

WHITEPAPER



ChatGPT®, Claude®, Gemini®: Die beste KI sitzt in den USA. Ihre Daten bleiben 100 % anonym. 100 % DSGVO-konform.

Anonix Privacy Proxy

KI nutzen. Daten schützen. Ohne Kompromisse.

Version 1.1 – Oktober 2026

Convecto GmbH

Inhalt



Das unsichtbare Risiko	2
Der CLOUD Act	3
Was wirklich passiert, wenn Ihre Software KI-APIs nutzt	4
Die Lösung: Anonix Privacy Proxy	5
So funktioniert der Schutz	6
Regierung, Verwaltung & öffentlicher Dienst	7
Krankenhäuser und Kliniken	8
Pflegeeinrichtungen	9
Gerichte und Justiz	10
Sozialträger und Jugendämter	11
Anwaltskanzleien	12
Steuerberater und Wirtschaftsprüfer	13
Banken und Versicherungen	14
HR-Abteilungen	15
Bildungseinrichtungen	16
Pharma und Life Sciences	17
Softwareunternehmen und IT-Dienstleister	18
Warum bestehende Lösungen scheitern	19
Die Architektur auf einen Blick	20
Investition und Wirtschaftlichkeit	21
Compliance auf Knopfdruck	22
Stimmen aus der Praxis	23
Ihr Weg zu Anonix	24
Impressum	25

Das unsichtbare Risiko



Stellen Sie sich vor: Ihre Fachanwendung sendet Bürgerdaten per API an einen KI-Dienst, um Bescheide verständlicher zu formulieren. Ihre Kanzleisoftware lässt Vertragsentwürfe mit Mandantennamen prüfen. Ihr Kliniksystem fragt die KI nach Therapieoptionen und überträgt dabei die Patientenakte. Oder ein Mitarbeiter kopiert sensible Daten direkt in ChatGPT®.

Das passiert. Jeden Tag. In Tausenden deutschen Unternehmen und Behörden. Und in den meisten Fällen weiß die Geschäftsleitung nichts davon.

54%

DER WISSENSARBEITER

nutzen inoffizielle KI-Tools am Arbeitsplatz

42%

DER UNTERNEHMEN

gehen von privater KI-Nutzung durch Mitarbeiter aus

49%

DER MITARBEITER

würden KI-Tools auch bei einem ausdrücklichen Verbot weiterhin verwenden

Quellen: Bitkom Research 2025, Cornerstone OnDemand 2025

Warum Verbote nicht funktionieren

Unternehmen, die KI einfach verbieten, verlieren gleich doppelt. Erstens nutzen die Mitarbeiter die Tools trotzdem, nur eben unkontrolliert und ohne jede Schutzmaßnahme. Zweitens verlieren diese Unternehmen den Produktivitätsvorsprung, den KI-Werkzeuge bieten. Das Marktforschungsunternehmen Gartner prognostiziert: Bis 2030 werden 40 Prozent aller Organisationen weltweit Sicherheitsvorfälle durch unkontrollierte KI-Nutzung erleben.

Die eigentliche Frage lautet nicht, ob Ihre Mitarbeiter KI nutzen. Sondern ob Sie wissen, welche Daten dabei das Unternehmen verlassen.

Der CLOUD Act – das Problem, das niemand sieht



OpenAI® sitzt in San Francisco. Anthropic® auch. Google® sowieso. Was viele Entscheider nicht wissen: Der US CLOUD Act von 2018 gibt amerikanischen Behörden das Recht, von US-Unternehmen die Herausgabe gespeicherter Daten zu verlangen. Egal, auf welchem Server die Daten liegen. Egal, in welchem Land.

Wenn Ihre Software oder Ihre Mitarbeiter personenbezogene Daten an OpenAI®, einen OpenAI®-kompatiblen Anbieter wie DeepSeek® oder Mistral®, an Claude® oder Gemini® senden – ob per API-Integration oder direkte Nutzung – können US-Behörden theoretisch auf diese Daten zugreifen. Das steht in direktem Widerspruch zur DSGVO.

US CLOUD Act

US-Behörden dürfen Daten von US-Firmen weltweit anfordern

Gilt unabhängig vom physischen Speicherort der Daten

Kein Richtervorbehalt nach EU-Maßstäben erforderlich

Betrifft OpenAI®, Google®, Microsoft®, Anthropic®, DeepSeek®, Mistral®, xAI®, Groq®, Perplexity® und alle anderen US- und Cloud-Anbieter

VS

EU-DSGVO

Personenbezogene Daten brauchen Rechtsgrundlage für Drittlandtransfer

Schrems-II-Urteil erklärte Privacy Shield für ungültig
EU-US Data Privacy Framework nur für zertifizierte Firmen gültig

Art. 48 DSGVO verbietet Herausgabe ohne Rechtshilfeabkommen

Die vermeintliche Lösung: EU-Rechenzentrum

Viele Unternehmen glauben, das Problem gelöst zu haben, indem sie KI-Modelle nicht direkt beim Anbieter buchen, sondern über AWS® Bedrock oder Microsoft® Azure® in einem europäischen Rechenzentrum betreiben. Die Daten verlassen physisch nie die EU – Problem gelöst?

Nein. Der CLOUD Act knüpft nicht an den Standort des Servers, sondern an den Sitz des Unternehmens. AWS® ist eine Tochter von Amazon® (USA). Microsoft® Azure® ist ein Produkt der Microsoft® Corporation (USA). Beide unterliegen dem CLOUD Act – unabhängig davon, ob die Daten in Frankfurt, Dublin oder Stockholm verarbeitet werden.

Rechtliche Realität: Ein EU-Rechenzentrum eines US-Anbieters schützt nicht vor dem CLOUD Act. US-Behörden können die Herausgabe der Daten verlangen, und der Anbieter ist gesetzlich zur Kooperation verpflichtet. Das bestätigen sowohl der Europäische Datenschutzausschuss (EDSA) als auch das Schrems-II-Urteil des EuGH.

Mit Anonix spielt der Serverstandort keine Rolle mehr: Der KI-Anbieter – ob direkt oder über ein EU-Rechenzentrum – sieht ausschließlich anonymisierte Daten mit Platzhaltern. Selbst bei einer CLOUD-Act-Anforderung gibt es nichts Verwertbares herauszugeben.

Die Konsequenzen sind real

5,9

MILLIARDEN EUR

DSGVO-Bußgelder seit 2018 in ganz Europa

1,2

MILLIARDEN EUR

höchste Einzelstrafe (Meta®, 2023, wegen Drittlandtransfer)

62%

DER UNTERNEHMEN

in Deutschland transferieren Daten in Nicht-EU-Länder

Quellen: DLA Piper GDPR Fines Survey 2025, Bitkom Research 2025

Das Dilemma: KI-Nutzung ohne Datenschutz ist illegal. Aber auf KI zu verzichten, ist wirtschaftlich fahrlässig. Die Lösung muss beides vereinen.

