basebox
KI-Plattform

Anlage: KI-Nutzung und Verantwortlichkeiten

Zum Software-Lizenzvertrag basebox KI-Plattform

Version: 1. November 2026

1. Geltung dieser Anlage

(1) Diese Anlage regelt die Verantwortlichkeiten der Parteien bei der Nutzung von KI-Funktionen in der basebox KI-Plattform.

(2) Diese Anlage gilt nur, wenn sie im Angebot ausdrücklich einbezogen wird.

(3) Diese Anlage ist kein eigenständiger Vertrag. Sie ergänzt den Software-Lizenzvertrag basebox KI-Plattform.

(4) Soweit im Angebot nichts Abweichendes vereinbart ist, gilt diese Anlage für alle Betriebswege.

2. Rolle von basebox

(1) basebox stellt mit der basebox KI-Plattform eine technische Softwareplattform bereit, die den Einsatz von KI-Modellen, Apps, Konnektoren, der Suche in Dokumenten und weiteren KI-gestützten Funktionen ermöglicht.

(2) basebox bestimmt nicht den konkreten Einsatzzweck, die Einsatzart, die Fachprozesse, die Dateninhalte oder die fachliche Verwendung der KI-Ausgaben durch den Kunden.

(3) basebox stellt technische Informationen, Dokumentation, Modellinformationen, Modellregister, Empfehlungen und Hinweise zur sicheren und sachgerechten Nutzung bereit.

(4) Empfehlungen von basebox dienen der technischen und fachlichen Orientierung. Die Entscheidung über den konkreten Einsatz und die Freigabe für den jeweiligen Anwendungsfall trifft der Kunde.

(5) Eine weitergehende Rolle von basebox, insbesondere als Anbieter eines kundenspezifisch trainierten oder feinabgestimmten KI-Modells, besteht nur, wenn dies im Angebot ausdrücklich vereinbart ist.

3. Rolle des Kunden

(1) Der Kunde ist für den konkreten Einsatz der basebox KI-Plattform verantwortlich.

(2) Der Kunde bestimmt insbesondere:
a) den Einsatzzweck,
b) die eingesetzten Daten und Datenquellen,
c) die Gruppen und Personen, die die Plattform nutzen,
d) die Fachprozesse,
e) die Konfiguration der Apps,
f) die Freigabe von Modellen für Apps und Gruppen sowie den Einsatz weiterer Modelle, soweit im Angebot nichts Abweichendes vereinbart ist,
g) die Prüfung und Verwendung der KI-Ausgaben,
h) die Information und Schulung der Personen, die die Plattform nutzen,
i) die Einhaltung seiner gesetzlichen, regulatorischen und internen Anforderungen.

(3) Der Kunde ist verantwortlich für die Bewertung, ob sein konkreter Einsatz besonderen gesetzlichen, regulatorischen oder internen Anforderungen unterliegt.

(4) Der Kunde ist insbesondere verantwortlich für die Bewertung, ob sein konkreter Einsatz als Hochrisiko-KI-System oder als Einsatz in einem besonders regulierten Bereich einzuordnen ist.

(5) Der Kunde ist verantwortlich für die Einhaltung der DSGVO und sonstiger Datenschutzvorgaben, soweit er Zwecke und Mittel der Verarbeitung bestimmt.

(6) Der Kunde ist verantwortlich für Transparenz gegenüber Nutzern, Betroffenen oder Endanwendern, soweit dies für den konkreten Einsatz erforderlich ist.

4. Menschliche Aufsicht und Prüfung von KI-Ausgaben

(1) KI-Ausgaben können unvollständig, unrichtig, missverständlich, verzerrt oder für den konkreten Zweck ungeeignet sein.

(2) Der Kunde stellt sicher, dass KI-Ausgaben vor fachlicher, rechtlicher, medizinischer, sozialrechtlicher, finanzbezogener, personalbezogener, behördlicher oder sonst entscheidungserheblicher Verwendung angemessen geprüft werden.

