

Heyblocks — Datenschutzerklärung (deutsche Fassung, verbindlich) (valid until 2026-09-22)

1. Verantwortlicher

Verantwortlicher im Sinne der Datenschutz-Grundverordnung (DSGVO):

Justin Hofmann, handelnd unter der Bezeichnung „Heyblocks“

Einzelunternehmen

Helene-Junghans-Str. 43/1, 78713 Schramberg

E-Mail: info@heyblockslabs.com

Inhaltlich verantwortlich gemäß § 18 Abs. 2 MStV: Justin Hofmann,

Helene-Junghans-Str. 43/1, 78713 Schramberg

2. Datenschutz auf einen Blick

Allgemeine Hinweise

Die folgenden Hinweise geben einen einfachen Überblick darüber, was mit deinen personenbezogenen Daten passiert, wenn du unsere Anwendung nutzt. Personenbezogene Daten sind alle Daten, mit denen du persönlich identifiziert werden kannst.

Datenerfassung

Ein Teil der Daten wird erhoben, um die fehlerfreie Bereitstellung der Anwendung zu gewährleisten. Andere Daten werden erhoben, wenn du sie uns im Rahmen der Registrierung, Nutzung oder Kontaktaufnahme mitteilst. Hochgeladene Inhalte (Audiodateien, Videodateien, Texte, URLs) werden zur Verarbeitung an externe KI-Dienstleister übermittelt (siehe Abschnitt 5). Bei Nutzung der Recherche-Funktion werden Websuchen über einen externen Suchdienst durchgeführt (siehe Abschnitt 5.4).

Deine Rechte

Du hast jederzeit das Recht, unentgeltlich Auskunft über Herkunft, Empfänger und Zweck deiner gespeicherten personenbezogenen Daten zu erhalten. Außerdem hast du ein Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung dieser Daten. Zudem steht dir ein Beschwerderecht bei der zuständigen Aufsichtsbehörde zu.

3. Allgemeines zur Datenverarbeitung

Wir verarbeiten personenbezogene Daten unserer Nutzer grundsätzlich nur, soweit dies zur Bereitstellung einer funktionsfähigen Webanwendung sowie unserer Inhalte und Leistungen erforderlich ist.

Heyblocks ist derzeit ausschließlich als Webanwendung (Browser) verfügbar. Eine Mobil-App oder Desktop-Anwendung wird derzeit nicht angeboten.

4. Hosting & Infrastruktur

4.1 Hosting über Railway

Unsere Anwendung wird über den Dienst Railway Corp. betrieben. Die Anwendung läuft in Docker-Containern auf Servern in den Niederlanden (EU).

Dabei können folgende Daten verarbeitet werden:

- IP-Adresse
- Browser- und Geräteinformationen
- Request-Header
- Logdateien

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der sicheren und effizienten Bereitstellung unserer Anwendung).

4.2 Railway Redis (Rate Limiting & kurzzeitiges Caching)

Zum Schutz vor missbräuchlicher Nutzung (z. B. Brute-Force-Angriffe, übermäßige API-Aufrufe) setzen wir einen über Railway Corp. bereitgestellten Redis-Dienst ein.

Dabei werden folgende Daten vorübergehend gespeichert:

IP-Adresse oder Nutzer-ID (als Teil des temporären Rate-Limit-Eintrags); für die öffentliche Kündigungsseite zusätzlich die eingegebene E-Mail-Adresse und eine zufällige Link-Kennung (zur Begrenzung des Mailversands pro Adresse und damit jeder Bestätigungslink nur einmal verwendet werden kann)

- Zeitstempel der Anfragen

Diese Daten dienen ausschließlich der Durchsetzung von Anfragelimits und werden nach Ablauf des jeweiligen Zeitfensters automatisch gelöscht (in der Regel wenige Minuten bis maximal 24 Stunden).

Zusätzlich dient eine separate Redis-Instanz (ebenfalls über Railway betrieben, EU) als kurzzeitiger Cache zur Beschleunigung des Ladens: häufig abgerufene Inhalte (z. B. deine Notizliste, Notizinhalte, Tabs, Quellen, Blueprints und Lern-Decks) werden dort vorübergehend unter einem an deine Nutzer-ID gebundenen Schlüssel vorgehalten.

Cache-Einträge werden automatisch gelöscht oder ersetzt, wenn sich die zugrunde liegenden Daten ändern, und laufen von selbst nach kurzer Zeit ab; alleiniger maßgeblicher Speicherort bleibt die in Abschnitt 4.3 beschriebene Datenbank.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Sicherheit und Integrität der Anwendung sowie an einem schnellen Dienst).

4.3 Cloudflare (Datenbank & DNS)

Wir nutzen Cloudflare Inc. als Infrastruktur- und Datenbankdienstleister. Nutzerdaten werden in einer Cloudflare-D1-Datenbank gespeichert.

Dabei können folgende Daten verarbeitet werden:

- Kontodaten (E-Mail, Benutzername, verschlüsseltes Passwort, Google-ID)

- Erstellte Notizen, Transkripte und generierte Tab-Inhalte
- Nutzungsstatistiken (Token-Verbrauch, Generierungsdauer, Kosten)
- Abonnementstufe, Nutzungskontingente und Transaktionshistorie

Cloudflare ist als Auftragsverarbeiter eingebunden. Soweit Daten in Drittländer (z. B. die USA) übermittelt werden, geschieht dies auf Grundlage der Standardvertragsklauseln.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO und Art. 6 Abs. 1 lit. f DSGVO.

4.4 Cloudflare Turnstile (Bot-Schutz)

Zum Schutz vor automatisierten Angriffen und Missbrauch (z. B. bei Zahlungsvorgängen) setzen wir Cloudflare Turnstile ein. Turnstile ist ein CAPTCHA-Dienst von Cloudflare Inc., der ohne sichtbare Interaktion oder mittels eines einfachen Klicks prüft, ob eine Anfrage von einem echten Nutzer stammt.

Dabei können folgende Daten verarbeitet werden:

- IP-Adresse
- Browser- und Geräteinformationen
- Interaktionsdaten (Mausbewegungen, Klickverhalten)

Die Daten werden von Cloudflare verarbeitet, um zwischen menschlichen Nutzern und Bots zu unterscheiden. Personenbezogene Kontodaten werden nicht an Turnstile übermittelt.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Sicherheit der Anwendung und der Betrugsprävention).

4.5 Tigris Object Storage (Mediendateien & Quelldateien)

Hochgeladene und verarbeitete Dateien werden bei Tigris Data Inc. gespeichert (S3-kompatibler Objektspeicher). Dateien werden unter einem nutzer- und notizspezifischen Pfad abgelegt.

- Audio- und Videodateien
- Als Quelle hochgeladene Dokumente und Bilddateien (z. B. PDF, Bilder)

Umfangreiche Transkript- und Quelltexte, die das Speicherlimit der Datenbank überschreiten, werden als Textdatei ausgelagert (maßgebliche Speicherung des jeweiligen Texts)

Der Zugriff auf gespeicherte Audiodateien erfolgt über zeitlich begrenzte, signierte URLs (Gültigkeit: 4 Stunden).