Was wirklich passiert, wenn Ihre Software KI-APIs nutzt



Schauen wir uns einen typischen Vorgang an. Ihre Fachanwendung ruft eine KI-API auf, um einen Bescheid verständlicher zu formulieren:

API-Request an den LLM-Anbieter:

Bitte formuliere folgenden Bescheid verständlicher:

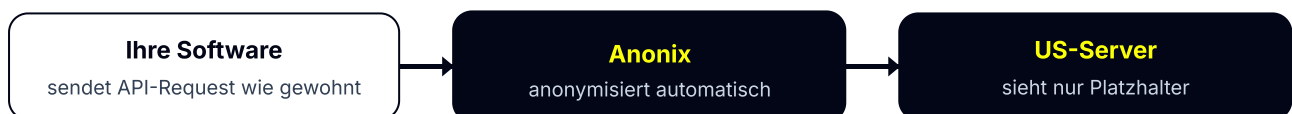
Sehr geehrte Frau Ingrid Bergmann,
Ihr Antrag auf Wohngeld (Az. WG-2026-04817) wird bewilligt.
Überweisungskonto: DE89 3704 0044 0532 0130 00
Anschrift: Goethestr. 14, 60313 Frankfurt am Main

Ohne Anonix verlassen vier Kategorien personenbezogener Daten Ihre Infrastruktur: Name, Aktenzeichen, IBAN und vollständige Adresse. Sie landen auf Servern in den USA.

VORHER: Ohne Schutz



NACHHER: Mit Anonix Privacy Proxy



Was der LLM-Anbieter sieht:

Bitte formuliere folgenden Bescheid verständlicher:

Sehr geehrte **[PERSON_1]**,
Ihr Antrag auf Wohngeld (Az. **[AKTENZEICHEN_1]**) wird bewilligt.
Überweisungskonto: **[IBAN_1]**
Anschrift: **[ADRESSE_1]**, **[PLZ_1]**

Die KI arbeitet mit den Platzhaltern genauso gut wie mit den echten Daten. In der Antwort setzt Anonix die Originaldaten automatisch wieder ein – in Echtzeit, auch bei gestreamten Antworten. Für Ihre Software und Ihre Mitarbeiter ändert sich nichts am Ablauf.

Die Lösung – Anonix Privacy Proxy

Anonix ist ein transparenter Proxy, der zwischen Ihren Anwendungen und dem KI-Anbieter sitzt – egal ob OpenAI®, DeepSeek®, Mistral®, Groq®, Perplexity®, xAI® Grok®, Claude®, Gemini® oder ein selbst gehostetes Modell. Jede Anfrage wird automatisch anonymisiert, bevor sie die EU-Infrastruktur verlässt. Jede Antwort wird automatisch de-anonymisiert, bevor sie den Mitarbeiter erreicht.

Zero Integration: Tauschen Sie lediglich die API-URL und den API-Key in Ihrer bestehenden Software. Kein Umbau. Keine Code-Änderung. Anonix funktioniert mit jeder Software, die OpenAI®-kompatible, Claude®- oder Gemini®-APIs nutzt – ob eigene Fachanwendungen, SaaS-Produkte oder Developer-Tools.

Was Anonix einzigartig macht

Für Entscheider

- **DSGVO-konform by Design** – personenbezogene Daten verlassen nie die EU
- **CLOUD Act neutralisiert** – US-Anbieter sehen nur Platzhalter
- **Kein Produktivitätsverlust** – Mitarbeiter arbeiten wie gewohnt
- **EU-gehostet als SaaS** – sofort einsatzbereit, volle Datensouveränität
- **Mandantenfähig** – isolierte Daten pro Abteilung oder Kunde

Für die IT

- **Cloud-basiert** – kein eigener Server nötig, sofort startklar
- **Alle großen LLM-APIs** – OpenAI® + alle OpenAI®-kompatiblen (DeepSeek®, Mistral®, Grok® u.v.m.), Claude®, Gemini®
- **Streaming** – Echtzeit-De-Anonymisierung auch bei SSE-Responses
- **Admin-GUI** – Provider verwalten, Regeln konfigurieren, Kosten überwachen
- **Audit-Log** – lückenlose Protokollierung, CSV-Export

Unterstützte KI-Anbieter und Modelle

ANBIETER / PROTOKOLL	MODELLE (BEISPIELE)	STREAMING
OpenAI® und alle kompatiblen APIs	GPT®-4o, GPT®-4, GPT®-3.5 Turbo, o1, o3	Ja (SSE)
OpenAI®-kompatible Anbieter	DeepSeek®, Mistral®, xAI® Grok®, Perplexity®, Together AI®, Groq®, OpenRouter® und viele weitere	Ja (SSE)
Anthropic® Claude®	Claude® 4 Opus, Claude® 3.5 Sonnet, Claude® 3 Haiku	Ja (SSE)
Google® Gemini®	Gemini® 2.0 Flash, Gemini® 1.5 Pro, Gemini® 1.5 Flash	Ja (SSE)
Lokale / Self-hosted Modelle	Ollama®, LM Studio®, vLLM® (jedes OpenAI®-kompatible Modell)	Ja (SSE)

Entscheidend: Jede Software, die eine OpenAI®-kompatible, Claude®- oder Gemini®-API nutzt, funktioniert mit Anonix. Das schließt Hunderte von Anbietern ein – von OpenAI® über DeepSeek®, Mistral®, xAI® Grok®, Perplexity® und Groq® bis hin zu selbst gehosteten Modellen. Ob eigene Fachanwendungen, ERP-Systeme, Kanzleisoftware, Developer-Tools (Cursor®, GitHub® Copilot®), KI-Frameworks (LangChain®, LlamaIndex®) oder direkte Browser-Nutzung.

So funktioniert der Schutz



Anonix erkennt personenbezogene Daten nicht mit einer einzigen Methode, sondern durch vier aufeinander aufbauende Schutzschichten. Jede Schicht fängt ab, was die vorherige übersehen hat.



Schicht 1: Mustererkennung

Über 60 Muster erkennen strukturierte Daten wie E-Mail-Adressen, Telefonnummern, IBAN, Steuer-IDs, Geldbeträge und Datumsangaben. Das funktioniert zuverlässig und schnell, weil diese Datentypen einem festen Format folgen.

Schicht 2: Anonix ConvNet NER

Für unstrukturierte Daten wie Personennamen, Firmennamen und Orte kommt ein neuronales Netzwerk zum Einsatz. Es versteht den sprachlichen Kontext und erkennt, dass „München“ ein Ort ist und „Frau Weber“ ein Name. In acht Sprachen: Deutsch, Englisch, Französisch, Spanisch, Italienisch, Niederländisch, Portugiesisch und Polnisch.

Schicht 3: Anonix Zero-Shot NER

Manche Branchen haben eigene sensible Datentypen: Diagnosen, Aktenzeichen, Projektnummern, Kostenstellen. Anonix erkennt diese ohne Programmierung. Sie beschreiben die Kategorie in Ihren eigenen Worten, und das System lernt sie sofort.

Schicht 4: KI-Qualitätsprüfung

Ein eigenes Small Language Model prüft den bereits anonymisierten Text noch einmal auf übersehene Fragmente. Es arbeitet als zweite Meinung, die unabhängig von allen anderen Schichten urteilt.

