

Auftragsverarbeitungsvertrag

Anlage zu den AGB des KI-Denkraums

Fassung vom 6. Oktober 2026 · Kennung denkraum-avv-2026-10-06 · kidenkraum.com/de/avv/2026-10-06

zwischen dem **Kunden**, der ein Abo des KI-Denkraums oder einen Einzelvertrag über ein Team abschließt (Verantwortlicher), und der **lennartgehl.com GmbH**, Hans-Henny-Jahnn-Weg 53, 22085 Hamburg, Amtsgericht Hamburg HRB 173152, vertreten durch den Geschäftsführer Lennart Maximilian Gehl (**Anbieter**, Auftragsverarbeiter).

§ 1 Vertragsschluss und Anwendungsbereich

(1) Dieser Vertrag ist Anlage der AGB des KI-Denkraums (§ 17 Abs. 2 der AGB). Kunde und Anbieter vereinbaren ihn mit dem Abschluss eines Abos oder eines Einzelvertrags über ein Team (§ 1 Abs. 4 der AGB), etwa eines Piloten, ohne dass es einer gesonderten Erklärung bedarf. Maßgeblich ist die bei Vertragsschluss gültige Fassung; der Anbieter speichert, welche Fassung galt, beim Einzelvertrag nennt dieser sie.

(2) Der Vertrag gilt, soweit der Anbieter personenbezogene Daten der Nutzer im Auftrag des Kunden verarbeitet. Das ist der Fall, sobald der Kunde im KI-Denkraum ein Team anlegt oder der Anbieter es nach einem Einzelvertrag für ihn anlegt, und solange das Team besteht. Nutzer sind die natürlichen Personen, denen der Kunde über das Team eine Einzellizenz gibt, einschließlich der Personen mit der Rolle Inhaber oder Admin.

(3) Der Vertrag ist unter kidenkraum.com als Seite und als PDF abrufbar und lässt sich speichern und ausdrucken (elektronisches Format nach Art. 28 Abs. 9 DSGVO).

(4) Für die Verarbeitung im Auftrag geht dieser Vertrag den AGB vor. Im Übrigen gelten die Begriffe der AGB.

§ 2 Gegenstand, Art, Zweck und Dauer

(1) Gegenstand ist die Bereitstellung von Einzellizenzen für den KI-Denkraum an die vom Kunden berechtigten Nutzer im Rahmen des Abos oder Einzelvertrags eines Teams. Dazu gehören:

1. Einladungen an die geschäftlichen E-Mail-Adressen, die Inhaber oder Admins angeben, und bei einem Team nach Einzelvertrag an die Adressen, die der Kunde dem Anbieter nennt;
2. die Teamverwaltung: Mitgliedschaft, Rollen (Inhaber, Admin, Mitglied), Einzellizenzen, Einladungsstatus und das Protokoll dieser Vorgänge;
3. die Kontoführung der eingeladenen Nutzer, soweit sie dem Teamzugang dient: Registrierung, Anmeldung, Passwort, Herunterladen der eigenen Daten, Löschen des Kontos;
4. die zugehörigen Mails, insbesondere Einladung, Bestätigung der Adresse und Zurücksetzen des Passworts;
5. die persönliche Merkliste und Bewertungen von Folgen, soweit die Plattform sie im Konto eines Nutzers speichert, sowie die Suche.

(2) Art der Verarbeitung: Erheben, Speichern, Ordnen, Abgleichen, Anzeigen für den Nutzer selbst und für Inhaber und Admins, Versenden per E-Mail, Löschen.

(3) Die Daten dienen ausschließlich den Leistungen nach Absatz 1. Die Plattform übermittelt sie an kein KI-Modell; nutzt die Suche ein KI-Modell, gibt sie ihm über Amazon Web Services in der EU nur den

einggegebenen Suchbegriff weiter, ohne Bezug zum Konto und ohne Speicherung beim Betreiber des Modells (Anlage 2). Für Support und Betrieb, etwa bei der Klärung einer Anfrage oder eines Fehlers, kann der Anbieter ein KI-Modell über Amazon Web Services in der EU einsetzen (Anlage 2), und zwar nur in einer dafür getrennten Arbeitssitzung; AWS speichert die Daten dabei nicht und gibt sie nicht an den Hersteller des Modells weiter. Zum Training von KI-Modellen und für Werbung nutzt der Anbieter die Daten nicht.

