basebox
KI-Plattform

Anlage: Technische und organisatorische Maßnahmen basebox KI-Plattform

Version: 1. November 2026

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

Nr.	Bereich	Maßnahme / Regelung
1 (1)	Geltung	Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO für die basebox KI-Plattform.
1 (2)	Geltung	Diese Anlage gilt für die Betriebswege: a) Cloud, b) Server, Betrieb durch basebox (beim Kunden oder im Rechenzentrum), c) Server, Betrieb durch die IT des Kunden, d) Übergangsumgebung bis zum Start der Cloud im November 2026 (Ziffer 1 (6)). Als Server gelten Server von basebox und vom Kunden selbst beschaffte Hardware.
1 (3)	Geltung	Die Maßnahmen gelten jeweils nur für den Verantwortungsbereich von basebox im vereinbarten Betriebsweg.
1 (4)	Geltung	Für kundenseitig bereitgestellte Infrastruktur, Netzwerke, Systeme, Zugänge, Backups, Monitoring, Logs, Sicherheitsmaßnahmen und Betriebsprozesse ist der Kunde verantwortlich, soweit im Angebot nichts Abweichendes vereinbart ist.
1 (5)	Geltung	basebox betreibt ein Informationssicherheitsmanagementsystem nach ISO/IEC 27001 im Umfang des jeweils gültigen Zertifikats.
1 (6)	Geltung	Konten, die vor dem Start der Cloud im November 2026 entstehen, laufen bis dahin in einer von basebox betriebenen, gemeinsam genutzten Übergangsumgebung bei einem in der Liste der Unterauftragsverarbeiter genannten Hosting-Anbieter (Hetzner, Nürnberg). Die Kunden sind dort als Mandanten logisch voneinander getrennt. Eine eigene Umgebung und eine eigene Benutzerverwaltung je Kunde gibt es dort nicht. Die KI-Modelle kommen bis dahin von Google Vertex in Frankfurt; Google verwendet die Eingaben nicht für Training und protokolliert sie zur Missbrauchserkennung längstens 30 Tage. Mit dem Start der Cloud zieht basebox diese Konten in die Cloud um.
1 (7)	Geltung	Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO verarbeitet der Kunde nach Empfehlung von basebox nicht in der Übergangsumgebung, sondern in der Cloud oder auf dem Server.
2	Verantwortungsmatrix	Siehe Tabelle „Verantwortungsmatrix nach Betriebsweg“ unten.

Nr.	Bereich	Maßnahme / Regelung
3 a)	Verschlüsselung	Verschlüsselte Verbindungen, insbesondere HTTPS/TLS nach Stand der Technik
3 b)	Verschlüsselung	Einsatz vertrauenswürdiger Zertifikate
3 c)	Verschlüsselung	Verschlüsselung von Kommunikation, soweit angemessen
3 d)	Verschlüsselung	Verschlüsselung von Speichermedien, Datenträgern oder Systemen, soweit technisch vorgesehen
3 e)	Verschlüsselung	Schutz kryptografischer Schlüssel durch angemessene Zugriffsbeschränkungen
3 f)	Verschlüsselung	Einsatz kryptografischer Verfahren nach Stand der Technik
4 a)	Zugriffskontrolle	Individuelle Benutzerkennungen
4 b)	Zugriffskontrolle	Rollen- und berechtigungsbasierte Zugriffskonzepte
4 c)	Zugriffskontrolle	Dokumentation von Berechtigungen
4 d)	Zugriffskontrolle	Starke Passwörter oder vergleichbare Authentifizierungsverfahren
4 e)	Zugriffskontrolle	Mehr-Faktor-Authentifizierung bei besonders schutzbedürftigen oder administrativen Zugriffen, soweit technisch vorgesehen
4 f)	Zugriffskontrolle	Beschränkung administrativer Zugriffe auf berechtigte Personen
4 g)	Zugriffskontrolle	Regelmäßige Überprüfung von Zugriffsrechten
5 a)	Vertraulichkeit	Verpflichtung von Mitarbeitenden auf Vertraulichkeit
5 b)	Vertraulichkeit	Datenschutz- und Sicherheitsrichtlinien
5 c)	Vertraulichkeit	Schulung und Sensibilisierung der Mitarbeitenden
5 d)	Vertraulichkeit	Zugriff nur nach Erforderlichkeit
5 e)	Vertraulichkeit	Sichere Zugriffsverfahren für Fernwartung, insbesondere PAM, VPN, Bastion Host oder vergleichbare Verfahren, soweit eingesetzt