Vorher und nachher: ein Beispiel

Originaltext:

Dr. Thomas Richter (t.richter@kanzlei-richter.de)
vertritt Frau Ingrid Bergmann im Verfahren Az. 7 O
234/26. Die nächste Verhandlung findet am
22.04.2026 am LG Frankfurt statt.

Was die KI sieht:

[PERSON_1] (**[EMAIL_1]**) vertritt **[PERSON_2]** im
Verfahren **[AKTENZEICHEN_1]**. Die nächste
Verhandlung findet am **[DATUM_1]** am **[ORG_1]**
statt.

Die KI versteht den Kontext weiterhin perfekt. Sie weiß, dass es um eine Gerichtsverhandlung geht, wer wen vertritt und wann der Termin ist. Sie weiß nur nicht mehr, *wer* genau beteiligt ist.

Regierung, Verwaltung & öffentlicher Dienst



Ministerien, Landesämter, Kommunen und nachgeordnete Behörden verarbeiten Bürgerdaten mit höchster Schutzklasse. Gleichzeitig verpflichtet das Onlinezugangsgesetz (OZG) zur Digitalisierung. Mehrere Bundesländer haben bereits KI-Strategien verabschiedet, doch der Datenschutzbeauftragte blockiert jede direkte API-Anbindung an US-KI-Dienste. Ein politisches Dilemma, das technisch lösbar ist.

Die Herausforderung

- Bürgerdaten unterliegen dem BSI-Grundschutz und den VS-NfD-Vorgaben
- Meldedaten, Sozialleistungsanträge, Baugenehmigungen und Steuerdaten dürfen nicht an Dritte gelangen
- Polizei und Sicherheitsbehörden verarbeiten Ermittlungsdaten und Zeugenschutzinformationen
- Bildungseinrichtungen verarbeiten Studierendendaten und Prüfungsergebnisse
- Landesdatenschutzgesetze verbieten Cloud-KI mit Personenbezug

Anonix in der Praxis

PROMPT:

Formuliere diesen Verwaltungsbescheid in einfacher, bürgerfreundlicher Sprache.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Sehr geehrte <u>Frau Ingrid Bergmann</u> , gemäß §§ 1, 3 WoGG wird Ihrem Antrag (Az. <u>WG-2026-04817</u>) stattgegeben. Die Leistung wird auf das Konto <u>DE89 3704 0044 0532 0130 00</u> überwiesen.	Sehr geehrte <u>[PERSON_1]</u> , gemäß §§ 1, 3 WoGG wird Ihrem Antrag (Az. <u>[AKTENZEICHEN_1]</u>) stattgegeben. Die Leistung wird auf das Konto <u>[IBAN_1]</u> überwiesen.	Liebe <u>Frau Ingrid Bergmann</u> , gute Nachricht: Ihr Wohngeld-Antrag (<u>WG-2026-04817</u>) wurde bewilligt. Das Geld überweisen wir direkt auf Ihr Konto <u>DE89 3704 0044 0532 0130 00</u> . Sie müssen nichts weiter tun.

Krankenhäuser und Kliniken



Gesundheitsdaten genießen nach Art. 9 DSGVO den höchsten Schutzstatus. Befunde, Diagnosen, Medikamentenpläne und Therapieverläufe sind besondere Kategorien personenbezogener Daten. Ein Verstoß ist nicht nur ein Bußgeld -- er zerstört das Vertrauen zwischen Arzt und Patient. Gleichzeitig versprechen KI-gestützte Systeme enorme Fortschritte bei Diagnostik, Dokumentation und Therapieplanung.

Die Herausforderung

- Art. 9 DSGVO: Gesundheitsdaten sind besondere Kategorien, deren Verarbeitung grundsätzlich verboten ist
- Krankenhausgesetze der Länder verschärfen die Anforderungen zusätzlich
- KIS-Systeme (Krankenhausinformationssysteme) enthalten vollständige Patientenakten
- Ärztliche Schweigepflicht nach Paragraph 203 StGB: Strafbare Weitergabe an Dritte
- Enormer Dokumentationsaufwand: Ärzte verbringen bis zu 40% ihrer Arbeitszeit mit Dokumentation

Anonix in der Praxis

PROMPT:

Erstelle aus diesen Stichpunkten einen strukturierten Arztbrief an den Hausarzt.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Patient <u>Thomas Weber</u> , geb. <u>14.03.1968</u> . Diagnose: <u>Typ-2-Diabetes</u> . HbA1c: <u>8,2%</u> . Medikation: <u>Metformin 1000mg</u> .	Patient <u>[PERSON_1]</u> , geb. <u>[DATUM_1]</u> . Diagnose: <u>[DIAGNOSE_1]</u> . HbA1c: <u>[WERT_1]</u> . Medikation: <u>[MEDIKAMENT_1]</u> .	Sehr geehrte Kollegin, sehr geehrter Kollege, wir berichten über unseren Patienten <u>Thomas Weber</u> , geb. <u>14.03.1968</u> . <u>Diagnose: Typ-2-Diabetes</u> <u>Labor: HbA1c 8,2%</u> <u>Medikation: Metformin 1000mg</u> <u>Procedere:</u> Wir empfehlen eine Therapieanpassung und Wiedervorstellung in 3 Monaten.

Pflegeeinrichtungen



Deutschland hat über 15.000 Pflegeheime und ambulante Pflegedienste. Der Fachkräftemangel ist akut: Über 35.000 Stellen sind unbesetzt. Pflegekräfte verbringen bis zu 30% ihrer Arbeitszeit mit Dokumentation statt mit den Bewohnern. KI kann diese Last reduzieren -- aber Pflegedokumentation enthält Gesundheitsdaten nach Art. 9 DSGVO, die nicht an externe Dienste gelangen dürfen.

Die Herausforderung

- Pflegedokumentation, Medikationspläne und Betreuungsprotokolle enthalten Art.-9-Daten
- Bewohnerdaten umfassen Diagnosen, kognitive Einschränkungen und Verhaltensauffälligkeiten
- MDK-Prüfungen verlangen lückenlose, revisionssichere Dokumentation
- Heimaufsicht und Datenschutzbehörden prüfen regelmäßig die Datenverarbeitung

Anonix in der Praxis

PROMPT:

Formuliere aus diesen Notizen einen strukturierten Übergabebericht für die Nachtschicht.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Bewohnerin <u>Frau Helga Schneider</u> , Zimmer <u>214</u> , Sturzgefahr erhöht. Medikation <u>Marcumar</u> angepasst auf <u>2,5</u> <u>mg</u> .	Bewohnerin <u>[PERSON_1]</u> , Zimmer <u>[RAUM_1]</u> , Sturzgefahr erhöht. Medikation <u>[MEDIKAMENT_1]</u> angepasst auf <u>[DOSIS_1]</u> .	Übergabe Nachtschicht <u>Frau Helga Schneider</u> (Zi. <u>214</u>): - Sturzgefahr erhöht – Bettgitter hochstellen - <u>Marcumar</u> auf <u>2,5 mg</u> angepasst - Engmaschige Kontrolle erforderlich - Nächste INR-Kontrolle einplanen

Gerichte und Justiz



Die deutsche Justiz verarbeitet jährlich Millionen von Verfahren. Verfahrensakten, Urteile, Anklageschriften und Zeugenaussagen enthalten die sensibelsten personenbezogenen Daten, die es gibt: Opferdaten, Zeugenschutzinformationen, Aussagen von Minderjährigen. Das Justizgeheimnis verbietet jede unkontrollierte Weitergabe. Gleichzeitig wächst der Druck, Verfahrensdauern durch KI-gestützte Recherche zu verkürzen.