Uploads und Abrufe dieser Dateien erfolgen direkt zwischen deinem Browser und Tigris über solche zeitlich begrenzten, signierten URLs. Im Rahmen dieser Direktverbindung verarbeitet Tigris technisch deine IP-Adresse und technische Verbindungsdaten (wie jeder Server, den dein Browser kontaktiert); Kontodaten werden nicht an Tigris übermittelt.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung).

5. KI-gestützte Verarbeitung

Inhalte, die andere Personen betreffen: Aufnahmen von Vorlesungen, Meetings

und Gesprächen enthalten regelmäßig die Stimmen, Namen und Äußerungen anderer Personen als dir. Für diese Inhalte entscheidest du über Zwecke und Mittel der Verarbeitung und bist damit Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO; bitte stelle sicher, dass du zur Aufnahme und zum Hochladen berechtigt bist. Unsere eigenen Pflichten bleiben davon unberührt: Diese Personen sind auch uns gegenüber betroffene Personen, und die in diesem Abschnitt beschriebene Verarbeitung — einschließlich der Übermittlung an die nachfolgend genannten Dienstleister — gilt für ihre Daten in gleicher Weise wie für deine, und wir minimieren sie in gleicher Weise: keine Kontodaten, keine E-Mail-Adressen und keine Zahlungsdaten werden an die KI-Dienste übermittelt.

5.1 Groq Inc. (Transkription & Inhaltserzeugung)

Heyblocks nutzt zur Verarbeitung deiner Inhalte KI-Dienste der Groq Inc. (Mountain View, USA).

Spracherkennung: Hochgeladene Audio- und Videodateien werden an die Speech-to-Text-API von Groq übermittelt, um eine automatische Transkription durchzuführen. Die Datei wird dabei vollständig an Groq übermittelt.

Inhaltserzeugung: Der erzeugte Transkripttext wird über Groq an ein KI-Sprachmodell übermittelt, um daraus strukturierte Inhalte zu generieren (z. B. Zusammenfassungen, Notizen, eigene Tabs).

Nach den Nutzungsbedingungen von Groq werden über die API übermittelte Daten nicht zum Training von Modellen verwendet.

Da Groq seinen Sitz in den USA hat, findet eine Übermittlung in ein Drittland statt. Die Übermittlung erfolgt auf Grundlage der Standardvertragsklauseln der Europäischen Kommission (Modul 2) sowie eines begleitenden Transfer Impact Assessment (TIA). Eine Zertifizierung nach dem EU-U.S. Data Privacy Framework besteht derzeit nicht.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung — die KI-Verarbeitung ist Kernbestandteil des Dienstes).

5.2 OpenAI Inc. (Inhaltserzeugung)

Heyblocks nutzt für die Inhaltserzeugung in beiden Modi (Fast und Pro) KI-Dienste der OpenAI Inc. (San Francisco, USA).

Inhaltserzeugung: Der Transkripttext wird an ein KI-Sprachmodell von OpenAI übermittelt, um daraus strukturierte Inhalte zu generieren (z. B. Zusammenfassungen, Notizen, eigene Tabs, Karteikarten, Quizfragen).

Textextraktion aus Dokumenten und Bildern (OCR): Wenn du ein Dokument (z. B. PDF) oder ein Bild als Quelle hinzufügst, wird die Datei — bei PDFs ein Abbild jeder Seite — an ein KI-Modell von OpenAI übermittelt, um den lesbaren Text zu extrahieren. Nur der extrahierte Text wird als Quelltext gespeichert (Abschnitte 4.5 und 7.1).

An Groq/OpenAI übermittelte Daten | Nicht übermittelt

Audio-/Videodateien (zur Transkription, nur Groq) | E-Mail-Adressen oder Kontodaten
Transkripttext und Quelltexte (zur Inhaltserzeugung) | Zahlungsinformationen
Tab-Bezeichnungen (zur Inhaltserzeugung) | IP-Adressen der Nutzer
Als Quelle hochgeladene Dokumente und Bilder (zur Textextraktion, nur OpenAI) | –
Dateinamen und, soweit vorhanden, das Aufnahmedatum deiner Quellen (als Kontext für die Inhaltserzeugung) | –

Von dir eingegebene Recherchethemen (zur Ableitung von Suchanfragen, siehe Abschnitt 5.4) | –
Nach den Nutzungsbedingungen von OpenAI werden über die API übermittelte Daten nicht zum Training der Modelle verwendet, es sei denn, der Kunde stimmt dem ausdrücklich zu. Wir haben dem nicht zugestimmt.

Unser Vertragspartner ist OpenAI Ireland Limited, sodass unsere eigene Übermittlung innerhalb des Europäischen Wirtschaftsraums stattfindet. Der Kontakt mit den USA entsteht als Weiterübermittlung: Nach Ziffer 4.1 des Data Processing Addendum von OpenAI gibt OpenAI Ireland Limited Daten nur auf Grundlage der Standardvertragsklauseln der Europäischen Kommission an OpenAI Inc. und andere Empfänger außerhalb des EWR weiter. Da die Daten tatsächlich in den USA verarbeitet werden, haben wir die dortige Rechtslage in einem Transfer Impact Assessment (TIA) so geprüft, als würden wir direkt übermitteln. OpenAI ist nicht nach dem EU-U.S. Data Privacy Framework zertifiziert; Garantie sind daher allein die Standardvertragsklauseln.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung — die KI-Verarbeitung ist Kernbestandteil des Dienstes).

5.3 Automatisierte Inhaltsprüfung (Content Safety)

Vor der Verarbeitung durch KI-Modelle wird der Transkripttext automatisiert auf mögliche Verstöße gegen unsere Inhaltsrichtlinien geprüft. Dazu wird der Transkripttext an ein Sicherheitsmodell der Groq Inc. übermittelt. Bei außergewöhnlich langen Transkripten wird der Teil, der die technische Verarbeitungsgrenze des Sicherheitsmodells überschreitet, zusätzlich an den Moderationsdienst der OpenAI Inc. (San Francisco, USA) übermittelt. Diese Prüfung dient dem Schutz vor missbräuchlichen Inhalten (z. B. Gewaltverherrlichung, Hassrede, illegale Inhalte) sowie vor Versuchen, die KI-Systeme zu manipulieren (Prompt Injection). An die Sicherheits- und Moderationsdienste werden keine personenbezogenen Kontodaten übermittelt — nur der zu prüfende Inhalt (Transkripttext oder Bild).

Bildmoderation: Als Quelle hochgeladene Bilddateien werden vor der weiteren Verarbeitung an den Moderationsdienst der OpenAI Inc. (San Francisco, USA) übermittelt, um sie automatisiert auf Verstöße gegen unsere Inhaltsrichtlinien zu prüfen. Übermittelt wird ausschließlich die jeweilige Bilddatei, keine Kontodaten. Die Übermittlung an OpenAI folgt der in Abschnitt 5.2 beschriebenen Struktur: Unser Vertragspartner ist OpenAI Ireland Limited, die Verarbeitung in den USA erfolgt als Weiterübermittlung auf Grundlage der Standardvertragsklauseln.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der

Sicherheit und Integrität der Anwendung sowie am Schutz vor rechtswidrigen Inhalten).