Nr.	Bereich	Maßnahme / Regelung
5 f)	Vertraulichkeit	Physische Schutzmaßnahmen für Standorte (Zutritt, Strom, Kühlung, Brandschutz), soweit diese im Verantwortungsbereich von basebox oder eingesetzter Unterauftragsverarbeiter liegen. In der Cloud und beim Server im Rechenzentrum verantwortet sie der Rechenzentrumsbetreiber als Unterauftragsverarbeiter; steht der Server beim Kunden, der Kunde.
6 a)	Integrität	Einsatz geeigneter Firewalls und Schutzmechanismen
6 b)	Integrität	Protokollierung administrativer und sicherheitsrelevanter Vorgänge
6 c)	Integrität	Einsatz von Rollen- und Berechtigungskonzepten
6 d)	Integrität	Schutz vor unbefugter Änderung von Daten und Systemen
6 e)	Integrität	Durchführung administrativer Tätigkeiten nur durch geeignete und geschulte Personen
6 f)	Integrität	Technische und organisatorische Maßnahmen zur Nachvollziehbarkeit von Änderungen
7 a)	Verfügbarkeit, Backup	Backup-Verfahren, soweit im Betriebsweg oder Angebot durch basebox geschuldet; in der Cloud täglich, Aufbewahrung 7 Tage; 30 Tage und verschlüsselte Kopie in einem zweiten Rechenzentrum in Deutschland im Aufbau
7 b)	Verfügbarkeit, Backup	Notfall- und Wiederherstellungsprozesse; beim Server mit Betrieb durch basebox optional ein zweiter Standort (Standby) bei der noris network AG mit einem Umschalttest pro Jahr und Protokoll
7 c)	Verfügbarkeit, Backup	Geeignete Datensicherungsmaßnahmen
7 d)	Verfügbarkeit, Backup	Wiederherstellungstests in angemessenem Umfang
7 e)	Verfügbarkeit, Backup	Vertretungsregelungen
7 f)	Verfügbarkeit, Backup	Schutzmaßnahmen gegen zufällige Zerstörung oder Verlust
7	Verfügbarkeit, Backup	Beim Server liegen Sicherung, Wiederherstellung und Verfügbarkeit der kundenseitigen Infrastruktur beim Kunden, soweit im Angebot nichts Abweichendes vereinbart ist. Beim Server mit Betrieb durch basebox richtet basebox die Sicherung ein.

Nr.	Bereich	Maßnahme / Regelung
8 a)	Patch- und Schwachstellenmanagement	Patch- und Updateprozesse
8 b)	Patch- und Schwachstellenmanagement	Regelmäßige Auswertung von Informationen zu Sicherheitslücken
8 c)	Patch- und Schwachstellenmanagement	Inventarisierung wesentlicher Softwareversionen und Komponenten
8 d)	Patch- und Schwachstellenmanagement	Sicherheitsupdates nach Risikobewertung
8 e)	Patch- und Schwachstellenmanagement	Log-Auswertung zur Erkennung ungewöhnlicher Ereignisse
8 f)	Patch- und Schwachstellenmanagement	Penetrationstests oder vergleichbare Sicherheitsprüfungen in angemessenem Umfang
9 (1)	Protokollierung	Die basebox KI-Plattform kann technische Protokolle und Audit Logs erzeugen.
9 (2)	Protokollierung	Protokollierung und Monitoring dienen insbesondere der Sicherheit, Stabilität, Nachvollziehbarkeit, Fehleranalyse und Betriebsunterstützung.
9 (3)	Protokollierung	Inhalte von Fragen, Eingaben und Antworten werden nur im Audit Log erfasst, wenn der Kunde die ausführliche Protokollierung einschaltet; die Personen sehen dann im Chat einen Hinweis, der sich nicht abschalten lässt.
9 (4)	Protokollierung	Der Kunde ist verantwortlich für die datenschutzrechtliche Bewertung und Konfiguration des Audit Loggings.
9 (5)	Protokollierung	Beim Server ist der Kunde für Speicherung, Aufbewahrung, Zugriff, Export, Löschung und Auswertung von Logs verantwortlich, soweit diese auf Kundeninfrastruktur verarbeitet werden und nichts Abweichendes vereinbart ist.
10 (1)	KI-spezifische Maßnahmen	Kundendaten, insbesondere Fragen, Eingaben, Dokumente, Antworten und Protokolldaten, werden nicht zum Training von KI-Modellen verwendet, soweit im Angebot nichts Abweichendes ausdrücklich vereinbart ist.
10 (2)	KI-spezifische Maßnahmen	basebox setzt Unterauftragsverarbeiter, die KI-Modelle oder KI-gestützte Dienste bereitstellen, nur ein, wenn deren Vertrag die Nutzung der übermittelten Daten zum Training ausschließt.