Die Herausforderung

- Verfahrensakten enthalten Namen von Angeklagten, Opfern, Zeugen und Sachverständigen
- Jugendstrafrecht: Besonderer Schutz minderjähriger Angeklagter und Opfer
- Zeugenschutzprogramme: Jede Datenweitergabe kann Menschenleben gefährden
- Richterliche Unabhängigkeit erfordert, dass keine externen Dritten Zugriff auf Verfahrensdaten erhalten

Anonix in der Praxis

PROMPT:

Formuliere einen Beschlusstenor-Entwurf für diesen Sachverhalt.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Angeklagter <u>Marcus Klein</u> , Az. <u>7 O 234/26</u> . Vorwurf: Betrug nach §263 StGB. Geschädigte: <u>Firma Müller GmbH, Frankfurt</u> .	Angeklagter <u>[PERSON_1]</u> , Az. <u>[AKTENZEICHEN_1]</u> . Vorwurf: Betrug nach §263 StGB. Geschädigte: <u>[ORG_1]</u> , <u>[ORT_1]</u> .	Beschluss In der Strafsache gegen <u>Marcus Klein</u> , Az. <u>7 O 234/26</u> , wegen Betrugs gemäß § 263 StGB zum Nachteil der <u>Firma Müller GmbH</u> wird Termin zur Hauptverhandlung am Landgericht <u>Frankfurt</u> anberaunt.

Sozialträger und Jugendämter



Jugendämter und Sozialträger verarbeiten die sensibelsten Daten unserer Gesellschaft: Kindeswohlgefährdungen, Inobhutnahmen, Suchtproblematiken, häusliche Gewalt. Fallberichte und Gutachten betreffen Menschen in Krisensituationen. Eine Datenpanne ist hier keine abstrakte Compliance-Verletzung -- sie kann Familien zerstören und Kinder gefährden.

Die Herausforderung

- Fallberichte enthalten hochsensible Daten über Kinder, Eltern und Familienkonstellationen
- Paragraph 65 SGB VIII: Sozialdaten unterliegen einem erhöhten Vertrauensschutz
- Gutachten enthalten psychologische Einschätzungen und psychiatrische Diagnosen
- Sachbearbeiter sind chronisch überlastet, KI könnte Dokumentationsarbeit entlasten

Anonix in der Praxis

PROMPT:

Erstelle aus diesen Notizen eine strukturierte Fallübersicht mit empfohlenen Maßnahmen nach SGB VIII.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Familie <u>Yilmaz</u> , <u>3 Kinder</u> (Alter <u>4, 7, 12</u>). Meldung durch Schule, Verdacht auf Kindeswohlgefährdung. Hausbesuch am <u>12.02.2026</u> .	Familie <u>[PERSON_1]</u> , <u>[ANZAHL_1]</u> Kinder (Alter <u>[ALTER_1]</u>). Meldung durch Schule, Verdacht auf Kindeswohlgefährdung. Hausbesuch am <u>[DATUM_1]</u> .	Fallübersicht Familie: <u>Yilmaz</u> Kinder: <u>3</u> (<u>4, 7, 12</u> Jahre) Meldung: Schulische Institution Verdacht: § 8a SGB VIII Hausbesuch: <u>12.02.2026</u> Empfehlung: Erziehungsberatung gem. § 28 SGB VIII einleiten

Anwaltskanzleien



Das Mandantengeheimnis ist nicht nur standesrechtlich geschützt -- ein Verstoß ist nach Paragraph 203 StGB strafbar. Vertragsentwürfe, Schriftsätze, Due-Diligence-Berichte und Mandantendaten dürfen unter keinen Umständen an Dritte weitergegeben werden. Gleichzeitig bietet KI enormes Potenzial: Vertragsanalyse, Recherche, Schriftsatzprüfung und Legal Tech verändern die Branche grundlegend. Kanzleien, die KI nicht nutzen, verlieren Mandate.

Die Herausforderung

- Paragraph 203 StGB: Strafbare Verletzung des Mandantengeheimnisses bei Datenweitergabe
- Verträge enthalten Firmennamen, Geschäftsgeheimnisse, Kaufpreise und Konditionen
- M&A-Transaktionen: Due-Diligence-Dokumente mit höchster Vertraulichkeit
- Gegnerische Anwälte könnten bei einer Datenpanne Befangenheit geltend machen

Anonix in der Praxis

PROMPT:

Entwirf eine Haftungsklausel auf Basis dieser Vertragsdaten.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Verkäufer: <u>TechVision GmbH</u> , vertreten durch <u>Dr. Stefan Hofmann</u> . Kaufpreis: <u>EUR 4,2 Mio.</u> Haftungsobergrenze: <u>EUR 840.000.</u>	Verkäufer: <u>[ORG_1]</u> , vertreten durch <u>[PERSON_1]</u> . Kaufpreis: <u>[BETRAG_1]</u> . Haftungsobergrenze: <u>[BETRAG_2]</u> .	§ 7 Haftung (1) Die Haftung der <u>TechVision GmbH</u> , vertreten durch <u>Dr. Stefan Hofmann</u> , ist auf <u>EUR 840.000</u> begrenzt. (2) Ansprüche des Käufers verjähren 24 Monate nach Übergabe. (3) Die Begrenzung gilt nicht bei Vorsatz oder grober Fahrlässigkeit.

Steuerberater und Wirtschaftsprüfer



Das Steuergeheimnis nach Paragraph 203 StGB schützt Mandantendaten strafrechtlich. Steuererklärungen, Bilanzen, Gehaltsinformationen und Betriebsprüfungsunterlagen gehören zu den vertraulichsten Geschäftsdaten eines Unternehmens. Ein Verstoß bedroht nicht nur die Zulassung des Beraters -- er kann existenzbedrohende Haftungsansprüche auslösen.

Die Herausforderung

- Steuergeheimnis nach Paragraph 203 StGB und Paragraph 57 StBerG
- Mandantendaten umfassen Umsätze, Gehälter, Vermögensverhältnisse und Steuer-IDs
- Betriebsprüfungsunterlagen enthalten detaillierte Geschäftszahlen
- WPO und ISA-Standards fordern strenge Informationssicherheit bei Wirtschaftsprüfern

Anonix in der Praxis

PROMPT:

Formuliere ein Einspruchsschreiben an das Finanzamt für diesen Mandanten.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Mandant <u>Bäckerei Kraus GmbH</u> , St.-Nr. <u>013/123/45678</u> . Einspruch gegen Umsatzsteuerbescheid 2025. Fahrzeug: 60% gewerblich, 40% privat.	Mandant <u>[ORG_1]</u> , St.-Nr. <u>[STEUER_ID_1]</u> . Einspruch gegen Umsatzsteuerbescheid 2025. Fahrzeug: 60% gewerblich, 40% privat.	Einspruch Finanzamt ... St.-Nr.: <u>013/123/45678</u> Namens und in Vollmacht unseres Mandanten <u>Bäckerei Kraus GmbH</u> legen wir Einspruch gegen den Umsatzsteuerbescheid 2025 ein. Begründung: Bei 60% gewerblicher Nutzung ist ein anteiliger Vorsteuerabzug gem. § 15 UStG anzuerkennen. Wir beantragen Aussetzung der Vollziehung.