(4) Die Verarbeitung dauert so lange wie das Abo oder der Einzelvertrag des Teams; § 10 gilt darüber hinaus.

§ 3 Betroffene Personen und Arten von Daten

(1) Betroffen sind Beschäftigte des Kunden und sonstige vom Kunden berechnigte Personen, insbesondere für ihn tätige freie Mitarbeitende, sowie Personen, die der Kunde einlädt, schon vor Annahme der Einladung.

(2) Verarbeitet werden:

1. Kontodaten: Name, geschäftliche E-Mail-Adresse, Name des Unternehmens, Passwort (nur als Hash); bei Anmeldung mit Google zusätzlich Google-Kennung und Link zum Profilbild;
2. Teamdaten: Zugehörigkeit zum Team, Rolle, Zeitpunkt des Beitritts;
3. Einladungsdaten: eingeladene Adresse, vorgesehene Rolle, einladende Person, Zeitpunkte von Einladung, Ablauf, Annahme oder Rücknahme;
4. Protokoll der Teamverwaltung: wer wann eine Einladung verschickt, erneut gesendet oder zurückgenommen, eine Rolle geändert oder ein Mitglied entfernt hat, mit Adresse oder Kennung der betroffenen Person;
5. Anmelde- und Protokolldaten: Zeitpunkte von Registrierung, Bestätigung und Anmeldungen, IP-Adresse, Browserkennung;
6. Mails: Empfängeradresse, Name, Inhalt, Zustellstatus;
7. Merkliste und Bewertungen, soweit im Konto gespeichert: Kennung, Ausgabe oder Sammlung und Fassung gespeicherter Folgen, Muster, Kernaussagen und Anwendungsfälle, Bewertung einer Folge, jeweils mit Zeitpunkt;
8. Suchbegriffe: nur für die Dauer der Suche; die Plattform speichert sie nicht zum Konto, als Teil der aufgerufenen Adresse stehen sie bis zu 30 Tage in den technischen Protokollen des Hostings.

(3) Besondere Kategorien personenbezogener Daten (Art. 9 und 10 DSGVO) sind nicht Gegenstand. Der Kunde trägt solche Daten auch nicht in Freitextfelder ein, etwa in den Namen des Teams.

(4) Nicht erfasst ist das Leseverhalten: Der Anbieter wertet nicht nutzerbezogen aus, welche Inhalte ein Nutzer aufruft, sucht oder herunterlädt, und zeigt Inhabern und Admins nichts davon. Aufrufe erscheinen nur in den technischen Protokollen des Hostings. Merkliste und Bewertungen (Absatz 2 Nr. 7) sind nur für den Nutzer selbst sichtbar, nie für Inhaber oder Admins. Zusammengefasste Auswertungen, mit denen der Anbieter Auswahl und Darstellung der Inhalte verbessert, nimmt er in eigener Verantwortung vor (§ 4 Abs. 1 Nr. 7).

§ 4 Abgrenzung zur eigenen Verantwortung des Anbieters

(1) Nicht Gegenstand dieses Vertrags sind Verarbeitungen, für die der Anbieter selbst verantwortlich ist:

1. Vertragsabwicklung und Abrechnung mit dem Kunden, einschließlich Kasse, Zahlung, Rechnungen und der Zahl der gebuchten Einzellizenzen;
2. das Konto der Person, die das Abo für den Kunden bestellt oder die der Kunde als Ansprechperson eines Einzelvertrags nennt, soweit es der Vertragsabwicklung dient;