5.4 Serper Inc. (Websuche — Recherche-Funktion)

Wenn du die Recherche-Funktion nutzt, werden Suchanfragen an den Dienst Serper Inc. übermittelt, um Websuchen durchzuführen und relevante Quellen zu finden.

Dabei werden folgende Daten übermittelt:

Suchbegriffe: das vom Nutzer eingegebene Recherchethema sowie daraus automatisch abgeleitete Suchanfragen (im gründlichen Recherchemodus erzeugt ein KI-Modell aus deinem Thema mehrere verwandte Anfragen und verfeinert sie während der Recherche, siehe Abschnitt 5.2)

Es werden keine personenbezogenen Kontodaten, E-Mail-Adressen oder IP-Adressen der Nutzer an Serper übermittelt. Die Suchergebnisse (URLs und Titel) werden anschließend serverseitig abgerufen und verarbeitet.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung — die Recherche-Funktion ist Bestandteil des Dienstes).

6. Nutzerkonten & Registrierung

Für die Nutzung der Anwendung ist die Erstellung eines Nutzerkontos erforderlich.

6.1 Registrierung mit E-Mail und Passwort

Bei der Registrierung mit E-Mail und Passwort verarbeiten wir:

- E-Mail-Adresse
- Benutzername

Passwort (ausschließlich als kryptografischer Hash mit Argon2 gespeichert; für ältere Bestandskonten wird bcrypt verwendet und beim nächsten Anmelden automatisch auf Argon2 migriert. Das Klartextpasswort wird nicht gespeichert.)

6.2 Registrierung / Anmeldung über Google (OAuth)

Alternativ kannst du dich über dein Google-Konto anmelden. Dabei erhalten wir von Google:

- E-Mail-Adresse
- Name
- Google-Nutzer-ID
- Profilbild-URL

Die Authentifizierung erfolgt über den Dienst „Google Identity Services“ der Google Ireland Limited. Wir erhalten kein Google-Passwort und keinen Zugriff auf weitere Google-Kontodaten.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung).

6.3 Sitzungsverwaltung

Nach erfolgreicher Anmeldung wird ein JSON Web Token (JWT) erstellt und als HttpOnly-Cookie im Browser gespeichert. Dieses Cookie:

enthält ausschließlich die Nutzer-ID, einen technischen Sitzungszähler (mit dem alle Sitzungen eines Kontos auf einmal ungültig gemacht werden können, z. B. nach einer Passwortänderung) und eine Ablaufzeit

- kann nicht per JavaScript ausgelesen werden (HttpOnly)
- wird nur über verschlüsselte Verbindungen übertragen (Secure-Flag)
- hat eine Gültigkeit von 7 Tagen

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO i. V. m. § 25 Abs. 2 TDDDG
(technisch notwendiges Cookie).

6.4 Anmelde- und Sicherheitsereignisse

Zum Schutz deines Kontos und zur Erkennung und Abwehr von Missbrauch (z. B. Credential-Angriffe) zeichnen wir sicherheitsrelevante Kontoereignisse auf: erfolgreiche und fehlgeschlagene Anmeldungen, Abmeldungen, Passwortänderungen und Anfragen zum Zurücksetzen des Passworts. Je Ereignis speichern wir die Ereignisart, den Zeitpunkt, die IP-Adresse, den verwendeten Browser (User Agent) und die betroffene E-Mail-Adresse. Deine letzten Anmeldungen werden dir außerdem in den Kontoeinstellungen angezeigt (Anmeldeverlauf), damit du unberechtigte Zugriffe erkennen kannst.

Diese Aufzeichnungen werden spätestens nach 90 Tagen automatisch gelöscht und zusätzlich entfernt, wenn das Konto endgültig gelöscht wird (nach dem 30-tägigen Wiederherstellungsfenster, Abschnitt 12). Anders als bei den Anwendungslogs in Abschnitt 11.2 wird die IP-Adresse hier im Klartext gespeichert, weil erst der Vergleich exakter Adressen das Erkennen von Kontoübernahmen und gezielten Angriffen möglich macht.
Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an Kontosicherheit und Missbrauchsprävention).

6a. Minderjährige & Einwilligung der Erziehungsberechtigten

6a.1 Altersgrenzen

Wer das 16. Lebensjahr vollendet hat, kann Heyblocks selbständig nutzen. Wer zwischen 13 und 15 Jahre alt ist, kann Heyblocks nur nutzen, wenn ein Träger der elterlichen Verantwortung zuvor bestätigt hat. Personen unter 13 Jahren dürfen Heyblocks nicht nutzen.

6a.2 Altersangabe

Bei der Registrierung fragen wir das Geburtsdatum ab. Wir speichern das Geburtsdatum nicht. Gespeichert werden ausschließlich zwei daraus abgeleitete Werte: die Alterskategorie („volljährig im datenschutzrechtlichen Sinne“ bzw. „minderjährig“) und das Datum, an dem das 16. Lebensjahr vollendet wird. Mehr benötigen wir nicht, um unsere Pflichten aus Art. 8 DSGVO zu erfüllen, und weniger zu speichern reduziert das Risiko im Fall einer Datenpanne.

6a.3 Daten der Erziehungsberechtigten

Für Konten von 13- bis 15-Jährigen verarbeiten wir zusätzlich: die E-Mail-Adresse des Trägers der elterlichen Verantwortung, den Zeitpunkt der Anfrage und der Bestätigung, die IP-Adresse und den Browser (User Agent) zum Zeitpunkt der Bestätigung sowie die zu diesem Zeitpunkt geltende Fassung der AGB und dieser Datenschutzerklärung. Diese Angaben sind der Nachweis, dass die Einwilligung tatsächlich erteilt wurde.

Um zu erschweren, dass ein Minderjähriger die Bestätigung selbst erteilt, vergleichen wir die angegebene Adresse mit der Adresse des Kontos, schließen Wegwerf-Adressen aus und begrenzen die Zahl der Bestätigungen je Adresse. Wir können damit nicht mit Sicherheit feststellen, dass die bestätigende Person tatsächlich erziehungsberechtigt ist — wir unternehmen aber die nach Art. 8 Abs. 2 DSGVO angemessenen Anstrengungen.

6a.4 Rechtsgrundlagen

Rechtsgrundlage: Art. 6 Abs. 1 lit. a i. V. m. Art. 8 Abs. 1 DSGVO

(Einwilligung, erteilt bzw. autorisiert durch den Träger der elterlichen Verantwortung) für die Verarbeitung der Daten des Minderjährigen; Art. 6 Abs. 1 lit. c DSGVO für die Speicherung des Einwilligungsnachweises (Nachweispflicht nach Art. 7 Abs. 1, Verifizierungspflicht nach Art. 8 Abs. 2 DSGVO); Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Verhinderung von Umgehungsversuchen) für die Prüf- und Begrenzungsmaßnahmen nach Abschnitt 6a.3.

