUTZER

Gruppen

Wählen Sie eine Gruppe

test

SCHREIBEN ✕

LESEN ✕

- Anmeldung mit Oauth möglich
- Rechte können als **Administrator** verwaltet werden, **Benutzern** werden dann die Rechte zugewiesen
- Das Teilen von **Chats / Wissen / Modellen** kann granular auf **privater Ebene (+Gruppen)** oder komplett **öffentlich** gestellt werden
- Gruppenrechte können auf **lesen (nur sichtbar)** oder **schreiben (editierbar)** gestellt werden

4.2 Tool Insights

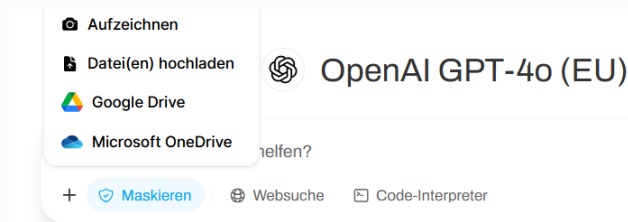
Nutzen Sie interne und externe Informationen für KI

Unzählige Möglichkeiten für die Integration von Wissen und Informationen in Ihre KI-Workflows

Dateien und Dokumente

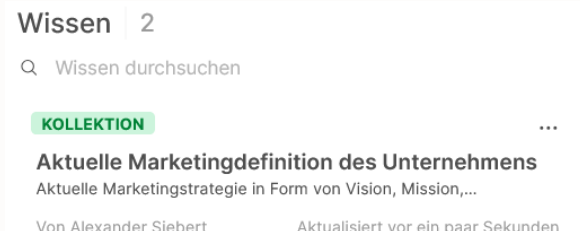
Kontextualisieren Sie Ihre KI-Anfragen mit den nötigen Informationen mittels:

- Anbindung von **OneDrive** und **Google Drive**
- **Upload** von unterschiedlichen Dokumenten, wie Word, PDF und vielen mehr
- **Upload** von **Screenshots**, **Bildern** und **Audioaufnahmen**



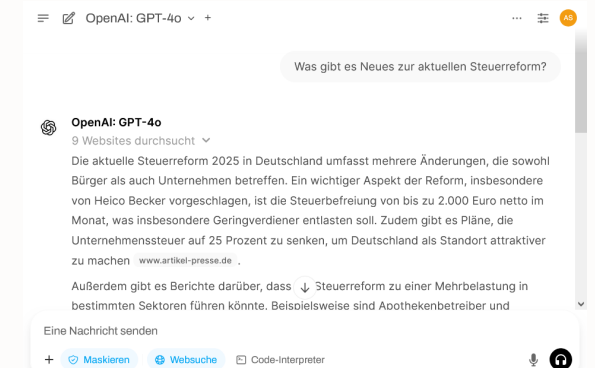
Internes Wissen

- **Kuratieren** und **teilen** Sie relevantes **Wissen** in **Kollektionen** im Unternehmen.
- Erstellen Sie sich **Notizen**, reichern und verfeinern diese mittels KI und benutzen Sie sie als Wissen für ihre Arbeit mit KI-Modellen.
- Binden Sie **interne Datenbanken** an mittels Integrationen und MCP-Server.