3. Nachweise über die Bestätigung der Unternehmereigenschaft und die Annahme der AGB und dieses Vertrags;
4. die Sicherheit der Plattform insgesamt und die Abwehr von Missbrauch, etwa die Auswertung technischer Protokolle zur Erkennung von Angriffen und das Sperren missbräuchlicher Zugriffe;
5. die Erfüllung gesetzlicher Pflichten, etwa zur Aufbewahrung;
6. die Testphase und Konten außerhalb eines Teams, etwa ein Konto, das schon vor der Einladung bestand, und ein Konto nach Ende der Teamzugehörigkeit (§ 10 Abs. 3);
7. das Zusammenfassen von Merkliste und Bewertungen zu Summen ohne Bezug zu einzelnen Personen, nie je Team oder Kunde und nur über mindestens zehn Nutzer; die Summen enthalten keine personenbezogenen Daten.

(2) Diese Abgrenzung verkürzt die Verarbeitung im Auftrag nicht. Einladungen, Teamverwaltung und die Konten der Nutzer bleiben, soweit sie dem Teamzugang dienen, Verarbeitung im Auftrag, auch wenn der Anbieter daraus Angaben für einen Zweck nach Absatz 1 braucht. Er nutzt dann nur das dafür Erforderliche; Stripe erhält aus der Teamverwaltung etwa nur die Zahl der Einzellizenzen, keine Namen oder Adressen, aus einem Team nach Einzelvertrag gar nichts. Die Maßnahmen nach Anlage 1 bleiben Pflicht aus diesem Vertrag.

(3) Für die Verarbeitungen nach Absatz 1 gilt die Datenschutzerklärung des KI-Denkraums.

§ 5 Weisungen

(1) Der Anbieter verarbeitet die Daten nur auf dokumentierte Weisung des Kunden, auch bei einer Übermittlung in ein Drittland. Verpflichtet ihn das Recht der Europäischen Union oder Deutschlands zu einer anderen Verarbeitung, teilt er dem Kunden diese Pflicht vorher mit, sofern das Recht die Mitteilung nicht verbietet.

(2) Die Weisungen des Kunden sind die AGB, dieser Vertrag, die Eingaben der Nutzer in Merkliste, Bewertung und Suche und die Einstellungen, die Inhaber und Admins in der Teamverwaltung vornehmen: einladen, Einladungen erneut senden oder zurücknehmen, Rollen ändern, Mitglieder entfernen. Bei einem Team nach Einzelvertrag sind Weisungen auch der Einzelvertrag mit seinen Änderungen, die Adressen und Rollen, die der Kunde dem Anbieter für Einladungen nennt, und ein Wechsel des Inhabers, den er in Textform verlangt. Der Kunde weist den Anbieter außerdem an, jedem Nutzer auf der Kontoseite das Herunterladen seiner Daten und das Löschen seines Kontos zu ermöglichen.

(3) Weitere Weisungen erteilen die gesetzlichen Vertreter des Kunden oder der Inhaber des Teams in Textform an hallo@kidenkraum.com. Der Anbieter dokumentiert sie. Eine Weisung, die über den vereinbarten Leistungsumfang hinausgeht, behandelt er als Wunsch nach einer Vertragsänderung.

(4) Hält der Anbieter eine Weisung für rechtswidrig, weist er den Kunden unverzüglich darauf hin. Er darf die Ausführung aussetzen, bis der Kunde die Weisung bestätigt oder ändert.

§ 6 Vertraulichkeit und Sicherheit

(1) Der Anbieter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen, und gibt ihnen nur den Zugriff, den ihre Aufgabe erfordert. Die Pflicht besteht nach Vertragsende fort.

(2) Der Anbieter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die Anlage 1 beschreibt. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt, und teilt wesentliche

Änderungen in Textform mit.

(3) Ansprechpartner für Datenschutz ist die Geschäftsführung unter hallo@kidenkraum.com. Einen Datenschutzbeauftragten hat der Anbieter nicht benannt, weil keine Pflicht dazu besteht (Art. 37 DSGVO, § 38 BDSG).

