basebox
KI-Plattform

Verzeichnis von Verarbeitungstätigkeiten
Vorlage für den Einsatz der basebox KI-Plattform

Stand: 1. November 2026

So nutzen Sie diese Vorlage

Als Verantwortlicher führen Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten (Art. 30 Abs. 1 DSGVO). Diese Vorlage hilft Ihnen beim Eintrag für die KI-Plattform von basebox.

- Legen Sie für jeden Einsatzzweck einen eigenen Eintrag an, zum Beispiel einen für Arztbriefe und einen für die Suche in Leitlinien.
- Die Angaben zu basebox sind vorausgefüllt.
- Beispiele sind mit *[Beispiel]* markiert. Ersetzen oder löschen Sie sie.
- Felder mit „Ihre Angabe“ füllen Sie aus.
- Die Vorlage ersetzt nicht Ihre eigene datenschutzrechtliche Bewertung.

1. Bezeichnung der Verarbeitungstätigkeit

Ihre Angabe:
[Beispiel] Entwürfe für Arztbriefe mit der KI-Plattform

2. Verantwortlicher (Art. 30 Abs. 1 lit. a DSGVO)

Feld	Angabe
Name und Anschrift	Ihre Angabe
Vertreter, falls vorhanden	Ihre Angabe
Datenschutzbeauftragter	Ihre Angabe
Fachlich zuständige Stelle	Ihre Angabe

3. Zwecke der Verarbeitung (lit. b)

Ihre Angabe:
[Beispiel] Unterstützung von Ärztinnen und Ärzten beim Verfassen von Arztbriefen. Die Fachperson prüft jeden Entwurf und gibt ihn frei.

4. Rechtsgrundlage

Art. 30 DSGVO verlangt diese Angabe nicht. Viele Verzeichnisse führen sie trotzdem.

Ihre Angabe:

5. Kategorien betroffener Personen (lit. c)

Immer betroffen:

- Nutzerinnen und Nutzer der KI-Plattform (Ihre Beschäftigten)

Je nach Einsatz – bitte auswählen:

- Patientinnen und Patienten
- Bürgerinnen und Bürger
- Versicherte oder Leistungsempfänger
- Geschäftspartner, Lieferanten
- Sonstige: Ihre Angabe

6. Kategorien personenbezogener Daten (lit. c)

Immer verarbeitet:

- Nutzerdaten aus Ihrer bestehenden Benutzerverwaltung: Kennung, Rolle, Gruppe
- Anmelde- und Berechtigungsdaten
- Audit-Log: wer wann welche App und welchen Konnektor genutzt hat. Es enthält nur Kennungen, keine Namen oder E-Mail-Adressen.

Je nach Nutzung:

- Fragen und Eingaben der Personen, die die KI-Plattform nutzen
- Hochgeladene Dokumente und angebundene Wissensquellen
- Antworten der KI
- Chatverläufe
- Suchbegriffe, wenn Sie die Websuche freischalten
- Inhalte von Fragen und Antworten im Protokoll, nur wenn Sie die ausführliche Protokollierung einschalten

Besondere Kategorien nach Art. 9 DSGVO, zum Beispiel Gesundheitsdaten oder genetische Daten:
Ja / Nein – Ihre Angabe

7. Empfänger (lit. d)

Intern:

- Nur Personen, denen Sie die jeweilige App freigegeben haben. Rollen und Gruppen kommen aus Ihrer Benutzerverwaltung. Die KI sieht nie mehr als die Person, die sie nutzt.

basebox
KI-Plattform

Auftragsverarbeiter:

- basebox GmbH, Bahnhofplatz 3, 86919 Utting am Ammersee
- Datenschutzkontakt: datenschutz@basebox.ai
- Datenschutzbeauftragter: Philipp Gärtner
- Grundlage: Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO
- Beim Server mit Betrieb durch Ihre IT verarbeitet basebox Ihre Daten nur, wenn Sie für den Support Zugriff geben.

Unterauftragsverarbeiter von basebox:

Anbieter	Leistung	Ort	Wann eingesetzt
STACKIT GmbH & Co. KG	Zusätzliche Rechenleistung für das KI-Modell	Deutschland	Nur Cloud
Mistral AI SAS	Zusätzliche Rechenleistung, auf Wunsch statt STACKIT	EU (Frankreich)	Nur Cloud, nur wenn vereinbart
noris network AG	Rechenzentrum	Deutschland (München Ost)	Cloud; Server mit Betrieb durch basebox im Rechenzentrum, wenn Sie noris network wählen; zweiter Standort (Standby), wenn vereinbart; größeres Modell für Apps beim Server
FAST LTA GmbH	Server und Hardware-Service	Deutschland (München Ost)	Cloud; größeres Modell für Apps beim Server
Hetzner Online GmbH	Hosting der KI-Plattform	Deutschland (Nürnberg)	Nur Übergangsumgebung (Konten vor dem Start der Cloud im November 2026)
Staan.ai	Websuche. Kein Training mit den Suchanfragen. Übertragen wird nur der Suchbegriff, ohne Identität der Person.	EU	Alle Betriebswege und Übergangsumgebung, nur wenn Sie die Websuche freischalten
Google Ireland Ltd. / Google LLC	Ausgewählte externe KI-Modelle (Modelle von Anthropic, auf Ihren Wunsch auch von Google) über Google Vertex AI. Kein Training, Protokollierung zur Missbrauchserkennung längstens 30 Tage.	EU	Cloud und Server, nur wenn Sie eine App mit externem Modell freischalten; in der Übergangsumgebung bis November 2026 für alle KI-Modelle