(3) Der Kunde darf KI-Ausgaben nicht ungeprüft als alleinige Grundlage für Entscheidungen verwenden, die rechtliche Wirkung entfalten oder Personen erheblich beeinträchtigen können.

(4) Der Kunde stellt angemessene menschliche Aufsicht sicher.

(5) Der Kunde legt intern fest, welche Personen KI-Ausgaben prüfen dürfen und welche fachlichen Qualifikationen dafür erforderlich sind.

(6) basebox schuldet keine fachliche, medizinische, rechtliche, sozialrechtliche, finanzbezogene oder behördliche Prüfung von KI-Ausgaben.

5. Unzulässige und gesondert zu vereinbarende Nutzungen

(1) Der Kunde darf die basebox KI-Plattform nicht für gesetzlich verbotene Zwecke verwenden.

(2) Insbesondere nicht zulässig sind Nutzungen für:
a) unzulässiges Social Scoring,
b) manipulative oder täuschende Systeme,
c) unzulässige Ausnutzung besonderer Schutzbedürftigkeit von Personen,
d) unzulässige biometrische Echtzeitüberwachung,
e) sonstige gesetzlich verbotene KI-Praktiken.

(3) Einsätze in Hochrisiko- oder besonders regulierten Bereichen sind nur zulässig, wenn der Kunde die dafür erforderlichen rechtlichen, organisatorischen und technischen Voraussetzungen erfüllt.

(4) Die Verarbeitung von Verschlusssachen, insbesondere VS-NfD oder höher eingestufter Informationen, ist nicht zulässig. Die basebox KI-Plattform hat keine Zulassung des BSI für Verschlusssachen.

(5) Die Nutzung des Systems für automatisierte Entscheidungen mit rechtlicher Wirkung oder vergleichbarer erheblicher Beeinträchtigung natürlicher Personen ist nur

zulässig, wenn dies im Angebot ausdrücklich vereinbart wurde und der Kunde die hierfür erforderlichen Voraussetzungen sicherstellt.

6. Modelle, Modellwahl und Empfehlungen

(1) basebox wählt das KI-Modell in basebox aus und stellt es bereit. Der Kunde entscheidet, ob er weitere Modelle einsetzt, etwa eine App mit externem Modell oder eigene Modelle, und für welche Apps und Gruppen er Modelle freigibt, soweit im Angebot nichts Abweichendes vereinbart ist.

(2) basebox kann dem Kunden technische Informationen, Links, Modellregister, Modellvorschläge und Empfehlungen zur Auswahl geeigneter Modelle bereitstellen.

(3) Empfehlungen von basebox dienen der technischen Orientierung. Sie ersetzen nicht die Prüfung, Auswahlentscheidung und Freigabe durch den Kunden für den konkreten Einsatz.

(4) Setzt der Kunde selbst beschaffte Hardware ein, ist er dafür verantwortlich, dass sie für die eingesetzten Modelle und den beabsichtigten Einsatz ausreichend dimensioniert ist. basebox prüft vorher kostenlos, ob die Hardware passt.

(5) Die Eignung eines Modells hängt insbesondere von Hardware, GPU-Speicher, Kontextlänge, Nebenläufigkeit, Datenvolumen, Workload, Latenzanforderungen, Fachdomäne und eingesetzter Produktkonfiguration ab.

(6) In der Cloud teilen sich die Organisationen die Rechenleistung des KI-Modells auf gemeinsam genutzten Servern. Eine andere Bereitstellungsform gilt nur, wenn sie im Angebot vereinbart ist.

(7) Gemeinsam genutzte Modelle können für besonders schutzbedürftige oder kritische Daten geeignet sein, wenn die Verarbeitung zustandslos erfolgt, keine Kundendaten dauerhaft im Modell gespeichert werden und keine Nutzung von Kundendaten zum Training des Modells erfolgt, soweit im Angebot nichts Abweichendes vereinbart ist.

