basebox
KI-Plattform

Datenschutz und Informationssicherheit – Kurzübersicht

basebox KI-Plattform · Stand: 12. November 2026

1. Auf einen Blick

Thema	Status
ISO 27001	Zertifiziert. Informationssicherheit der basebox GmbH.
BSI C5 Typ 1	In Arbeit. Vorprüfung und Testierung für die Cloud sind terminiert.
DSGVO	Erfüllt. AVV, TOMs, Verarbeitung in Deutschland.
§ 203 StGB	Erfüllt. Vereinbarung für Berufsgeheimnisträger.
EU AI Act	basebox unterstützt Sie mit Schulungen, Modellregister und Protokollen.
Cyber Resilience Act	In Arbeit. Software-Stückliste (SBOM) vorhanden.
NIS2, KRITIS, B3S Krankenhaus, BSI IT-Grundschutz	basebox liefert die Nachweise für Ihre Pflichten.
ISO 13485	Nicht nötig. Die KI-Plattform ist kein Medizinprodukt.
TISAX, SOC 2	Kein Label. ISO 27001 ist die Grundlage.

2. Betriebswege: Wer verarbeitet Ihre Daten?

	Cloud	Server, Betrieb durch basebox	Server, Betrieb durch Ihre IT	Übergangsumgebung bis November 2026
Wo die Daten liegen	Rechenzentrum in Deutschland (München-Ost)	Ihr Haus oder ein Rechenzentrum Ihrer Wahl (Standard noris network, München-Ost)	Ihr Haus	Rechenzentrum in Deutschland (Nürnberg)
Trennung von anderen Kunden	Eigene Umgebung je Organisation	Ihr Server	Ihre Infrastruktur	Gemeinsame Umgebung, logische Trennung über Mandanten
Verarbeitet basebox Daten in Ihrem Auftrag?	Ja	Ja, für Betrieb, Wartung und Support	Nur beim Support, wenn Sie dafür Zugriff geben	Ja

basebox GmbH
info@basebox.ai
www.basebox.ai

Geschäftsführer
René Herzer
HRB37614 Amtsgericht Augsburg
USt-IdNr. DE 354674574

Bahnhofplatz 3
86919 Utting am Ammersee
+49 8806 9590600

	Cloud	Server, Betrieb durch basebox	Server, Betrieb durch Ihre IT	Übergangsumgebung bis November 2026
AVV und TOMs	Teil des Vertrags	Teil des Vertrags	Teil des Vertrags	Teil des Vertrags
Zugriff durch basebox	basebox betreibt die Umgebung	Nur nach Ihrer Freigabe, über ein sicheres Zugriffsverfahren	Nur für Support, über Zugänge, die Sie bereitstellen	basebox betreibt die Umgebung
Protokolle	In Ihrer Cloud-Umgebung	Bei Ihnen	Bei Ihnen	In Ihrem Mandanten
Backup	Täglich, Aufbewahrung 7 Tage; 30 Tage und verschlüsselte Kopie in einem zweiten Rechenzentrum in Deutschland im Aufbau	Bei Ihnen; basebox richtet die Sicherung ein	Bei Ihnen	Täglich, Aufbewahrung bis zu 7 Tage

Gesundheitsdaten und andere besondere Kategorien nach Art. 9 DSGVO verarbeiten Sie am besten nicht in der Übergangsumgebung, sondern in der Cloud oder auf dem Server.

3. Datenschutz

- basebox verarbeitet Daten nur auf Ihre Weisung.
- Patienten-, Bürger- und Sozialdaten dürfen verarbeitet werden, auf dem Server und in der Cloud.
- Unterauftragsverarbeiter setzt basebox nur ein, wenn sie im Vertrag genannt sind. Über geplante Änderungen informiert basebox Sie vorab, und Sie können widersprechen.
- Verletzungen des Schutzes Ihrer Daten meldet basebox Ihnen unverzüglich, spätestens innerhalb von 12 Stunden (Art. 33 Abs. 2 DSGVO).
- basebox unterstützt Sie bei Anfragen von Betroffenen und bei Ihrer Datenschutz-Folgenabschätzung.
- Nach Vertragsende löscht basebox alle Daten oder übergibt sie Ihnen.
- Sie müssen Ihre Daten nicht anonymisieren. Die Daten bleiben in Ihrem Rahmen, und die KI arbeitet mit den vollständigen Unterlagen.
- Für Berufsgeheimnisträger gilt die Vereinbarung nach § 203 StGB. Alle Beschäftigten von basebox sind zur Verschwiegenheit verpflichtet.