6a.5 Speicherdauer

Die E-Mail-Adresse des Erziehungsberechtigten wird gelöscht, sobald sie nicht mehr benötigt wird — spätestens mit Vollendung des 16. Lebensjahres des Nutzers. Der übrige Einwilligungsnachweis wird in gekürzter Form (ohne Klartext-Adresse) für die Dauer des Kontos und anschließend drei Jahre aufbewahrt (Verjährungsfrist, § 195 BGB) und danach gelöscht. Wird die Bestätigung nicht innerhalb von 14 Tagen erteilt, löschen wir das angelegte Konto und alle hierzu gespeicherten Daten vollständig.

6a.6 Widerruf

Der Träger der elterlichen Verantwortung kann die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen, ohne sich anzumelden — über den Link in jeder Benachrichtigungs-E-Mail. Der Widerruf ist damit so einfach wie die Erteilung (Art. 7 Abs. 3 DSGVO). Nach dem Widerruf wird das Konto gesperrt und nach 30 Tagen, in denen die Inhalte exportiert werden können, gelöscht.

6a.7 Keine Werbung, kein Profiling

Für Konten von 13- bis 15-Jährigen versenden wir keine Werbe-E-Mails und übermitteln keine Konversionsereignisse an Werbenetzwerke. Es findet keine auf Profiling gestützte Werbung statt. Die Erziehungsberechtigten werden über wesentliche Ereignisse (Erteilung der Einwilligung, Versuch eines kostenpflichtigen Abschlusses, Löschung des Kontos) per E-Mail

informiert.

7. Verarbeitete Nutzungsdaten

7.1 Quelldateien

Vom Nutzer hochgeladene Audio- und Videodateien werden:

- vorübergehend auf dem Server gespeichert (zur Verarbeitung)
- zur Transkription an Groq übermittelt (siehe Abschnitt 5)
- im Tigris Object Storage gespeichert (siehe Abschnitt 4.5)
- nach Abschluss der Verarbeitung vom Server gelöscht

automatisch aus dem Objektspeicher gelöscht, sobald die zugehörige Notiz entfernt wird, spätestens jedoch nach rund 30 Tagen. Als nicht richtlinienkonform markierte Uploads werden innerhalb dieses Zeitraums für die Moderationsprüfung aufbewahrt; unabhängig von der Datei wird ein Nachweis der Prüfung — einschließlich eines kurzen Auszugs, soweit einer gespeichert wird (siehe Abschnitt 15a) — so lange aufbewahrt, wie in den Abschnitten 12 und 15a beschrieben. Das Transkript bleibt davon unberührt und in der Datenbank gespeichert. Einzige Ausnahme für die Datei selbst ist als Beweismittel gesichertes Material in einem Kinderschutzfall: Es wird separat und länger gespeichert, wie in den Abschnitten 12 und 15a beschrieben.

Vom Nutzer hinzugefügte URLs und Texte werden serverseitig extrahiert und als Quelltext in der Datenbank gespeichert. Als Quelle hochgeladene Dokumente und Bilddateien werden ebenfalls verarbeitet, und der extrahierte Text wird als Quelltext gespeichert (siehe Abschnitt 4.5). Über die Recherche-Funktion gesammelte Webquellen werden ebenfalls als Quelltext gespeichert.

7.2 Generierte Inhalte

Folgende KI-generierte Inhalte werden in unserer Datenbank gespeichert:

- Transkripte
- Automatisch generierter Titel
- Zusammenfassung
- Eigene Tab-Inhalte (z. B. Stichpunkte, Vokabeln usw.)
- Karteikarten (Frage/Antwort-Paare) für Spaced Repetition
- Quizfragen einschließlich Antwortoptionen

7.3 Nutzungsstatistiken

Zur internen Kostenkalkulation, Abrechnung, Durchsetzung der Nutzungslimits deines Tarifs und zur Überwachung der technischen Leistung des Dienstes (z. B. durchschnittliche und maximale Generierungszeiten) speichern wir je Generierung:

- Anzahl verbrauchter Tokens (Eingabe und Ausgabe)
- Dauer der Audiodatei
- Generierungsdauer

- Berechnete API-Kosten (intern, nicht personenbezogen ausgewertet)
- Verbrauchte Nutzungszeit (Minuten)

Rechtsgrundlage hierfür: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung — Messung und Abrechnung des von dir gebuchten Tarifs) sowie, soweit diese Aufzeichnungen aggregiert für die interne Kostenanalyse und die technische Leistungsüberwachung ausgewertet werden, Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an einem wirtschaftlich tragfähigen, stabilen und schnellen Dienst). Da die Messaufzeichnungen für die Erbringung des Dienstes selbst erforderlich sind, können sie nicht abgeschaltet werden. Die kurzlebigen Messereignisse zur Durchsetzung des Minutenkontingents deines Tarifs werden automatisch nach 30 Tagen gelöscht; die Statistiken je Generierung werden mit der Löschung deines Kontos gelöscht (Abschnitt 12). Der aggregierten Auswertung kannst du jederzeit nach Art. 21 DSGVO über die Kontaktdaten in Abschnitt 1 widersprechen.

Zusätzlich erfassen wir, um zu verstehen, welche Funktionen tatsächlich genutzt werden, und um sie zu verbessern, wenn du ein generiertes Set exportierst (z. B. Karteikarten zu Anki). Wir speichern nur das Exportformat, die betroffene Notiz und den Zeitpunkt — niemals den exportierten Inhalt selbst. Diese Auswertung ist intern, wird nicht an Dritte weitergegeben, und es findet kein Profiling statt. Diese Einträge werden spätestens nach 30 Tagen automatisch gelöscht. Du kannst dieser Erfassung jederzeit in deinen Kontoeinstellungen widersprechen (Option „Datenerfassung“); danach werden keine weiteren mit deiner Nutzer-ID verknüpften Einträge gespeichert.

Rechtsgrundlage für die Exportaufzeichnungen: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der bedarfsgerechten Weiterentwicklung und Verbesserung unserer eigenen Funktionen).

7.4 Blueprints

Nutzer können „Blueprints“ (Vorlagen) erstellen, die Tab-Bezeichnungen enthalten. Diese werden serverseitig in der Datenbank gespeichert.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung).

7.5 Lerndaten (Karteikarten & Quiz)

Wenn du die Lernfunktionen nutzt, speichern wir zur Bereitstellung der Wiederholungs- und Fortschrittslogik:

Karteikarten-Wiederholungen: deine Selbsteinschätzung je Karte sowie die daraus berechneten Planungsdaten für die nächste Wiederholung (Spaced-Repetition-Algorithmus) und die zugehörigen Zeitstempel

- Quizversuche: erreichte Punktzahl, Anzahl der Fragen und Zeitpunkt des Versuchs

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung — Bereitstellung der Lernfunktionen).

7.6 Blueprint-Store (Veröffentlichen von Vorlagen)

Nutzer können ihre selbst erstellten Blueprints freiwillig im „Store“ veröffentlichen, um sie anderen Nutzern zur Verfügung zu stellen. Die Veröffentlichung erfolgt ausschließlich auf deine aktive Initiative.

Mit der Veröffentlichung werden folgende Daten für alle Nutzer sichtbar:

- Name des Blueprints und dessen Tab-Bezeichnungen
- Dein Benutzername (als Autor des Blueprints)
- Anzahl der Installationen

Du kannst einen veröffentlichten Blueprint jederzeit wieder aus dem Store entfernen, indem du den zugrunde liegenden Blueprint löschst.

Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO (Einwilligung durch aktive Veröffentlichung).

7.7 Teilen von Notizen

Nutzer können einzelne Notizen freiwillig mit anderen teilen. Das Teilen erfolgt ausschließlich auf deine aktive Initiative und kann jederzeit widerrufen werden. Zwei Modi stehen zur Verfügung:

Öffentlicher Link: Jeder, der den Link kennt, kann die geteilte Notiz ansehen (Titel, Tab-Inhalte und dein Benutzername als Autor). Der Link enthält ein zufällig erzeugtes, nicht erratbares Token; die Notiz ist darüber hinaus nicht gelistet oder auffindbar.

Bestimmte Personen: Die Notiz ist nur für die von dir angegebenen

E-Mail-Adressen zugänglich. Diese Empfänger müssen sich mit der eingeladenen E-Mail-Adresse anmelden, um die Notiz anzusehen.

Wenn du eine Notiz teilst, werden folgende Daten verarbeitet:

die E-Mail-Adressen der von dir eingeladenen Personen (im Modus „bestimmte Personen“), gespeichert zur Zugriffssteuerung — dies können auch Adressen von Personen sein, die selbst keine Nutzer sind;

- die geteilten Inhalte (Titel, Tabs), die für die jeweiligen Empfänger sichtbar werden;
- dein Benutzername, der Empfängern als Autor der geteilten Notiz angezeigt wird.

Im Modus „bestimmte Personen“ senden wir an jede neu hinzugefügte Adresse eine einmalige Einladungs-E-Mail (siehe Abschnitt 8a). Empfänger können eine geteilte Notiz in ihre eigene Bibliothek übernehmen; dabei entsteht eine unabhängige Kopie in ihrem Konto. Du kannst das Teilen jederzeit beenden, indem du die Freigabe entfernst — der Link funktioniert dann sofort nicht mehr — und auch das Löschen der Notiz entfernt die Freigabe.

Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO (Einwilligung durch aktives Teilen); für die Einladungs-E-Mails zusätzlich Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse, das vom Nutzer gewünschte Teilen zu ermöglichen).

7.8 Karteikarten-Erinnerungs-E-Mails (Opt-in)

Optional kannst du E-Mail-Erinnerungen aktivieren, die dich benachrichtigen, wenn gespeicherte Karteikarten zur Wiederholung fällig sind. Diese Funktion ist standardmäßig deaktiviert und wird nur nach deiner aktiven Einwilligung (Opt-in) genutzt — über den Schalter in den Einstellungen oder die entsprechende Abfrage während einer Lerneinheit.

Bei Aktivierung verarbeiten wir folgende Daten:

deine Benachrichtigungseinstellung (aktiviert/deaktiviert) und den Zeitpunkt der zuletzt versandten Erinnerung (um höchstens eine Erinnerung pro Tag sicherzustellen); ein grobes regionales Versandfenster („Asien-Pazifik“, „Europa/Naher Osten/Afrika“ oder „Amerika“), einmalig abgeleitet aus dem UTC-Versatz deines Browsers im Moment der Aktivierung, damit Erinnerungen zu einer sinnvollen Ortszeit ankommen. Gespeichert wird nur dieser dreistufige Regionswert — niemals deine genaue Zeitzone oder dein Standort — und er wird ausschließlich für den Versandzeitpunkt verwendet.

Jede Erinnerungs-E-Mail enthält die Anzahl fälliger Karteikarten, die Titel der betroffenen Notizen und deinen Benutzernamen; der Versand erfolgt über unseren E-Mail-Dienstleister (siehe Abschnitt 8a). Jede Erinnerung enthält einen Abmeldelink, der ohne Anmeldung funktioniert; du kannst die Erinnerungen außerdem jederzeit in den Einstellungen deaktivieren. Bei Deaktivierung — auf beiden Wegen — wird das gespeicherte Versandfenster sofort gelöscht; die Einstellung und der Zeitstempel werden spätestens mit dem Nutzerkonto gelöscht.

Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO (Einwilligung). Du kannst deine Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen (Art. 7 Abs. 3 DSGVO) — über die Einstellungen oder den Abmeldelink.

8. Zahlungsabwicklung

Für entgeltliche Leistungen (z. B. Abschluss und Verwaltung von Abonnements) nutzen wir den Zahlungsdienstleister Stripe Inc. Stripe verarbeitet personenbezogene Daten in eigener Verantwortung nach den jeweils geltenden Datenschutzbestimmungen von Stripe. Vollständige Zahlungsinformationen (z. B. Kreditkartennummern) erhalten wir von Stripe nicht.

Wenn du einen Bezahlvorgang startest, übermitteln wir an Stripe deine E-Mail-Adresse (damit die Zahlung deinem Konto zugeordnet und Belege versandt werden können) und deine interne Nutzer-ID (als Referenznummer). Keine Notizinhalt und keine sonstigen Kontodaten werden übermittelt.

Nach erfolgreicher Zahlung erhalten wir von Stripe ausschließlich:

- eine Bestätigung der Transaktion
- die gewählte Abonnementstufe und den Abrechnungszeitraum

Beim Abschluss eines Abonnements erklärst du im Bezahlvorgang ausdrücklich deine Zustimmung, dass mit der Ausführung des Vertrags vor Ablauf der Widerrufsfrist

begonnen wird (§ 356 Abs. 5 Nr. 2 BGB). Als Nachweis dieser Erklärung speichern wir den Zeitpunkt der Zustimmung und die dabei geltende Fassung der AGB (Speicherdauer siehe Abschnitt 12). Anschließend bestätigen wir dir den Vertragsschluss per E-Mail (§ 312f BGB, siehe Abschnitt 8a).

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung);
für die Aufbewahrung des Zustimmungsnachweises zudem Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Nachweisbarkeit der gesetzlich vorgesehenen Zustimmung).

8a. E-Mail-Versand

Für den Versand transaktionaler E-Mails nutzen wir den Dienst Resend Inc. Dies sind insbesondere: die Willkommens-E-Mail nach der Registrierung, E-Mail-Verifizierungscodes, E-Mails zum Zurücksetzen des Passworts, ein Hinweis, wenn jemand versucht, sich mit einer bereits registrierten Adresse zu registrieren, Antworten auf Kontaktanfragen, die Vertragsbestätigung beim Abschluss eines Abonnements (§ 312f BGB, einschließlich der Wiedergabe deiner Zustimmungserklärung aus dem Bezahlvorgang, siehe Abschnitt 8), Bestätigungen einer Abonnement-Kündigung (einschließlich der Bestätigungslink-E-Mail und der Eingangsbestätigung bei Kündigungen über die öffentliche Kündigungsseite, § 312k BGB), einmalige Einladungs-E-Mails, wenn du eine Notiz mit bestimmten E-Mail-Adressen teilst, eine automatische Bestätigung über den Eingang deiner Support-Anfrage, Hinweise zu Änderungen dieser Datenschutzerklärung oder der Nutzungsbedingungen sowie — nur mit deiner Einwilligung — Erinnerungs-E-Mails zu fälligen Karteikarten (siehe Abschnitt 7.8).