(8) Dedizierte Modelle können zusätzliche Kosten, technische Anforderungen oder Betriebsaufwände verursachen. Diese ergeben sich aus dem Angebot oder einer gesonderten Vereinbarung.

(9) Modelle können je App, Fachbereich, Gruppe oder Anwendungsfall unterschiedlich konfiguriert oder ausgewählt werden, soweit die jeweilige Produktversion und der vereinbarte Betriebsweg dies unterstützen.
(10) Die in der basebox KI-Plattform eingesetzten oder empfohlenen Modelle können im Rahmen von Produktpflege, Sicherheitsanforderungen, Lizenzänderungen, technischer Weiterentwicklung, Verfügbarkeit oder Eignung geändert oder ersetzt werden. Wesentliche Änderungen im produktiven Einsatz werden mit dem Kunden abgestimmt.

(11) Nutzt der Kunde eigene Modelle, externe Modell-APIs, Cloud-Dienste oder sonstige Drittanbieter-Modelle, ist der Kunde für deren Auswahl, Zulässigkeit, Lizenzierung, Datenschutz, Sicherheit, Kosten, Konfiguration, Einsatz und rechtliche Bewertung verantwortlich.

(12) basebox übernimmt keine Verantwortung für Modelle, APIs oder Dienste, die vom Kunden ausgewählt, bereitgestellt, lizenziert oder freigegeben werden, soweit basebox diese nicht ausdrücklich als eigene Leistung im Angebot übernommen hat.

(13) Das Modellregister und die Modelldokumentation können Informationen über von basebox bereitgestellte, unterstützte oder empfohlene Modelle enthalten, insbesondere Modellname, Anbieter, Version, Lizenz, Bereitstellungsstatus, technische Variante, bekannte Einschränkungen und Hinweise zur Nutzung.

(14) Die von basebox bereitgestellten Modellinformationen, Links und Empfehlungen dienen der Dokumentation und Orientierung. Maßgeblich bleibt die konkret vereinbarte oder vom Kunden freigegebene Modellnutzung.

(15) Ist im Angebot ein Modell eines Drittanbieters als Leistung von basebox vereinbart, etwa eine App mit externem Modell, schuldet basebox dessen technische Bereitstellung im vereinbarten Umfang. Der Kunde entscheidet, welche Daten er diesem Modell zur Verarbeitung überlässt, und bewertet diese Entscheidung datenschutzrechtlich selbst, insbesondere im Hinblick auf Zugriffe aus Drittländern. Der Kunde legt fest, für welche Apps und Gruppen dieses Modell freigegeben ist. Als externe Modelle stellt basebox ausgewählte Modelle von Anthropic über Google Vertex AI in der Europäischen Union bereit; sie werden über Tokens nach Preisliste genutzt. Auf Wunsch des Kunden stellt basebox über eigene Zugänge auch Modelle von OpenAI oder Google bereit, ebenfalls über Tokens; die datenschutzrechtliche Bewertung nach Satz 2 trifft der Kunde auch für diese Modelle. Bindet der Kunde einen Anbieter mit eigenem Vertrag und eigenem Zugang an, gilt Absatz 11.

7. Änderungen, Finetuning und eigene Modelle des Kunden

(1) Der Kunde darf Modelle nur ändern, feinabstimmen, trainieren, erneut trainieren, veröffentlichen oder Dritten bereitstellen, wenn dies rechtlich zulässig und technisch vereinbart ist.

(2) Nimmt der Kunde solche Änderungen vor oder bindet eigene Modelle ein, ist der Kunde für die daraus folgenden rechtlichen, technischen und regulatorischen Pflichten verantwortlich.

(3) Dies kann insbesondere Pflichten zur Dokumentation, Risikobewertung, Konformitätsbewertung, Kennzeichnung, Überwachung oder Registrierung auslösen.

(4) basebox übernimmt keine Verantwortung für kundenseitig geänderte, trainierte, feinabgestimmte, veröffentlichte oder eingebundene Modelle, soweit dies nicht ausdrücklich vereinbart ist.