Banken und Versicherungen

BaFin-regulierte Unternehmen unterliegen dem Bankgeheimnis und mit DORA (Digital Operational Resilience Act) seit Januar 2025 den strengsten IT-Sicherheitsanforderungen in der EU. Kontodaten, Kreditanträge, Schadensmeldungen und Risikobewertungen erfordern höchsten Schutz. Gleichzeitig investieren Banken und Versicherer Milliarden in KI-gestützte Prozessautomatisierung.

Die Herausforderung

- Bankgeheimnis nach Paragraph 383 ZPO und AGB der Banken
- DORA: Strenge Anforderungen an IT-Risikomanagement und Drittanbieter-Überwachung
- MaRisk/BAIT: Auslagerungsregelungen für IT-Dienstleistungen
- Kunden-KYC-Daten, Kontobewegungen und Kreditscoring-Ergebnisse sind hochsensibel

Anonix in der Praxis

PROMPT:
Erstelle aus dieser Schadensmeldung ein Anschreiben an den Versicherungsnehmer zur Regulierung.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
VN <u>Sabine Hartmann</u> , V.-Nr. <u>KFZ-2026-881234</u> . Unfall am <u>03.03.2026</u> in <u>München, Leopoldstr. 42</u> . Schaden: <u>EUR 12.400</u> .	VN <u>[PERSON_1]</u> , V.-Nr. <u>[VERTRAGSNR_1]</u> . Unfall am <u>[DATUM_1]</u> in <u>[ORT_1]</u> , <u>[ADRESSE_1]</u> . Schaden: <u>[BETRAG_1]</u> .	Sehr geehrte <u>Frau Hartmann</u> , zu Ihrem Schadensfall vom <u>03.03.2026</u> (V.-Nr. <u>KFZ-2026-881234</u>) teilen wir Ihnen mit, dass die Regulierung eingeleitet wurde. <u>Schadensort: München, Leopoldstr. 42</u> <u>Gemeldeter Schaden: EUR 12.400</u> Ein Gutachter wird sich innerhalb von 5 Werktagen bei Ihnen melden.

HR-Abteilungen



Jedes Unternehmen -- unabhängig von der Branche -- verarbeitet in der Personalabteilung hochsensible Mitarbeiterdaten. Personalakten, Bewerberdaten, Gehaltsinformationen, Krankmeldungen und Mitarbeiterbewertungen sind personenbezogene Daten, deren Weitergabe an Dritte arbeitsrechtliche und datenschutzrechtliche Konsequenzen hat. KI-gestütztes Recruiting, Performance Reviews und Personalplanung boomen -- oft ohne Wissen des Datenschutzbeauftragten.

Die Herausforderung

- Paragraph 26 BDSG: Strenge Zweckbindung bei der Verarbeitung von Beschäftigtendaten
- Bewerberdaten: AGG-Konformität und Diskriminierungsrisiken bei KI-gestützter Vorauswahl
- Betriebsvereinbarungen regeln oft explizit den Einsatz von KI-Werkzeugen
- Gehaltsdaten, Krankmeldungen und Abmahnungen sind besonders schützenswert

Anonix in der Praxis

PROMPT:

Erstelle aus dieser internen Jobbeschreibung eine externe Stellenausschreibung.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Nachfolge für <u>Martin Schäfer</u> , Abt. Controlling. Gehalt: <u>EUR 78.000</u> . Vorgesetzter: <u>Dr. Lisa Berger</u> . Kündigung zum <u>30.06.2026</u> .	Nachfolge für <u>[PERSON_1]</u> , Abt. Controlling. Gehalt: <u>[BETRAG_1]</u> . Vorgesetzter: <u>[PERSON_2]</u> . Kündigung zum <u>[DATUM_1]</u> .	Controller (m/w/d) Ihre Aufgaben: - Budgetplanung und Forecasting - Monats- und Jahresabschlüsse - Reporting an <u>Dr. Lisa Berger</u> Wir bieten: - Vergütung: <u>EUR 78.000</u> - Start: zum nächstmöglichen Zeitpunkt

Bildungseinrichtungen



Universitäten, Hochschulen, Schulen und Forschungseinrichtungen stehen unter doppeltem Druck: Einerseits sollen sie KI-Vorreiter sein und Studierenden moderne Werkzeuge bereitstellen. Andererseits verarbeiten sie Studierendendaten, Prüfungsergebnisse und personenbezogene Forschungsdaten, die unter die Landesdatenschutzgesetze fallen. Mehrere Landesdatenschutzbeauftragte haben bereits Empfehlungen gegen den Einsatz von US-Cloud-KI-Diensten veröffentlicht.

Die Herausforderung

- Landesdatenschutzgesetze und Hochschulgesetze regeln den Umgang mit Studierendendaten
- Prüfungsergebnisse, Matrikelnummern und Exmatrikulationsgründe sind besonders geschützt
- Forschungsdaten mit Personenbezug unterliegen den Ethikkommissionen
- Dozierende nutzen KI bereits massiv -- oft ohne institutionelle Freigabe

Anonix in der Praxis

PROMPT:

Erstelle aus dieser Lehrevaluation einen strukturierten Verbesserungsbericht für die Studienkommission.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Kurs <u>BWL-301</u> , Prof. <u>Dr. Andreas Keller</u> . Note: <u>2,3</u> . Kommentar: 'Dozent erklärt gut, aber <u>Frau Schneider</u> aus der Übung war unvorbereitet.'	Kurs <u>[KURS_1]</u> , Prof. <u>[PERSON_1]</u> . Note: <u>[WERT_1]</u> . Kommentar: 'Dozent erklärt gut, aber <u>[PERSON_2]</u> aus der Übung war unvorbereitet.'	Evaluationsbericht Kurs: <u>BWL-301</u> Dozent: Prof. <u>Dr. Andreas Keller</u> Gesamtnote: <u>2,3</u> Stärken: Verständliche Erklärungen in der Vorlesung. Handlungsbedarf: Übungsleitung (<u>Frau Schneider</u>) stärker einbinden und vorbereiten.

Pharma und Life Sciences



Die Pharmaindustrie und Life-Sciences-Branche verarbeiten klinische Studiendaten, Patienteninformationen und proprietäre Forschungsergebnisse. GxP-Regularien, FDA 21 CFR Part 11 und die EU-Verordnung über klinische Prüfungen stellen höchste Anforderungen an Datenintegrität und Vertraulichkeit. KI beschleunigt die Arzneimittelentwicklung um Jahre -- aber Studiendaten dürfen nicht in fremde Hände gelangen.