Dabei werden folgende Daten an Resend übermittelt:

- E-Mail-Adresse des Empfängers

Inhalt der E-Mail (z. B. Willkommenstext, Support-Antwort; bei Support-Anfragen umfasst dies deine Nachricht und, sofern du sie angehängt hast, die in Abschnitt 11.2 beschriebene technische Konsolenausgabe)

Resend verarbeitet diese Daten ausschließlich zum Zweck der E-Mail-Zustellung. Da Resend seinen Sitz in den USA hat, erfolgt die Übermittlung auf Grundlage der Standardvertragsklauseln der Europäischen Kommission.

Bei einer Kündigung über die öffentliche Kündigungsseite (§ 312k BGB) senden wir zusätzlich einen internen Hinweis über die Kündigungserklärung (die eingegebene E-Mail-Adresse, die Kündigungsart und einen etwaig angegebenen Grund) an unser Support-Postfach, damit eine Erklärung, deren Bestätigungslink nie verwendet wird, manuell nachverfolgt werden kann. Die Speicherdauer ist in Abschnitt 12 angegeben.

Support-Anfragen, die uns per Kontaktformular oder E-Mail erreichen, und unsere Antworten darauf werden in einem Support-Postfach in unserer Datenbank (Cloudflare D1, siehe

Abschnitt 4) gespeichert. Zu jedem Vorgang halten wir einen Bearbeitungsstatus (offen, wartet auf Antwort, erledigt) und gegebenenfalls einen internen Bearbeitungsvermerk fest. Der Vermerk ist nur für uns sichtbar und wird dir nicht zugesandt. Erledigte Vorgänge werden nach Ablauf der in Abschnitt 12 genannten Frist gelöscht, nicht erledigte spätestens zwölf Monate nach der letzten Nachricht; mit der Löschung deines Kontos wird die Korrespondenz zu deiner E-Mail-Adresse sofort entfernt.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) und Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Kommunikation mit Nutzern); für die Karteikarten-Erinnerungs-E-Mails Art. 6 Abs. 1 lit. a DSGVO (Einwilligung, siehe Abschnitt 7.8).

9. Cookies & Einwilligung

Unsere Anwendung verwendet folgende Cookies:

Cookie | Zweck | Art | Gültigkeit

heyblocks_session | Authentifizierung (JWT-Token) | Technisch notwendig | 7 Tage

heyblocks_consent | Speicherung der Cookie-Einwilligungseinstellungen | Technisch notwendig | 365 Tage

heyblocks_locale | Speichert deine gewählte Anzeigesprache, damit Seiten sofort in ihr dargestellt werden | Funktional (von dir gewünschte Einstellung) | 365 Tage

heyblocks_ai_mode | Speichert deinen gewählten KI-Modus (Fast/Pro), damit er sofort angewendet wird | Funktional (von dir gewünschte Einstellung) | 365 Tage

Diese Cookies sind technisch notwendig oder speichern eine von dir ausdrücklich gewählte Einstellung; sie werden nicht für Tracking genutzt und bedürfen keiner gesonderten Einwilligung nach § 25 Abs. 2 TDDDG.

Zusätzlich können folgende Cookies gesetzt werden, sofern du ausdrücklich einwilligst:

Cookie | Zweck | Art | Anbieter

_gcl_*, _gac_* | Google-Ads-Conversion-Tracking | Marketing (einwilligungspflichtig) | Google LLC

Beim ersten Besuch unserer Anwendung wirst du über einen Cookie-Banner um deine

Einwilligung gebeten. Dort kannst du zwischen folgenden Optionen wählen:

- Alle akzeptieren — Essenzielle und Marketing-Cookies werden aktiviert.
- Nur essenzielle — Nur technisch notwendige Cookies werden gesetzt. Kein Tracking.
- Einstellungen verwalten — Du kannst einzelne Cookie-Kategorien gezielt aktivieren oder deaktivieren.

Marketing-Cookies (Google-Ads-Conversion-Tracking) werden ausschließlich nach deiner ausdrücklichen Einwilligung geladen. Ohne Einwilligung findet kein Tracking statt.

Rechtsgrundlage: Essenzielle Cookies: Art. 6 Abs. 1 lit. f DSGVO

i. V. m. § 25 Abs. 2 TDDDG. Marketing-Cookies: Art. 6 Abs. 1 lit. a DSGVO

i. V. m. § 25 Abs. 1 TDDDG (Einwilligung).

10. Personalisierung

Personalisierungsfunktionen werden lokal im Browser gespeichert (localStorage) — z. B. die Theme-Einstellung — oder, wo der Server den Wert benötigt, um Seiten beim ersten Laden korrekt darzustellen, zusätzlich in einem funktionalen Cookie (Anzeigesprache und KI-Modus, siehe Abschnitt 9). Die gewählte Anzeigesprache speichern wir außerdem in deinem Konto, damit E-Mails an dich (z. B. Bestätigungen und Erinnerungen, Abschnitt 8a) in deiner Sprache versandt werden können; sie wird bei der Anmeldung und beim Ändern von Einstellungen aktualisiert und mit dem Konto gelöscht (Rechtsgrundlage Art. 6 Abs. 1 lit. b DSGVO). Eine serverseitige Auswertung oder ein Profiling findet nicht statt.

11. Analyse & Tracking

11.1 Google-Ads-Conversion-Tracking

Wir nutzen den Dienst Google Ads Conversion Tracking der Google LLC (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; nachfolgend „Google“).

Wichtig: Google-Ads-Tracking wird ausschließlich nach deiner ausdrücklichen Einwilligung über unseren Cookie-Banner aktiviert. Ohne deine Einwilligung werden keine Tracking-Skripte geladen und keine Cookies von Google gesetzt. Hast du eingewilligt, wird ein Cookie auf deinem Gerät gesetzt, wenn du über eine Google-Anzeige zu unserer Anwendung gelangst. Mit Hilfe dieses Cookies können wir und Google feststellen, ob ein Nutzer nach dem Klick auf eine Anzeige eine bestimmte Handlung ausgeführt hat (Registrierung, Generierung einer Notiz).

Dabei können folgende Daten verarbeitet werden:

- Cookie-Kennung (anonymisiert)
- Informationen über die besuchte Seite
- Datum und Uhrzeit des Besuchs

Conversion-Ereignisse, nämlich abgeschlossene Registrierung und die erfolgreiche Generierung einer Notiz. Übermittelt wird nur, dass das Ereignis stattgefunden hat — niemals der Inhalt deiner Notizen, Aufnahmen oder Dateien.

Die durch das Cookie erzeugten Informationen werden in der Regel an einen Server von Google in den USA übertragen und dort gespeichert. Google ist nach dem EU-U.S. Data Privacy Framework zertifiziert; die Übermittlung stützt sich zusätzlich auf die Standardvertragsklauseln der Europäischen Kommission.

Du kannst deine Einwilligung jederzeit widerrufen, indem du deine Cookie-Einstellungen in der Anwendung änderst oder deine Cookies löschst. Zusätzlich kannst du die Erfassung über den Google-Ads-Einstellungsmanager oder unter www.aboutads.info deaktivieren.