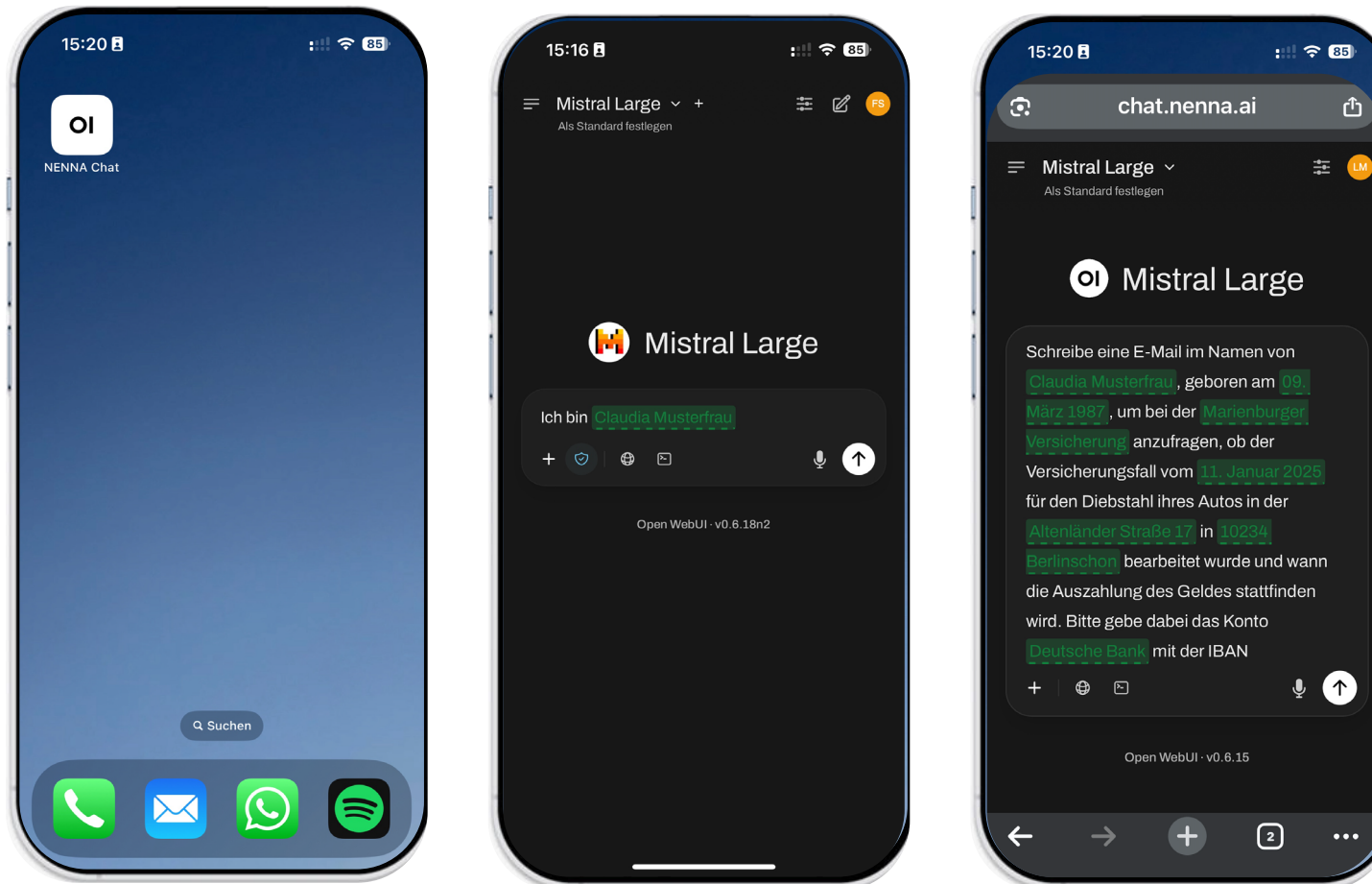
Externes Wissen

- Nutzen sie die integrierte **Websuche** für die Recherche oder KI-Modelle mit integriertem Webindex
- Binden Sie mittels Tools und Funktionen **externe Systeme** und **Wissensquellen** an.



4.2 Tool Insights

Nutzen Sie überall, sicher und jederzeit KI-Modelle



- Völlig **responsive** Browser App, perfekt für den Einsatz auf einem Desktop, Tablet oder Smartphone
- **Diktierfunktionen** und **Audiofunktionen** unterstützen die mobile Nutzung als echter KI-Assistent
- Integrierbar als **Browser-App** auf Ihrem Smartphone