Nr.	Bereich	Maßnahme / Regelung
10 (3)	KI-spezifische Maßnahmen	Die KI-Plattform greift auf Daten nur mit den Rechten der jeweiligen Person zu. Konnektoren nutzen den Zugang der Person, kein Dienstkonto.
10 (4)	KI-spezifische Maßnahmen	Agenten handeln immer im Namen einer Person. Schreibende Aktionen sind standardmäßig ausgeschaltet und erfordern eine Freigabe.
10 (5)	KI-spezifische Maßnahmen	Die Websuche ist standardmäßig ausgeschaltet und wird nur nach Freischaltung durch den Kunden genutzt. Übertragen wird nur der Suchbegriff, ohne Identität der Person und ohne IP-Adresse. Die Websuche ist von den internen Daten des Kunden getrennt. Webinhalte werden als Daten behandelt, nicht als Befehle.
10 (6)	KI-spezifische Maßnahmen	Externe Modelle (ausgewählte Modelle von Anthropic über Google Vertex AI in der EU, auf Wunsch des Kunden auch von OpenAI oder Google) und ein größeres Modell beim Server stehen nur als eigene App zur Verfügung, die der Kunde einrichten lässt und für ausgewählte Gruppen freigibt.
11 a)	Verarbeitung nach Weisung	Festlegung von Ansprechpartnern
11 b)	Verarbeitung nach Weisung	Interne Datenschutzrichtlinien
11 c)	Verarbeitung nach Weisung	Schulung der Mitarbeitenden
11 d)	Verarbeitung nach Weisung	Einbindung des Datenschutzkontakts oder Datenschutzbeauftragten, soweit erforderlich
11 e)	Verarbeitung nach Weisung	Dokumentierte Prozesse für Weisungen, Supportfälle und Sicherheitsvorfälle
12 (1)	Unterauftragsverarbeiter	Unterauftragsverarbeiter werden nur eingesetzt, soweit sie im Angebot oder in der einbezogenen Unterauftragsverarbeiterliste genannt sind.
12 (2)	Unterauftragsverarbeiter	basebox verpflichtet Unterauftragsverarbeiter auf angemessene Datenschutz- und Sicherheitsmaßnahmen.
12 (3)	Unterauftragsverarbeiter	Technische und organisatorische Maßnahmen von Unterauftragsverarbeitern gelten ergänzend, soweit diese für die vereinbarte Leistung eingesetzt werden.
12 (4)	Unterauftragsverarbeiter	Anbieter, die der Kunde selbst auswählt, beauftragt, bereitstellt oder freigibt, sind keine Unterauftragsverarbeiter von basebox.