Die Herausforderung

- Klinische Studiendaten enthalten Patientennamen, Diagnosen und Behandlungsverläufe
- Proprietäre Wirkstoffdaten und Forschungsergebnisse sind Geschäftsgeheimnisse
- GxP-Compliance verlangt lückenlose Nachvollziehbarkeit jeder Datenverarbeitung
- Adverse Event Reports enthalten personenbezogene Meldungen über Nebenwirkungen

Anonix in der Praxis

PROMPT:

Erstelle aus diesen Daten einen strukturierten Adverse-Event-Report im CIOMS-Format.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Proband <u>ID-4821</u> , Prüfärztin: <u>Dr. Maria Engel</u> . Nebenwirkung: <u>Übelkeit Grad 2</u> nach <u>Compound XR-7</u> .	Proband <u>[ID_1]</u> , Prüfärztin: <u>[PERSON_1]</u> . Nebenwirkung: <u>[SYMPTOM_1]</u> nach <u>[WIRKSTOFF_1]</u> .	CIOMS Adverse Event Report Proband: <u>ID-4821</u> Prüfärztin: <u>Dr. Maria Engel</u> Ereignis: <u>Übelkeit Grad 2</u> Verdachtstoff: <u>Compound XR-7</u> Kausalität: möglich SAE: Nein Maßnahme: Symptomatische Therapie, Weiterbeobachtung

Softwareunternehmen und IT-Dienstleister



Softwareunternehmen und IT-Dienstleister integrieren LLM-APIs in ihre eigenen Produkte -- für Kunden aus allen Branchen. Sie tragen die Verantwortung dafür, dass die Daten ihrer Endkunden geschützt bleiben. Ein Datenschutzverstoß betrifft nicht nur das eigene Unternehmen, sondern alle Kunden, deren Daten über die API fließen. Anonix wird hier zur Infrastrukturkomponente, die in das eigene Produkt eingebaut wird.

Die Herausforderung

- Auftragsverarbeitung nach Art. 28 DSGVO: Der Softwareanbieter haftet für die Daten seiner Kunden
- Kundendaten aus regulierten Branchen (Gesundheit, Finanzen, Recht) fließen durch die API
- SOC-2- und ISO-27001-Zertifizierungen verlangen nachweisbare Datenschutzmaßnahmen
- Kunden fordern zunehmend Nachweise über DSGVO-konforme KI-Nutzung in Ausschreibungen

Anonix in der Praxis

PROMPT:

Formuliere aus diesen Bewerbungsdaten eine strukturierte Eingangsbestätigung an die Bewerberin.

ORIGINALDATEN	GESENDET AN DIE KI	ERGEBNIS (DE-ANONYMISIERT)
Bewerbung von <u>Anna Fischer</u> , <u>anna.fischer@email.de</u> , für <u>Senior</u> <u>Controller</u> bei <u>Autohaus Schmidt GmbH</u> . Gehaltswunsch: <u>EUR 85.000</u> .	Bewerbung von <u>[PERSON_1]</u> , <u>[EMAIL_1]</u> , für <u>[POSITION_1]</u> bei <u>[ORG_1]</u> . Gehaltswunsch: <u>[BETRAG_1]</u> .	Sehr geehrte <u>Frau Fischer</u> , vielen Dank für Ihre Bewerbung als <u>Senior Controller</u> bei der <u>Autohaus</u> <u>Schmidt GmbH</u> . Wir haben Ihre Unterlagen erhalten und prüfen diese sorgfältig. Sie hören innerhalb von 10 Werktagen von uns. Mit freundlichen Grüßen HR-Team der <u>Autohaus Schmidt GmbH</u>

Warum bestehende Lösungen scheitern



Es gibt durchaus Produkte, die personenbezogene Daten erkennen können. Aber keines davon löst das eigentliche Problem: den sicheren Einsatz von KI-APIs, ohne dass Daten das Unternehmen verlassen.

KRITERIUM	ANONIX	OPENROUTER®	MICROSOFT® PRESIDIO®	GOOGLE® CLOUD DLP	AWS® COMPREHEND
Transparenter KI-Proxy	Ja	Ja (KI-Gateway)	Nein	Nein	Nein
Unterstützte LLM-Anbieter	OpenAI® + alle kompatiblen, Claude®, Gemini®	400+ Modelle	Kein Proxy	Kein Proxy	Kein Proxy
Daten bleiben in der EU	Ja (EU-SaaS)	EU-Routing ab Business-Tarif	Ja	Google® Cloud	AWS® Cloud
Automatische De-Anonymisierung	Ja	Nein, nur Schwärzung	Nein	Nein	Nein
Branchenspezifische Erkennung	Zero-Shot NER	8 Typen + Regex	Nur Standard	150+ Typen	Nur Standard
Mehrsprachig (> 5 Sprachen)	8 Sprachen	Nicht dokumentiert	Teilweise	Ja	2 Sprachen
KI-gestützte Qualitätsprüfung	SLM-Review	Nein	Nein	Nein	Nein
Echtzeit-Streaming	SSE-Support	Keine De-Anonymisierung	Nein	Nein	Nein
Tippfehlertoleranz	Fuzzy-Matching	Nein	Nein	Nein	Nein
EU-konform einsetzbar	EU-SaaS	US Cloud Act	Open Source	US Cloud Act	US Cloud Act

Wo liegt der Unterschied?

OpenRouter® ist ein KI-Gateway mit über 400 Modellen und bietet seit Kurzem eine Schwärzung sensibler Daten an. Geprüft wird aber erst auf den Servern des US-Unternehmens, die Daten verlassen das Unternehmen also im Klartext. Die Schwärzung ist endgültig: Alle Namen werden zu [PERSON_NAME], die KI kann Personen nicht mehr unterscheiden, und die Antwort enthält keine Originaldaten. Namen und Adressen erkennt OpenRouter® nur als Beta-Funktion. Läuft diese Prüfung in eine Zeitüberschreitung, wird die Anfrage ungeschwärzt weitergeleitet.

Google® Cloud DLP und **AWS® Comprehend** erkennen zwar personenbezogene Daten, aber sie sind selbst Cloud-Dienste von US-Unternehmen. Auch der Umweg über AWS® Bedrock oder Microsoft® Azure® in einem EU-Rechenzentrum ändert nichts: Der CLOUD Act greift unabhängig vom Serverstandort, weil das Mutterunternehmen in den USA sitzt.