§ 7 Unterauftragsverarbeiter

(1) Der Kunde erteilt die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen (Art. 28 Abs. 2 DSGVO). Die bei Vertragsschluss eingesetzten nennt Anlage 2; die aktuelle Liste ist unter /de/avv (Anlage 2) abrufbar.

(2) Bevor der Anbieter einen Unterauftragsverarbeiter hinzuzieht oder ersetzt, informiert er den Kunden mindestens 30 Tage vorher in Textform, per E-Mail an den Inhaber des Teams.

(3) Der Kunde kann der Änderung aus einem sachlichen datenschutzrechtlichen Grund innerhalb von 14 Tagen nach Zugang der Information in Textform widersprechen. Die Parteien suchen dann eine Lösung. Gelingt das nicht, kann der Kunde das Abo oder den Einzelvertrag des Teams außerordentlich zu dem Zeitpunkt kündigen, zu dem die Änderung wirksam wird; im Voraus gezahlte Entgelte erstattet der Anbieter nach § 10 Abs. 8 der AGB anteilig.

(4) Der Anbieter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf die Datenschutzpflichten dieses Vertrags, soweit sie für dessen Leistung gelten, in der Regel über dessen Vertrag zur Auftragsverarbeitung. Für die Erfüllung dieser Pflichten haftet der Anbieter gegenüber dem Kunden (Art. 28 Abs. 4 DSGVO).

§ 8 Übermittlung in Drittländer

(1) Verarbeitet ein Unterauftragsverarbeiter Daten außerhalb der EU und des EWR oder greift er von dort auf sie zu, geschieht das nur unter den Voraussetzungen der Art. 44 bis 49 DSGVO: auf Grundlage des Angemessenheitsbeschlusses zum EU-US Data Privacy Framework (Durchführungsbeschluss (EU) 2023/1795) bei zertifizierten Empfängern oder von Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914). Anlage 2 nennt die Grundlage je Dienst.

(2) Entfällt eine Grundlage, stellt der Anbieter die Übermittlung auf eine andere Garantie um oder beendet sie und informiert den Kunden.

§ 9 Unterstützung und Datenschutzverletzungen

(1) Der Anbieter unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei den Rechten betroffener Personen (Art. 12 bis 22 DSGVO). Inhaber und Admins können Mitglieder entfernen und Einladungen zurücknehmen; jeder Nutzer kann seine Daten herunterladen und sein Konto löschen. Bittet ein Nutzer den Anbieter um Export oder Löschung seines Kontos, erledigt der Anbieter das nach § 5 Abs. 2. Andere Anfragen zur Teamverwaltung leitet er unverzüglich an den Kunden weiter.

(2) Bei den Pflichten nach Art. 32 bis 36 DSGVO unterstützt der Anbieter den Kunden mit den Informationen, die ihm vorliegen.

(3) Eine Verletzung des Schutzes personenbezogener Daten, die im Auftrag verarbeitete Daten betrifft, meldet der Anbieter dem Kunden unverzüglich, nachdem sie ihm bekannt geworden ist, nach Möglichkeit innerhalb von 48 Stunden. Die Meldung geht per E-Mail an den Inhaber des Teams und enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO; fehlende Angaben reicht er nach. Er ergreift unverzüglich Maßnahmen, um die Verletzung zu beheben und ihre Folgen zu mildern. Aufsichtsbehörde und Betroffene benachrichtigt der Kunde; der Anbieter tut das nur auf Weisung oder aufgrund eigener gesetzlicher Pflicht.

(4) Für Unterstützung, die über die Funktionen der Plattform und einen geringen Aufwand hinausgeht, kann der Anbieter eine angemessene Vergütung verlangen, außer sie beruht auf einer eigenen Pflichtverletzung.

§ 10 Löschung und Rückgabe

(1) Während der Laufzeit löscht der Anbieter die Teamzugehörigkeit eines Mitglieds, sobald Inhaber oder Admins es entfernen, und eine Einladung 30 Tage nach ihrer Annahme, Rücknahme oder ihrem Ablauf; eine Einladung läuft nach sieben Tagen ab, in einem Team nach Einzelvertrag nach 30 Tagen, spätestens mit dem Ende der Laufzeit (§ 9 Abs. 4 und 9 der AGB). Einträge im Protokoll der Teamverwaltung löscht er zwölf Monate nach ihrer Entstehung. Einträge der Merkliste und Bewertungen löscht er, sobald der Nutzer sie entfernt oder sein Konto löscht.