(5) basebox ist nicht verantwortlich für Ergebnisse, Schäden oder Rechtsverstöße, die durch kundenseitige Modelländerungen, eigene Modelle, Drittmodelle oder externe KI-Dienste entstehen.

(6) Die basebox-Dokumentation weist darauf hin, dass Kunden bei eigenem Training, Finetuning, Modifikation oder Veröffentlichung eines Modells eine eigene Provider-Rolle übernehmen können.

8. Daten, Eingaben und Dokumente

(1) Der Kunde ist verantwortlich für die Rechtmäßigkeit der Daten, Eingaben, Anweisungen, Dokumente, Wissensquellen und sonstigen Inhalte, die in die basebox KI-Plattform eingebracht werden.

(2) Der Kunde stellt sicher, dass nur solche Daten verarbeitet werden, deren Verarbeitung im konkreten Einsatz zulässig ist.

(3) Besonders schutzbedürftige Daten, insbesondere Gesundheitsdaten, Patientendaten, Sozialdaten, Bürgerdaten, Finanzdaten, Berufsgeheimnisse, Geschäftsgeheimnisse und sonstige vertrauliche Informationen, dürfen nur im Rahmen des vereinbarten Betriebswegs, der AVV, der TOMs und des Angebots verarbeitet werden.

(4) Verschlusssachen, insbesondere VS-NfD oder höher eingestufte Informationen, dürfen nicht verarbeitet werden.

(5) Der Kunde ist verantwortlich für die Qualität, Aktualität, Richtigkeit und Vollständigkeit der eingebrachten Daten und Wissensquellen.

9. Logging, Monitoring und Nachvollziehbarkeit

(1) Die basebox KI-Plattform stellt Funktionen zur technischen Protokollierung und Auditierbarkeit bereit.

(2) Umfang, Aufbewahrung, Zugriff, Export und Löschung von Protokollen und Audit-Logs richten sich nach dem Angebot, der Produktdokumentation, der Auftragsverarbeitungsvereinbarung, den TOMs und dem vereinbarten Betriebsweg.

(3) Soweit die basebox KI-Plattform ein Audit Log bereitstellt, kann dieses insbesondere technische Ereignisse, administrative Aktionen, sicherheitsrelevante Ereignisse, Handlungen der Personen und systembezogene Verarbeitungsvorgänge erfassen.

(4) 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.

(5) Der Kunde ist verantwortlich dafür, die Protokollierungs- und Audit-Log-Konfiguration entsprechend seinem Einsatzkontext, seinen datenschutzrechtlichen Vorgaben, internen Richtlinien und gesetzlichen Anforderungen festzulegen.

(6) Der Kunde ist insbesondere verantwortlich dafür zu prüfen, ob eine Erfassung von Fragen, Eingaben, Antworten oder sonstigen Inhaltsdaten im Audit Log zulässig ist und welche Informations-, Schutz-, Zugriffs-, Lösch- und Aufbewahrungspflichten hierfür gelten.

(7) basebox schuldet keine bestimmte Protokollierungs- oder Audit-Log-Konfiguration, sofern diese nicht im Angebot oder in einer einbezogenen Anlage ausdrücklich vereinbart ist.

(8) 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. Information und KI-Kompetenz

(1) Der Kunde stellt sicher, dass die Personen, die die basebox KI-Plattform nutzen, angemessen über Möglichkeiten, Grenzen und Risiken der KI-Nutzung informiert werden.

(2) Der Kunde sorgt für eine angemessene Unterweisung oder Schulung dieser Personen, soweit dies für den konkreten Einsatz erforderlich ist.

(3) Die Schulung sollte insbesondere umfassen:
a) Grenzen und Fehlerrisiken von KI-Ausgaben,
b) Umgang mit besonders schutzbedürftigen Daten,
c) zulässige und unzulässige Nutzungen,
d) Prüfungspflichten,
e) Umgang mit Anweisungen und Dokumenten,
f) Datenschutz und Vertraulichkeit,
g) Meldung von Fehlern, Risiken und Sicherheitsvorfällen.