Nr.	Bereich	Maßnahme / Regelung
13 (1)	Überprüfung und Nachweise	basebox überprüft die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig und anlassbezogen.
13 (2)	Überprüfung und Nachweise	Dazu gehören insbesondere: a) regelmäßige Sicherheits- und Datenschutzüberprüfungen, b) Auswertung von Prüfberichten und Protokollen, c) Überprüfung von Backup- und Wiederherstellungsprozessen, d) Sensibilisierung und Schulung von Mitarbeitenden, e) Bewertung und Umsetzung geeigneter Verbesserungsmaßnahmen.
13 (3)	Überprüfung und Nachweise	Auf Anfrage stellt basebox dem Kunden angemessene weitere Nachweise zur Verfügung, soweit diese für die Prüfung der Auftragsverarbeitung erforderlich sind und keine berechtigten Sicherheits-, Geheimhaltungs- oder Vertraulichkeitsinteressen entgegenstehen.
13 (4)	Überprüfung und Nachweise	Solche Nachweise können insbesondere umfassen: a) ISO-27001-Zertifikat im jeweils gültigen Umfang, b) Unterauftragsverarbeiterliste, c) produktbezogene Sicherheitsinformationen, d) Informationen zu Backup-, Logging- und Löschprozessen, e) Informationen zu eingesetzten Hosting-, Infrastruktur- oder Betriebsdienstleistern, f) sonstige geeignete Sicherheits- oder Datenschutzdokumentation.
13 (5)	Überprüfung und Nachweise	Die Bereitstellung von Nachweisen kann davon abhängig gemacht werden, dass der Kunde und etwaige Prüfer angemessene Vertraulichkeitsverpflichtungen einhalten.
14 (1)	Änderungen der TOMs	basebox kann diese technischen und organisatorischen Maßnahmen weiterentwickeln oder anpassen.
14 (2)	Änderungen der TOMs	Änderungen dürfen das vereinbarte Sicherheitsniveau nicht wesentlich unterschreiten.
14 (3)	Änderungen der TOMs	Wesentliche Änderungen werden dem Kunden in geeigneter Form mitgeteilt, soweit sie die vereinbarte Verarbeitung wesentlich betreffen.

Verantwortungsmatrix nach Betriebsweg (Ziffer 2)

Bereich	Cloud	Übergangsumgebung (bis November 2026)	Server, Betrieb durch basebox	Server, Betrieb durch die IT des Kunden
Infrastruktur	basebox / Unterauftragsverarbeiter	basebox / Unterauftragsverarbeiter	Kunde (Server ist Eigentum des Kunden); im Rechenzentrum Stellplatz, Strom, Netz und physische Sicherheit durch den Rechenzentrumsbetreiber (Unterauftragsverarbeiter)	Kunde
Trennung von anderen Kunden	eigene Umgebung je Organisation (eigene Datenbank, eigener Speicher, eigene Benutzerverwaltung); die Rechenleistung des KI-Modells teilen sich die Organisationen	gemeinsame Umgebung, logische Trennung über Mandanten	Server des Kunden	Infrastruktur des Kunden
Identitätsverwaltung	eigene Benutzerverwaltung je Organisation	gemeinsame Instanz, Trennung über Mandanten	auf dem Server des Kunden	auf Infrastruktur des Kunden
Betrieb der Plattform	basebox	basebox	basebox	Kunde
Updates bereitstellen	basebox	basebox	basebox	basebox
Updates einspielen	basebox	basebox	basebox (Betriebssystem, Plattform, KI-Modelle)	Kunde

Bereich	Cloud	Übergangsumgebung (bis November 2026)	Server, Betrieb durch basebox	Server, Betrieb durch die IT des Kunden
Backup Infrastruktur	basebox: täglich, Aufbewahrung 7 Tage; 30 Tage und verschlüsselte Kopie in einem zweiten Rechenzentrum in Deutschland im Aufbau	basebox: tägliches Backup beim Hosting-Anbieter, Aufbewahrung bis zu 7 Tage, Speicherort am Standort des Servers	Kunde; basebox richtet die Sicherung ein	Kunde
Monitoring Infrastruktur	basebox, automatisch rund um die Uhr	basebox	Kunde	Kunde
Monitoring Softwareplattform	basebox, automatisch rund um die Uhr	basebox	basebox, automatisch rund um die Uhr, soweit die Infrastruktur des Kunden die Zugänge ermöglicht; Störungen bearbeitet basebox in den Support-Zeiten	Kunde
Personen, Gruppen und Rechte	Kunde, soweit nicht anders vereinbart	Kunde im eigenen Mandanten	Kunde	Kunde
Audit Logs	nach Produktfunktion und Kundenkonfiguration	nach Produktfunktion und Kundenkonfiguration, getrennt nach Mandant	nach Produktfunktion und Kundenkonfiguration	nach Produktfunktion und Kundenkonfiguration
Supportzugang	basebox	basebox	über vom Kunden bereitgestellte Zugänge	nur auf Auftrag des Kunden, zeitlich begrenzt, vom Kunden freigegeben, protokolliert und widerrufbar