Rechtsgrundlage: Art. 6 Abs. 1 lit. a DSGVO (Einwilligung)

i. V. m. § 25 Abs. 1 TDDDG.

11.2 Log- und Diagnosedaten

Zur Gewährleistung der Sicherheit, zur Fehleranalyse und zur Abwehr von Missbrauch speichern wir serverseitige Anwendungslogs in unserer Datenbank (siehe Abschnitt 4.3).

Diese Logs dienen ausschließlich dem Betrieb und der Sicherheit der Anwendung; ein Profiling oder eine werbliche Auswertung findet nicht statt.

Dabei können folgende Daten verarbeitet werden:

- IP-Adresse ausschließlich in pseudonymisierter Form (gesalzener Hash, niemals im Klartext; zu den separaten Anmelde- und Sicherheitsereignissen siehe Abschnitt 6.4)
- Browser-/Geräteerkennung (User Agent)
- Nutzer-ID (sofern angemeldet)
- Aufgerufener Pfad, HTTP-Methode und Antwortstatus
- Fehlerinformationen (Fehlerart, technische Fehlermeldung)
- Verarbeitungsdauer und Größe der Anfrage

Um Fehler zu erkennen, die nur im Browser auftreten, übermittelt die Anwendung zusätzlich Fehlerberichte aus deinem Browser an unseren Server (Fehlermeldung, technischer Fehlerverlauf und die betroffene Funktion); sie werden als Teil derselben Anwendungslogs gespeichert und unterliegen derselben 90-tägigen Löschung. Wenn du ein Problem mit einer bestimmten Notiz oder Quelle meldest, wird deine Beschreibung zusammen mit den bereits auf unserem Server erfassten technischen Fehlerdetails (niemals aus deinem Browser entnommen) gespeichert, bis das Konto oder alle Daten gelöscht werden (Abschnitt 12). Wenn du den Support kontaktierst, kannst du zusätzlich wählen, die jüngste technische Konsolenausgabe deiner Browser-Sitzung anzuhängen; sie wird dann als Teil deiner Support-Anfrage per E-Mail übermittelt (Abschnitt 8a) und mit der Support-Korrespondenz aufbewahrt (sechs Monate, Abschnitt 12).

Widerspruchsrecht: Du kannst der nutzerbezogenen Protokollierung in deinen Kontoeinstellungen widersprechen (Option „Datenerfassung“). Ist diese deaktiviert, werden keine weiteren Logs gespeichert, die mit deiner Nutzer-ID verknüpft sind. Aus zwingenden Sicherheitsgründen (z. B. Abwehr von Angriffen) können weiterhin technisch notwendige, nicht kontobezogene Logs erzeugt werden. Logdaten werden automatisch nach 90 Tagen gelöscht.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Sicherheit, Stabilität und Fehlerfreiheit der Anwendung).

12. Speicherdauer & Löschung

Personenbezogene Daten werden nur so lange gespeichert, wie es für die jeweiligen Zwecke erforderlich ist:

Datenart | Speicherdauer

Nutzerkonto | Bis zur Löschung durch den Nutzer; endgültige Löschung 30 Tage nach der Kontolöschung

Audio-/Videodateien | Bis zur Löschung der zugehörigen Notiz, spätestens nach ca. 30 Tagen

Quelldateien (Dokumente, Bilder) | Bis zur Löschung der zugehörigen Notiz durch den Nutzer

Notizen, Transkripte, Tabs | Bis zur Löschung durch den Nutzer

Lernkarten (Karteikarten, Quiz, Wiederholungs- und Versuchshistorie) | Bis zur Löschung der zugehörigen Notiz oder des Nutzerkontos

Karteikarten-Erinnerungseinstellungen (Benachrichtigungseinstellung, regionales Versandfenster, Zeitpunkt der letzten Erinnerung) | Versandfenster: sofortige Löschung bei Deaktivierung/Abmeldung; Einstellung und Zeitstempel: bis zur Löschung des Nutzerkontos

Nachweis der Zustimmung zum vorzeitigen Beginn der Vertragsausführung beim Abo-Abschluss (Zeitpunkt der Erklärung, geltende AGB-Fassung, Abschnitt 8) | Bis zur Löschung des Nutzerkontos. Verlangst du die Löschung deiner Daten, ohne das Konto zu löschen, bleibt der Nachweis zur Abwicklung des Vertragsverhältnisses und zur Verteidigung von Rechtsansprüchen erhalten (Art. 17 Abs. 3 lit. e DSGVO)

Nutzungsstatistiken (Aufzeichnungen je Generierung, Abschnitt 7.3) | Bis zur Löschung des Nutzerkontos

Nutzungs-Messereignisse (Durchsetzung des Minutenkontingents) | 30 Tage

Anmelde- und Sicherheitsereignisse (Abschnitt 6.4; Ereignisart, Zeitpunkt, IP-Adresse, Browser, E-Mail-Adresse) | 90 Tage; zusätzlich entfernt, wenn das Konto endgültig gelöscht wird

Passwort-Zurücksetzungsanfragen (Token in gehashter Form, Gültigkeit, Zeitpunkt) | Automatische Löschung kurz nach Ablauf des Tokens, spätestens nach ca. 14 Tagen; zusätzlich entfernt, wenn das Konto endgültig gelöscht wird

Fehlerberichte (deine Beschreibung, technische Fehlerdetails) | Bis zur Löschung des Nutzerkontos oder aller Daten

Exportereignisse (Abschnitt 7.3) | Automatisch spätestens nach 30 Tagen

Blueprints | Bis zur Löschung durch den Nutzer

Anwendungslogs (Diagnosedaten, siehe 11.2) | 90 Tage

Verstoßeinträge (automatisierte Inhaltsprüfung) | Bis zur Löschung des Nutzerkontos. Verlangst du die Löschung deiner Daten, ohne das Konto zu löschen, werden diese Einträge zur Verhinderung weiteren Missbrauchs und zur Verteidigung von Rechtsansprüchen aufbewahrt (Art. 17 Abs. 3 lit. e DSGVO) und erst mit der Löschung des Kontos selbst entfernt

Support-Korrespondenz im Support-Postfach (Anfrage, Antworten, Bearbeitungsstatus, interner Vermerk; Abschnitt 8a) | 6 Monate nach Abschluss des Vorgangs, spätestens 12 Monate nach der letzten Nachricht; sofort mit der Löschung des Nutzerkontos

Moderations-Hinweis-E-Mails an den Verantwortlichen (enthalten den Auszug und die Nutzer-ID) | 6 Monate im Postfach, entsprechend der Frist für Support-Korrespondenz

Interne Hinweise über Kündigungserklärungen über die öffentliche Kündigungsseite (enthalten die eingegebene E-Mail-Adresse, die Kündigungsart und einen etwaig angegebenen Grund) | 6 Monate im Postfach, entsprechend der Frist für Support-Korrespondenz