(2) Nach Ende des Abos oder Einzelvertrags des Teams löscht der Anbieter innerhalb von 30 Tagen die Teamdaten, die Einladungen und das Protokoll der Teamverwaltung. Verlangt der Kunde vor dem Ende in Textform die Rückgabe, übergibt der Anbieter ihm vorher eine Liste der Mitglieder und Einladungen in einem gängigen maschinenlesbaren Format. Kopien in Datensicherungen werden im regulären Zyklus überschrieben. Daten, die der Anbieter gesetzlich aufbewahren muss, sperrt er bis zum Ablauf der Frist. Auf Verlangen bestätigt er die Löschung in Textform.

(3) Die Konten der Nutzer löscht der Anbieter mit dem Ende der Teamzugehörigkeit nicht. Endet sie, durch Entfernen aus dem Team oder mit dem Ende des Abos oder Einzelvertrags des Teams, bleibt das Konto mit Zugang zur Vorschau bestehen, bis der Nutzer es löscht (§ 10 Abs. 8 der AGB). Von da an verarbeitet der Anbieter die Kontodaten sowie Merkliste und Bewertungen in eigener Verantwortung wie bei jedem Konto außerhalb eines Teams; darüber informiert die Datenschutzerklärung.

§ 11 Nachweise und Überprüfungen

(1) Der Anbieter stellt dem Kunden auf Anfrage die Informationen zur Verfügung, die den Nachweis der Pflichten aus Art. 28 DSGVO ermöglichen, vorrangig durch Unterlagen: diesen Vertrag mit Anlagen, schriftliche Auskünfte, etwa Antworten auf Fragebögen, sowie Verträge, Zertifikate und Prüfberichte der Unterauftragsverarbeiter, soweit diese sie zur Weitergabe bereitstellen.

(2) Reichen die Unterlagen im Einzelfall nicht aus, kann der Kunde den Anbieter vor Ort prüfen, selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer, der kein Wettbewerber des Anbieters ist. Der Kunde meldet die Prüfung mindestens 30 Tage vorher in Textform an. Sie findet zu üblichen Geschäftszeiten und höchstens einmal im Kalenderjahr statt, außer bei konkretem Anlass wie einer Datenschutzverletzung, und darf den Betrieb nicht unverhältnismäßig stören. Die Kosten trägt der Kunde, soweit angemessen auch den Aufwand des Anbieters; das gilt nicht, wenn die Prüfung einen wesentlichen Verstoß des Anbieters ergibt.

(3) Der Anbieter betreibt keine eigenen Server. Die Rechenzentren beurteilt der Kunde anhand der Zertifikate und Prüfberichte der Unterauftragsverarbeiter.

(4) Die Befugnisse der Aufsichtsbehörden bleiben unberührt.

§ 12 Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere dafür, dass er Nutzer einladen und ihre Daten dem Anbieter überlassen darf. Er informiert die Nutzer über die Verarbeitung (Art. 13 und 14 DSGVO). Der Anbieter unterstützt ihn, indem jede Mail an Nutzer auf die Datenschutzerklärung des KI-Denkraums verweist.

- (2) Der Kunde lädt nur geschäftliche Adressen ein und entfernt Nutzer, die keinen Zugang mehr haben sollen, etwa nach ihrem Ausscheiden.
- (3) Stellt der Kunde Fehler oder Unregelmäßigkeiten bei der Verarbeitung fest, informiert er den Anbieter unverzüglich.
- (4) Ansprechpartner des Kunden ist der Inhaber des Teams, sofern der Kunde in Textform keine andere Person benennt.