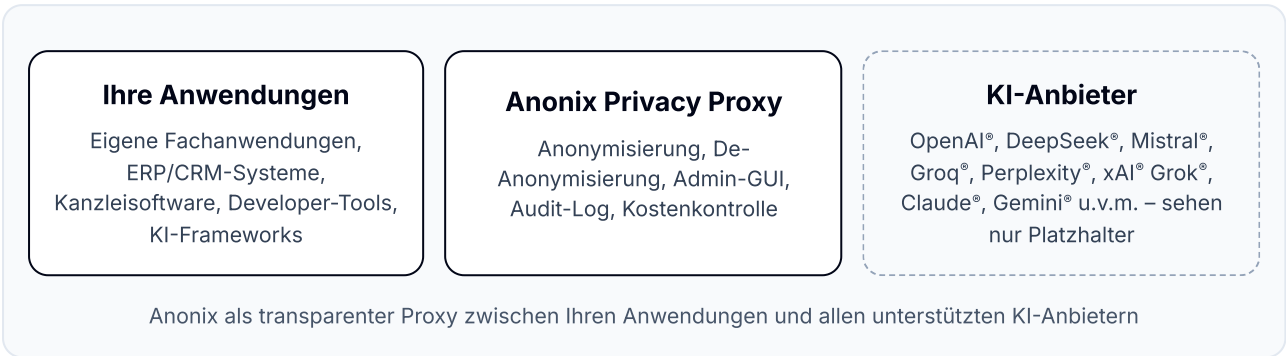
Microsoft® Presidio® ist Open Source und kann lokal betrieben werden. Aber es hat keine Proxy-Funktion, keine De-Anonymisierung und keine Zero-Shot-Erkennung. Es ist ein Werkzeugkasten, kein fertiges Produkt.

Anonix ist das einzige System, das alle drei Anforderungen in einem Produkt vereint: datenschutzkonforme KI-Erkennung, transparente LLM-Proxy-Integration und vollständige De-Anonymisierung der KI-Antwort.

Die Architektur auf einen Blick



Anonix besteht aus fünf Komponenten, die als vollständig verwalteter SaaS-Dienst in der EU betrieben werden. Kein einziges Byte personenbezogener Daten verlässt die europäische Infrastruktur.



Die fünf Bausteine

KOMPONENTE	AUFGABE	TECHNOLOGIE
Anonix Backend	Proxy-Engine, Anonymisierung, Benutzerverwaltung, API	Python® / FastAPI
Anonix Frontend	Admin-Oberfläche für Provider, Regeln, Audit-Log	React
Anonix ConvNet NER	Neuronales Netz zur Erkennung von Namen, Orten, Firmen	CNN-Microservice (8 Sprachen)
Anonix Zero-Shot NER	Branchenspezifische Erkennung ohne Training	Transformer-Microservice
KI-Qualitätsprüfung	Letzte Prüfschicht für übersehene Daten	Small Language Model (lokal oder API)

Sicherheit auf jeder Ebene

- AES-256-GCM-Verschlüsselung aller gespeicherten API-Keys
- Argon2id-Passwort-Hashing (militärischer Standard)
- Isolierte Datenbanken pro Mandant
- Zwei-Faktor-Authentifizierung (TOTP)
- Rate-Limiting und CSRF-Schutz
- Strukturiertes Audit-Logging

Investition und Wirtschaftlichkeit



Datenschutz muss kein Kostentreiber sein. Anonix kostet einen Bruchteil dessen, was ein einziger Datenschutzverstoß kosten würde. Und ermöglicht gleichzeitig den produktiven KI-Einsatz, den Ihre Mitarbeiter ohnehin schon fordern.

Was ein Verstoß kostet

530 Mio.

EUR BUSSGELD

TikTok (2025) wegen
rechtswidriger Datentransfers

45 Mio.

EUR BUSSGELD

Höchste Strafe in Deutschland
(Vodafone, 2025)

4%

DES JAHRESUMSATZES

Maximale DSGVO-Strafe für
Unternehmen

Was Anonix kostet

Anonix rechnet nach Nutzung – nicht nach Nutzern. Grundgebühr plus Preis pro Anonymisierungs-Request. Unbegrenzt viele Nutzer in jedem Paket.

VOLUMEN / MONAT	PREIS PRO REQUEST	IN EURO	BEMERKUNG
Bis 50.000	1,4 Cent	EUR 0,014	Einstieg / kleine Kunden
50.000 – 250.000	0,7 Cent	EUR 0,007	Standard / Mittelstand
Über 250.000	0,5 Cent	EUR 0,005	Enterprise / Großkunden

Grundgebühr: EUR 99 – 999 / Monat je nach Paket und Unternehmensgröße. Alle Preise zzgl. MwSt. SLM-Premium-Modul (KI-Qualitätsprüfung mit eigener GPU-Inferenz): +1,4 Cent pro Request.

Rechenbeispiel: 100 Mitarbeiter

Mitarbeiter	100
Requests/Monat	22.000
Grundgebühr	EUR 99
22.000 × EUR 0,014	EUR 308
Gesamt / Monat	EUR 407

Rechenbeispiel: 500 Mitarbeiter

Mitarbeiter	500
Requests/Monat	110.000
Grundgebühr	EUR 199
110.000 × EUR 0,007	EUR 770
Gesamt / Monat	EUR 969

Rechenbeispiel: 1.000 Mitarbeiter

Mitarbeiter	1.000
Requests/Monat	220.000
Grundgebühr	EUR 499
220.000 × EUR 0,007	EUR 1.540
Gesamt / Monat	EUR 2.039

Rechenbeispiel: 5.000 Mitarbeiter

Mitarbeiter	5.000
Requests/Monat	1.100.000
Grundgebühr	EUR 999
1.100.000 × EUR 0,005	EUR 5.500
Gesamt / Monat	EUR 6.499

Basis: ~10 KI-Anfragen pro Mitarbeiter pro Arbeitstag × 22 Arbeitstage = ca. 220 Requests pro Mitarbeiter und Monat. Je mehr Ihr Unternehmen KI nutzt, desto günstiger wird jeder einzelne Request.

Alle Preise sind Nettopreise zzgl. MwSt.

Die Rechnung ist einfach: Die Jahreskosten von Anonix entsprechen einem Bruchteil eines einzigen DSGVO-Bußgeldes. Und sie sind günstiger als ein einziger Tag Produktivitätsverlust, wenn Sie KI komplett verbieten müssen.

Compliance auf Knopfdruck



Datenschutz ist kein Projekt mit Anfang und Ende. Es ist ein laufender Prozess. Anonix automatisiert die technischen Maßnahmen, die Regulierungsbehörden verlangen.

DSGVO-Konformität

- ✓ **Art. 5 Abs. 1 lit. c (Datenminimierung)** – Nur Platzhalter erreichen den KI-Anbieter. Personenbezogene Daten werden auf das technisch notwendige Minimum reduziert.
- ✓ **Art. 25 (Data Protection by Design)** – Die Anonymisierung ist dem API-Aufruf vorgeschaltet. Ohne Proxy-Konfiguration ist keine ungeschützte Nutzung möglich.
- ✓ **Art. 32 (Sicherheit der Verarbeitung)** – AES-256-Verschlüsselung, Argon2id-Hashing, Zwei-Faktor-Authentifizierung und isolierte Mandantendatenbanken.
- ✓ **Art. 28 (Auftragsverarbeitung)** – Der KI-Anbieter sieht keine personenbezogenen Daten. Die Anforderungen an den Auftragsverarbeiter reduzieren sich erheblich.
- ✓ **Art. 30 (Verzeichnis der Verarbeitungstätigkeiten)** – Vollständiges Audit-Log mit lückenloser Protokollierung aller Proxy-Anfragen.