4. Modelle und Training

- Ihre Daten trainieren kein Modell. Eingaben, Dokumente und Antworten werden nicht im Modell gespeichert.
- Anbieter von KI-Diensten setzt basebox nur ein, wenn deren Vertrag ein Training mit Ihren Daten ausschließt.
- Das Modellregister dokumentiert Entwickler, Version und Lizenz jedes eingesetzten Modells.
- Ein externes Modell gibt es in der Cloud und beim Server nur als eigene App, wenn Sie sie einrichten lassen. Ihr Administrator gibt sie für ausgewählte Gruppen frei. basebox stellt dafür ausgewählte Modelle von Anthropic über Google Vertex in der EU bereit. Google trainiert nicht mit Ihren Daten und protokolliert zur Missbrauchserkennung längstens 30 Tage. Weil Google ein US-Unternehmen ist, gilt dort der US Cloud Act. Auf Ihren Wunsch stellt basebox auch Modelle von OpenAI oder Google bereit; für OpenAI gilt ebenfalls der US Cloud Act. Ob Sie diese Modelle nutzen, bewerten Sie datenschutzrechtlich selbst. In der Übergangsumgebung bis November 2026 kommen alle KI-Modelle von Google Vertex.

5. Websuche

- Die Websuche ist standardmäßig ausgeschaltet. Sie steht auf allen Betriebswegen zur Verfügung, wenn Sie sie freischalten.
- Die Suche läuft über Staan.ai in der EU. basebox hat mit Staan einen AVV, ein Training mit den Suchanfragen ist ausgeschlossen.
- Übertragen wird nur der Suchbegriff, ohne Identität der Person und ohne IP-Adresse.
- Die Websuche hat keinen Zugang zu Ihren internen Daten. Webinhalte gelten als Daten, nicht als Befehle.

6. Datenfluss beim Server

- Von Ihrem Server zu basebox wird nichts übertragen: keine Telemetrie, keine Lizenzabfrage, keine Update-Prüfung nach außen.
- Software und Modelle kommen bei Installation und Update in Ihre Umgebung. Ohne Internet geschieht das als Offline-Paket.
- Nach außen geht nur, was Sie selbst freischalten oder einrichten: die Websuche, angebundene Systeme, Apps mit externem oder größerem Modell, ein SMS-Dienst für die Zwei-Faktor-Anmeldung, Ihr SIEM, ein externes Backup-Ziel und, mit Betrieb durch basebox, die dritte Kopie der Sicherungen und der zweite Standort (Standby).

7. Rechte

- Die KI darf nie mehr als die Person, die sie nutzt.
- Rollen und Gruppen kommen aus Ihrer bestehenden Benutzerverwaltung.

- Konnektoren greifen mit dem Zugang der Person auf Ihre Systeme zu, nicht über ein Dienstkonto.
- Agenten handeln immer im Namen einer Person. Schreiben ist standardmäßig ausgeschaltet, und schreibende Aktionen brauchen eine Freigabe.

8. Protokolle, Löschen, Sicherung

- Das Audit-Log hält fest, wer was wann getan hat. Es enthält nur Kennungen, keine Namen oder E-Mail-Adressen. Einträge sind nicht änderbar. Export als CSV, auf Anfrage für Ihr SIEM.
- Inhalte von Fragen und Antworten werden nur protokolliert, wenn Ihre Organisation das einschaltet. Das entscheiden Sie.
- Die Personen löschen ihre Chats und Dokumente selbst, Ihre Administratoren alles Weitere.
- Beim Server liegen alle Protokolle und Sicherungen bei Ihnen. Mit Betrieb durch basebox hält basebox eine dritte Kopie der Sicherungen bei noris network in Nürnberg; sonst hat basebox keine Kopie.

9. Nachvollziehbarkeit

- Jede Aussage aus Dokumenten trägt eine Quellenangabe mit der zitierten Textstelle.
- Welches Modell in welcher Version geantwortet hat, ist dokumentiert.
- Die Fachperson prüft an der Quelle und verantwortet die Verwendung.

10. Betriebs- und Personalrat

- Protokolliert wird zur Sicherheit, nicht zur Leistungskontrolle.
- Es entstehen keine neuen Profile und keine zweite Datenhaltung.

11. Unterlagen

Sofort oder vor Vertragsschluss erhalten Sie: AVV, Liste der Unterauftragsverarbeiter, TOMs, Vereinbarung nach § 203 StGB, ISO-27001-Zertifikat, SBOM und eine Vorlage für Ihr Verzeichnis von Verarbeitungstätigkeiten.

Kontakt

Datenschutz: datenschutz@basebox.ai
Sicherheitslücken: security@basebox.ai