§ 13 Haftung

- (1) Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO.
- (2) Im Verhältnis zwischen Kunde und Anbieter gelten die Haftungsregeln der AGB (§ 16) auch für Ansprüche aus diesem Vertrag. Art. 82 DSGVO bleibt unberührt.

§ 14 Laufzeit, Änderungen, Schlussbestimmungen

- (1) Dieser Vertrag gilt für die Laufzeit des Abos oder Einzelvertrags und endet mit ihr, ohne dass es einer Kündigung bedarf. § 6 Abs. 1 und § 10 wirken über das Ende hinaus.
- (2) Änderungen dieses Vertrags vereinbaren die Parteien in Textform oder nach dem Verfahren für Änderungen der AGB (§ 18). Für Unterauftragsverarbeiter gilt § 7.
- (3) Die deutsche Fassung ist maßgeblich, die englische Fassung ist eine Übersetzung.
- (4) Im Übrigen gelten die Schlussbestimmungen der AGB (§ 19), insbesondere zu anwendbarem Recht und Gerichtsstand.

Anlage 1: Technische und organisatorische Maßnahmen

Stand 6. Oktober 2026.

1. Rechenzentren

- Der Anbieter betreibt keine eigenen Server. Datenbank und Anmeldung laufen bei Supabase in Rechenzentren von Amazon Web Services in Frankfurt am Main (Region eu-central-1), die Serverfunktionen der Anwendung bei Vercel ebenfalls in Frankfurt am Main.
- Zertifizierungen: Supabase SOC 2 Type 2, Vercel SOC 2 Type 2, Amazon Web Services für die Region Frankfurt unter anderem ISO 27001 und BSI C5.

2. Zugang und Zugriff

- Jeder Nutzer hat ein persönliches Konto. Einladungen gehen nur an geschäftliche Adressen; Adressen allgemeiner E-Mail-Anbieter lehnt der Server ab.
- Die Adresse wird per Link bestätigt, über die Einladung oder über eine Bestätigungsmail, deren Link eine Stunde gilt.
- Passwörter speichert Supabase Auth nur als Hash (bcrypt).
- Einladungslinks enthalten einen zufälligen Schlüssel mit 256 Bit, gelten sieben Tage, in Teams nach Einzelvertrag 30 Tage, längstens bis zum Ende der Laufzeit, und lassen sich nur mit dem Konto der eingeladenen Adresse annehmen. In Teams nach Einzelvertrag tritt das Konto der eingeladenen Adresse mit der Anmeldung bei.
- In der Teamverwaltung sehen und ändern nur Inhaber und Admins Mitglieder, Einladungen und Einzellizenzen ihres Teams; der Server prüft Rolle und Teamzugehörigkeit bei jeder dieser Aktionen. Die

Geschäftsführung des Anbieters sieht Konten und Teams in ihrer Verwaltung, legt dort Teams nach Einzelvertrag an, lädt für sie ein, ändert ihre Laufzeit und ihre Einzellizenzen und setzt ihren Inhaber; andere Teams ändert sie nur auf Weisung (§ 5).

- Zeilenrechte in der Datenbank (Row Level Security) begrenzen jeden Zugriff aus dem Browser: Ein Nutzer liest nur sein eigenes Profil und die Mitgliedschaften seines Teams; Einladungen und Protokoll lesen nur Inhaber und Admins dieses Teams. Team, Mitgliedschaften und Einladungen ändert nur der Server.
- Der Dienstschlüssel mit Vollzugriff auf die Datenbank liegt nur auf dem Server. Datenbankfunktionen mit erhöhten Rechten, etwa die Suche eines Kontos nach E-Mail-Adresse, kann nur der Server aufrufen.
- Schutz vor automatisierten Angriffen: Cloudflare Turnstile bei der Registrierung und bei „Passwort vergessen“, höchstens fünf Registrierungen je IP-Adresse und Minute, Ratenbegrenzungen von Supabase Auth für Anmeldung und Registrierung.
- Scheidet eine Person mit Zugang aus, werden ihre Zugänge entzogen und die Schlüssel erneuert, die sie kannte.
- Administrative Zugänge zu Supabase, Vercel, Postmark, Cloudflare, Stripe und GitHub hat nur die Geschäftsführung, jeweils mit Zwei-Faktor-Anmeldung.