CLOUD Act und Drittlandtransfer

Architektonische Garantie: Selbst wenn US-Behörden den KI-Anbieter zur Herausgabe von Daten verpflichten, erhalten sie nur anonymisierte Textfragmente mit Platzhaltern. Anonix speichert kein Mapping zwischen Platzhaltern und Originaldaten. Die Zuordnung existiert nur während der Verarbeitung im Arbeitsspeicher und wird danach sofort verworfen. Die Originaldaten verbleiben ausschließlich beim Kunden. Eine Re-Identifikation ist technisch ausgeschlossen.

EU AI Act (Verordnung 2024/1689)

Anonix ist ein Datenminimierungstool und fällt in keine Hochrisiko-Kategorie des EU AI Act. Es trifft keine automatisierten Entscheidungen über Personen, erstellt keine Profile und beeinflusst keine Rechte. Vielmehr reduziert es die Risiken, die von den eigentlichen Hochrisiko-Anwendungen (den externen KI-Modellen) ausgehen.

Branchenspezifische Compliance

REGULIERUNG	BRANCHE	WIE ANONIX HILFT
Paragraph 203 StGB	Anwälte, Steuerberater, Ärzte	Berufsgeheimnis bleibt gewahrt, da keine Mandanten-/Patientendaten übermittelt werden
DORA (EU 2022/2554)	Banken, Versicherungen	IKT-Risikomanagement durch kontrollierte KI-Nutzung
Landesdatenschutzgesetze	Öffentliche Verwaltung	Bürgerdaten bleiben auf kommunaler/Landesinfrastruktur
SGB (Sozialdatenschutz)	Sozialträger, Jugendämter	Sozialdaten werden vor externer Verarbeitung anonymisiert

Stimmen aus der Praxis



Die Herausforderung ist branchenübergreifend dieselbe: Wie lässt sich der Produktivitätsgewinn durch KI nutzen, ohne die Kontrolle über sensible Daten zu verlieren? Drei Perspektiven.

„Wir hatten zwei Optionen: KI komplett verbieten oder einen Weg finden, sie datenschutzkonform einzusetzen. Ersteres hätte uns gegenüber dem Wettbewerb zurückgeworfen. Mit Anonix können unsere Mitarbeiter jetzt offiziell KI-Tools nutzen. Unser Datenschutzbeauftragter hat das Konzept geprüft und freigegeben. Der entscheidende Punkt war, dass personenbezogene Daten unsere Server tatsächlich nie verlassen.“

DR. KATHARINA SOMMER, DATENSCHUTZBEAUFTRAGTE, MITTELSTÄNDISCHES VERSICHERUNGSUNTERNEHMEN

„Als IT-Leiter einer Kommune hatte ich ein klares Problem: Unsere Fachanwendungen sollten KI-gestützte Textverarbeitung bekommen, aber der Datenschutzbeauftragte hat jede direkte API-Anbindung an US-Anbieter blockiert. Anonix hat uns eine saubere Lösung gegeben. Wir haben die API-Keys in unseren Systemen auf den Anonix Proxy umgestellt und fertig. Der SaaS-Dienst läuft in der EU, kein einziger Bürgername geht mehr an die KI-Anbieter.“

MICHAEL BRANDT, IT-LEITER, STADTVERWALTUNG (CA. 120.000 EINWOHNER)

„In unserer Kanzlei arbeiten 14 Anwälte. Jeder von uns könnte die KI gebrauchen, um Schriftsätze zu prüfen, Urteile zusammenzufassen oder Vertragsklauseln zu formulieren. Aber das Mandantengeheimnis steht über allem. Mit Anonix kann ich meinen Kollegen jetzt guten Gewissens sagen: Nutzt die KI. Eure Mandantendaten sind geschützt. Und das Beste: Es hat keine zwei Stunden gedauert, bis alles lief.“

DR. FLORIAN HARTMANN, PARTNER, WIRTSCHAFTSKANZLEI

Hinweis: Die hier dargestellten Erfahrungsberichte illustrieren typische Einsatzszenarien und Herausforderungen, wie sie in Gesprächen mit potenziellen Anwendern aus den jeweiligen Branchen beschrieben werden.

Ihr Weg zu Anonix



Anonix ist so konzipiert, dass Sie in wenigen Tagen von der ersten Kontaktaufnahme zur produktiven Nutzung gelangen. Keine langwierigen Implementierungsprojekte, kein Umbau Ihrer bestehenden Systeme.

1

Beratungsgespräch

Wir analysieren Ihre Anforderungen: Welche KI-Anbieter nutzen Sie? Welche Datentypen müssen geschützt werden? Welche branchenspezifischen Regeln gelten?

2

Pilotphase

Zugang zu Ihrem Anonix SaaS-Konto. Konfiguration der Anonymisierungsregeln. Testbetrieb mit einem Team.

3

Produktivbetrieb

Rollout auf alle Arbeitsplätze. API-Keys tauschen, fertig. Laufende Betreuung, automatische Updates und Support inklusive.

Bereitstellung

Anonix wird als vollständig verwalteter SaaS-Dienst bereitgestellt. Hosting, Updates, Wartung und Support sind im Paket enthalten. Sie können sich auf Ihr Kerngeschäft konzentrieren, während wir die Infrastruktur betreiben – selbstverständlich ausschließlich auf EU-Servern.

OPTION	BESCHREIBUNG	GEEIGNET FÜR
Anonix SaaS	Vollständig verwaltete Lösung auf EU-Infrastruktur. Hosting, Updates und Support inklusive. Sofort einsatzbereit.	Unternehmen, Behörden, Kanzleien, Praxen
Enterprise On-Premise	Für Organisationen mit besonderen Anforderungen an die Datenhoheit bieten wir auf Anfrage auch eine dedizierte On-Premise-Installation an.	Auf Anfrage

Bereit für den nächsten Schritt?

Lassen Sie uns gemeinsam herausfinden, wie Anonix in Ihre Organisation passt.

info@anonix.ai • www.anonix.ai

Impressum



Urheber-, Marken- und Lizenzrechte

Alle Urheber-, Marken- und Lizenzrechte an Anonix Privacy Proxy und diesem Dokument liegen bei der:

Unternehmen	Convecto GmbH
Anschrift	Ludwigstraße 180d, 63067 Offenbach
Telefon	+49 69 40897270
Web	www.convecto.com

Trademarks

Anonix, Anonix Privacy Proxy, Anonix ConvNet NER und Anonix Zero-Shot NER sind Trademarks der Convecto GmbH. OpenAI®, GPT®, Anthropic®, Claude®, Google®, Gemini®, Microsoft®, DeepSeek®, Mistral®, xAI®, Grok®, Groq®, Perplexity®, Together AI®, OpenRouter®, Ollama®, LM Studio®, Cursor®, GitHub® Copilot®, LangChain®, LlamaIndex® und AWS® sind Trademarks ihrer jeweiligen Inhaber.

© 2000–2026 Convecto GmbH. Alle Rechte vorbehalten.

Die in diesem Dokument enthaltenen Informationen wurden mit größter Sorgfalt zusammengestellt. Für die Richtigkeit, Vollständigkeit und Aktualität wird jedoch keine Gewähr übernommen.