(4) basebox bietet Schulungen als Teil der optionalen Inbetriebnahme in der IT des Kunden oder als Professional Services an, soweit dies im Angebot vereinbart ist.

11. Sicherheits- und Risikomeldungen

(1) Der Kunde meldet basebox sicherheitsrelevante Fehler, schwerwiegende Fehlfunktionen oder erkannte Risiken im Zusammenhang mit der basebox KI-Plattform unverzüglich.

(2) Meldungen sollen insbesondere enthalten:
a) Beschreibung des Vorfalls oder Risikos,
b) Zeitpunkt und betroffene Funktionen,
c) betroffene Datenarten,
d) mögliche Auswirkungen,
e) bereits ergriffene Maßnahmen,
f) verfügbare Logs oder Nachweise.

(3) Datenschutzvorfälle richten sich zusätzlich nach der Auftragsverarbeitungsvereinbarung.

(4) Sicherheitsvorfälle in Kundeninfrastruktur, Kundensystemen, Kundennetzwerken oder kundenseitigen Betriebsprozessen liegen im Verantwortungsbereich des Kunden, soweit nichts Abweichendes vereinbart ist.

(5) basebox informiert betroffene Kunden über bekannte relevante Sicherheitsrisiken, sicherheitsrelevante Fehler oder erforderliche Sicherheitsupdates im Rahmen der vereinbarten Support- und Updateprozesse.
(6) Die Safety Notice nennt die Meldung von Sicherheits- oder Funktionsproblemen sowie kritischen Ereignissen, etwa unautorisiertem Zugriff oder Datenlecks, als Betreiberpflicht.

12. Compliance-Paket und Dokumentation

(1) basebox stellt ein Compliance-Paket zum EU AI Act bereit. Dieses umfasst insbesondere die Compliance-Dokumentation, das Modellregister, den Disclaimer zur Rollenabgrenzung, die Infrastructure Policy und die Safety Notice.

(2) Das Compliance-Paket ist Bestandteil der technischen und rechtlichen Systemdokumentation und dient der Orientierung, Nachweisführung und Audit-Unterstützung.

(3) Das Compliance-Paket ersetzt nicht die Bewertung des konkreten Einsatzes durch den Kunden. Der Kunde ist verantwortlich dafür, die Dokumentation für seinen konkreten Einsatz zu prüfen und in eigene Governance-, Datenschutz-, Sicherheits- und Compliance-Prozesse zu übernehmen.

13. Keine Ergebnisgarantie

(1) basebox übernimmt keine Garantie für die inhaltliche Richtigkeit, Vollständigkeit, Aktualität oder fachliche Geeignetheit von KI-Ausgaben.

(2) KI-Ausgaben sind statistisch erzeugte Ergebnisse und können Fehler, Lücken, Verzerrungen oder unzutreffende Aussagen enthalten.

(3) Der Kunde ist verantwortlich für die Prüfung, Bewertung und Verwendung der KI-Ausgaben.

(4) basebox haftet nicht für Entscheidungen, Maßnahmen oder Arbeitsergebnisse, die auf ungeprüften oder fehlerhaften KI-Ausgaben beruhen, soweit gesetzlich zulässig und im Hauptvertrag geregelt.

(5) Die Safety Notice hält fest, dass Modellergebnisse statistische Wahrscheinlichkeiten und keine garantiert korrekten Fakten sind.

14. Vorrang des Angebots und der Anlagen zum Betriebsweg

(1) Der konkret vereinbarte Betriebsweg ergibt sich aus dem Angebot.

(2) Soweit diese Anlage auf technische Funktionen, Logging, Datenhaltung, Modellbetrieb, Fernzugriffe oder Verantwortlichkeiten Bezug nimmt, gelten ergänzend die Anlage zum jeweiligen Betriebsweg, die AVV, die TOM-Anlage und die Produktdokumentation.

(3) Bei Widersprüchen gelten die Rangfolgeregelungen des Hauptvertrags.