3. Trennung

- Die Teams sind über die Zeilenrechte und die serverseitige Prüfung der Teamzugehörigkeit voneinander getrennt.
- Test- und Produktivbetrieb nutzen getrennte Datenbanken und Schlüssel.

4. Übertragung und Integrität

- Alle Verbindungen zur Plattform und zu den Diensten laufen verschlüsselt über TLS; HSTS legt Browser dauerhaft auf HTTPS fest.
- Supabase und Vercel verschlüsseln gespeicherte Daten mit AES-256.
- Das Protokoll der Teamverwaltung hält jede Änderung mit Zeitpunkt und handelnder Person fest.
- Änderungen am Code laufen über Pull Requests mit automatischen Pflichtprüfungen (Unit-Tests, End-to-End-Tests, Codequalität) und einer automatischen Durchsicht. Bekannte Sicherheitslücken in Abhängigkeiten meldet GitHub automatisch.

5. Verfügbarkeit

- Ratenbegrenzung und Bot-Schutz verringern das Risiko einer Überlastung.
- Supabase sichert die Datenbank täglich und bewahrt die Sicherungen sieben Tage auf.

6. Datensparsamkeit und Löschung

- Keine Analyse-, Werbe- oder Trackingdienste, keine nutzerbezogene Auswertung des Leseverhaltens. Merkliste und Bewertungen sieht nur der Nutzer selbst; zusammengefasst werden sie nur zu Summen ohne Bezug zu einzelnen Personen (§ 4 Abs. 1 Nr. 7).
- Keine Öffnungs- und Klickverfolgung in Mails.
- KI-Unterstützung im Support nur in einer getrennten Arbeitssitzung über Amazon Bedrock in der EU (ohne Speicherung bei AWS); deren Verlauf wird beim Beenden gelöscht. In allen anderen Arbeitssitzungen verhindert eine technische Sperre Abfragen personenbezogener Daten.
- Nutzt die Suche ein KI-Modell, gibt sie ihm über Amazon Bedrock in der EU nur den Suchbegriff weiter, ohne Kennung des Kontos; AWS speichert ihn nicht. Die Anwendung schreibt Suchbegriffe in keine

eigenen Protokolle.

- E-Mail-Adressen stehen in Anwendungsprotokollen nur gekürzt.
- Ratenbegrenzungen zählen im Arbeitsspeicher und werden nicht gespeichert.
- Datenexport und Kontolöschung durch den Nutzer selbst (§ 9 Abs. 1).
- Feste Löschfristen: Einladungen 30 Tage nach ihrem Ende, Protokoll der Teamverwaltung nach zwölf Monaten, Teamdaten 30 Tage nach Ende des Abos oder Einzelvertrags (§ 10).
- Protokolle bei den Diensten laufen automatisch aus: bei Vercel nach höchstens 30 Tagen, die Anmeldeprotokolle bei Supabase nach sieben Tagen, Nachrichten und Zustelldaten bei Postmark nach 45 Tagen.

7. Organisation und Überprüfung

- Unterauftragsverarbeiter nur mit Vertrag nach Art. 28 DSGVO (Anlage 2).
- Meldeweg für Sicherheitsvorfälle: hallo@kidenkraum.com, Bewertung durch die Geschäftsführung, Meldung an den Kunden nach § 9 Abs. 3.
- Zugang zu den Daten hat nur die Geschäftsführung. Kommen weitere Personen hinzu, verpflichtet der Anbieter sie vor dem ersten Zugang schriftlich auf Vertraulichkeit und weist sie in den Datenschutz ein.
- Die Endgeräte der Geschäftsführung sind verschlüsselt.
- Der Anbieter überprüft diese Maßnahmen mindestens einmal im Jahr und passt sie an.