Anbieter	Leistung	Ort	Wann eingesetzt
OpenAI Ireland Ltd. / OpenAI, L.L.C.	Modelle von OpenAI, nur auf Ihren Wunsch. Nach den Bedingungen von OpenAI kein Training; Protokollierung zur Missbrauchserkennung bis zu 30 Tage, länger nur, wenn gesetzlich vorgeschrieben oder zum Schutz vor Schäden nötig.	USA oder EU, gemäß Angebot	Cloud und Server, nur wenn Sie eine App mit einem Modell von OpenAI freischalten

Beim Server in Ihrem Haus setzt basebox keine Unterauftragsverarbeiter für Infrastruktur ein. Steht der Server mit Betrieb durch basebox im Rechenzentrum, ist der von Ihnen gewählte Rechenzentrumsbetreiber Unterauftragsverarbeiter (Standard noris network AG, München-Ost; auf Wunsch Synaforce oder ein anderes Rechenzentrum Ihrer Wahl). Die Websuche läuft über Staan.ai, wenn Sie sie freischalten.

Ihr Betriebsweg (bitte auswählen):

- Cloud
- Server, Betrieb durch basebox (bei Ihnen oder im Rechenzentrum)
- Server, Betrieb durch Ihre IT
- Übergangsumgebung bis zum Start der Cloud im November 2026

Ihre Angabe: Websuche freigeschaltet Ja / Nein

8. Übermittlung in Drittländer (lit. e)

Standard: keine. Das KI-Modell in basebox läuft auf Servern in Deutschland oder auf Ihrem Server. Die Websuche läuft in der EU.

Nur bei freigeschaltetem externem Modell (Google Vertex AI) und in der Übergangsumgebung bis November 2026: Die Verarbeitung erfolgt in der EU. Weil Google ein US-Unternehmen ist, kann ein Zugriff nach dem US Cloud Act nicht ausgeschlossen werden. Für Modelle von OpenAI, wenn Sie sie wünschen: Die Verarbeitung kann auch in den USA erfolgen; der US Cloud Act gilt. Anbieter, die Sie mit eigenem Vertrag anbinden, tragen Sie hier selbst ein.

Ihre Angabe: externes Modell freigeschaltet Ja / Nein

9. Löschfristen (lit. f)

Die Fristen legen Sie fest: Ihre Angabe

So setzen Sie sie in der KI-Plattform um:

- Die Personen löschen ihre Chats und Dokumente selbst.
- Ihre Administratoren löschen alles Weitere.
- Einträge im Audit-Log sind nicht änderbar und nicht einzeln löschbar. Legen Sie die Aufbewahrungsdauer fest.
- Beim Server liegen alle Protokolle und Sicherungen bei Ihnen. In der Cloud laufen gelöschte Daten mit den Sicherungen nach 7 Tagen aus.
- Beim externen Modell protokolliert Google zur Missbrauchserkennung längstens 30 Tage.
- Nach Vertragsende löscht basebox alle Daten oder übergibt sie Ihnen (AVV, Ziffer 18).

10. Technische und organisatorische Maßnahmen (lit. g)

Maßnahmen von basebox (Einzelheiten in der TOM-Anlage zum AVV):

- Informationssicherheit der basebox GmbH nach ISO 27001 zertifiziert
- Rollen und Rechte aus Ihrer Benutzerverwaltung, die KI hat nie mehr Rechte als die Person
- Ihre Daten trainieren kein Modell
- Verarbeitung in Deutschland oder auf Ihrem Server; Websuche in der EU; externes Modell siehe Abschnitt 8
- Fernzugriff durch basebox nur über ein vereinbartes sicheres Verfahren (VPN, PAM oder Bastion Host)
- Audit-Log mit Export als CSV, auf Anfrage für Ihr SIEM
- Betrieb ohne Internet auf dem Server möglich

Ihre Maßnahmen (Infrastruktur, Netzwerk, Backup, Zugänge):
Ihre Angabe

11. Datenschutz-Folgenabschätzung

Erforderlich: Ja / Nein – Ihre Angabe

Bei KI mit Gesundheits- oder Sozialdaten ist eine Folgenabschätzung in der Regel nötig. Sie erstellen und verantworten sie. basebox unterstützt Sie dabei (AVV, Ziffer 17).

12. Stand des Eintrags

Datum, Bearbeiter: Ihre Angabe