Anlage 2: Unterauftragsverarbeiter

Stand 6. Oktober 2026; DPF-Status am 29. September 2026 in der Liste unter dataprivacyframework.gov geprüft.

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Garantie bei Drittlandbezug
Supabase Pte. Ltd. , 65 Chulia Street #38-02/03, OCBC Centre, Singapur 049513	Datenbank, Anmeldung (Supabase Auth)	Rechenzentren von Amazon Web Services in Frankfurt am Main (eu-central-1); Zugriffe für Betrieb und Support aus Singapur und den USA möglich	Standardvertragsklauseln im Vertrag zur Auftragsverarbeitung von Supabase. Für Singapur gibt es keinen Angemessenheitsbeschluss, Supabase ist nicht nach dem Data Privacy Framework zertifiziert.
Vercel Inc. , 440 N Barranca Ave #4133, Covina, CA 91723, USA	Hosting, Auslieferung, Serverfunktionen, technische Protokolle	Serverfunktionen in Frankfurt am Main, Auslieferung über ein weltweites Netz	EU-US Data Privacy Framework (zertifiziert, aktiv), zusätzlich Standardvertragsklauseln
AC PM, LLC (Postmark, Unternehmen von ActiveCampaign), 1 N Dearborn Street, Suite 500, Chicago, IL 60602, USA	Versand der Mails	USA (Rechenzentren von Deft und Amazon Web Services)	EU-US Data Privacy Framework (als verbundenes Unternehmen von ActiveCampaign, LLC zertifiziert, aktiv), zusätzlich Standardvertragsklauseln

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Garantie bei Drittlandbezug
Cloudflare, Inc. , 101 Townsend Street, San Francisco, CA 94107, USA	Turnstile: Prüfung bei der Registrierung mit E-Mail-Adresse, auch eingeladener Nutzer, und bei „Passwort vergessen“, ob ein Mensch das Formular ausfüllt (IP-Adresse, technische Merkmale des Browsers)	weltweites Netz von Cloudflare	EU-US Data Privacy Framework (zertifiziert, aktiv), zusätzlich Standardvertragsklauseln
Microsoft Ireland Operations Limited , One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	E-Mail-Postfach hallo@kidenkraum.com für Anfragen, Weisungen und Meldungen zur Teamverwaltung	Rechenzentren in der EU; Zugriffe aus den USA nicht ausgeschlossen	EU-US Data Privacy Framework (Microsoft Corporation zertifiziert), zusätzlich Standardvertragsklauseln
Amazon Web Services EMEA SARL , 38 Avenue John F. Kennedy, L-1855 Luxemburg	KI-Modell (Claude über Amazon Bedrock) für Support und Betrieb im Einzelfall, in einer getrennten Arbeitssitzung; sobald die Suche ein KI-Modell nutzt, die Umwandlung des Suchbegriffs (Modell von Cohere über Amazon Bedrock), ohne Kennung des Kontos	Rechenzentren in der EU; keine Speicherung von Ein- und Ausgaben; die Hersteller der Modelle haben keinen Zugriff	Verarbeitung in der EU; AWS-Auftragsverarbeitungsvertrag mit Standardvertragsklauseln, Amazon im EU-US Data Privacy Framework

Hinweise:

1. Die Dienste setzen eigene Unterauftragsverarbeiter ein, etwa Amazon Web Services, und veröffentlichen deren Listen.
2. Cloudflare nutzt die Signale von Turnstile nach eigener Angabe zusätzlich in eigener Verantwortung, um die Bot-Erkennung zu verbessern.
3. Stripe und Google sind keine Unterauftragsverarbeiter nach diesem Vertrag, weil der Anbieter die Abrechnung in eigener Verantwortung führt und Stripe aus der Teamverwaltung nur die Zahl der Einzellizenzen erhält, aus einem Team nach Einzelvertrag gar nichts, und weil Nutzer die Anmeldung mit Google freiwillig wählen und Google dafür selbst verantwortlich ist.
4. Cover-Bilder liefert der Anbieter über seinen eigenen Server aus; Spotify erhält dabei keine Daten der Nutzer.