Als Beweismittel gesicherte Inhalte in Kinderschutzfällen (Abschnitt 15a) | Getrennt und zugriffsbeschränkt gespeichert, bis das Melde- oder Behördenverfahren abgeschlossen ist, und unmittelbar danach gelöscht; ohne Rückmeldung der Behörden spätestens nach 90 Tagen. Diese Sicherung ist bewusst von allen automatischen Löschroutinen ausgenommen und überdauert auch einen Löschantrag oder die Löschung des Kontos, auf Grundlage von Art. 17 Abs. 3 lit. b und e DSGVO

Notiz-Freigaben (Freigabelinks, eingeladene E-Mail-Adressen) | Bis der Nutzer die Freigabe entfernt, die Notiz gelöscht wird oder das Nutzerkonto / alle Daten gelöscht werden

Server-Logdateien (Hosting/Railway) | 7–30 Tage

Verschlüsselte Backup-Kopien (Datenbank und Dateien, Abschnitt 12.1) | Maximal 35 Tage; automatische Löschung durch Rotation

Löschnachweis (pseudonymisiertes Verzeichnis ausgeführter Löschungen, Abschnitt 12.1) | 40 Tage, Entfernung durch einen täglichen Bereinigungslauf; enthält mit einem geheimen Schlüssel gebildete Hashwerte, eine Kategorienkennung und Zeitstempel — keine im Klartext lesbaren Kennungen

Wird eine Notiz zusammen mit ihren generierten Materialien gelöscht, wird die zugehörige

Audiodatei sofort aus dem Objektspeicher (Tigris) entfernt. Entscheidest du dich beim

Löschen einer Notiz, die generierten Materialien (Quellen, Karteikarten, Quizze) zu

behalten, bleiben sie gespeichert, bis du sie löschst; die Audiodatei wird in diesem Fall

automatisch durch die oben genannte ca. 30-Tage-Grenze entfernt.

12.1 Backup-Kopien und Löschung

Wir erstellen und verwahren verschlüsselte Backups unserer Datenbank und unseres Dateispeichers zur Notfallwiederherstellung und zur Erfüllung unserer vertraglichen Datensicherheitspflichten (Art. 32 DSGVO; Rechtsgrundlage Art. 6 Abs. 1 lit. f DSGVO — unser berechtigtes Interesse an der Verfügbarkeit und Integrität des Dienstes). Backups werden vor dem Upload auf unserer Seite verschlüsselt und schreibgeschützt bei einem europäischen Speicheranbieter abgelegt (Scaleway SAS, Frankreich — siehe Abschnitt 14); die Schlüssel verbleiben allein bei uns, sodass der Anbieter zu jedem Zeitpunkt nur unlesbaren Geheimtext hält. Backups werden spätestens 35 Tage nach ihrer Erstellung automatisch gelöscht. Das in diesem Abschnitt beschriebene Backup-Verfahren ist ab dem 13. September 2026 in Betrieb.

Löschst du deine Daten, wirkt die Löschung sofort in den Live-Systemen; löschst du dein Konto, wird es sofort unzugänglich und nach dem 30-tägigen Wiederherstellungsfenster endgültig gelöscht (siehe Tabelle oben). Zuvor erstellte Backup-Kopien können aus technischen und Sicherheitsgründen nicht nachträglich verändert werden (Schreibschutz); sie werden durch die automatische Rotation innerhalb von 35 Tagen entfernt. Alle Backup-Kopien gelöschter Kontodaten sind damit spätestens 65 Tage nach einer Kontolöschung verschwunden (30-tägiges Wiederherstellungsfenster plus 35-tägige Backup-Rotation). Sollten wir jemals ein Backup wiederherstellen müssen, wenden wir vor Wiederaufnahme des Dienstes alle zwischenzeitlich ausgeführten Löschungen erneut an. Zu diesem Zweck führen wir für 40 Tage ein pseudonymisiertes Löschverzeichnis (ein mit einem geheimen Schlüssel gebildeter Hash der Nutzer-ID und E-Mail-Adresse, dazu eine Kategorienkennung und Zeitstempel; Rechtsgrundlage ebenfalls Art. 6 Abs. 1 lit. f DSGVO i. V. m. Art. 17 Abs. 3 lit. b und Art. 32 DSGVO — das Verzeichnis existiert allein, um deiner Löschung Wirkung zu verschaffen). Ohne den Schlüssel, den nur wir halten, lassen sich diese Einträge keiner Person zuordnen.

13. Datensicherheit

Wir setzen folgende technische und organisatorische Sicherheitsmaßnahmen ein:

- Verschlüsselte Datenübertragung (TLS/HTTPS) mit HSTS-Preloading
- Content Security Policy (CSP) zum Schutz vor Cross-Site-Scripting (XSS)
- HttpOnly-Cookies zum Schutz der Sitzungsdaten vor JavaScript-Zugriff

Passwörter werden ausschließlich als kryptografische Hashes gespeichert (Argon2 für neue Konten; bcrypt für Bestandskonten mit automatischer Migration)

- Audiodateien sind nur über zeitlich begrenzte, signierte URLs zugänglich
- Die Anwendung läuft in isolierten Docker-Containern mit eingeschränkten Berechtigungen
- Eingabevalidierung und Pfadprüfung zum Schutz vor Injection-Angriffen
- CSRF-Schutz durch Origin-/Referer-Validierung bei allen verändernden API-Anfragen
- Rate Limiting auf allen sensiblen Endpunkten zum Schutz vor Brute-Force-Angriffen

Wöchentliche verschlüsselte, schreibgeschützte Backups bei einem separaten europäischen Anbieter (Abschnitt 12.1); Wiederherstellungsverfahren sind dokumentiert und werden regelmäßig getestet

14. Drittlandübermittlung

Folgende Dienstleister mit Sitz in den USA werden eingesetzt:

Dienstleister | Zweck | Garantie

Groq Inc. | KI-Transkription & Inhaltserzeugung | Standardvertragsklauseln (Modul 2) + TIA

OpenAI Ireland Ltd. (IE), Weiterübermittlung an OpenAI Inc. (USA) | KI-Inhaltserzeugung, Bild- & Textmoderation | Übermittlung innerhalb des EWR; Weiterübermittlung in die USA auf Grundlage der Standardvertragsklauseln nach Ziffer 4.1 des OpenAI-DPA + TIA

Cloudflare Inc. | Datenbank, DNS, Sicherheit | Standardvertragsklauseln, EU-U.S. Data Privacy Framework

Stripe Inc. | Zahlungsabwicklung | Standardvertragsklauseln, EU-U.S. Data Privacy Framework

Railway Corp. | Hosting, Redis (Rate Limiting) | Standardvertragsklauseln (Modul 2) + TIA

Tigris Data Inc. | Dateispeicher | Standardvertragsklauseln (Modul 2) + TIA

Google LLC | OAuth-Authentifizierung, Google-Ads-Conversion-Tracking (nur mit Einwilligung) | Standardvertragsklauseln, EU-U.S. Data Privacy Framework

Resend Inc. | Versand transaktionaler E-Mails | Standardvertragsklauseln, EU-U.S. Data Privacy Framework

Serper Inc. | Websuche (Recherche-Funktion) | Standardvertragsklauseln (Modul 2) + TIA

Zusätzlich setzen wir einen in der Europäischen Union niedergelassenen

Auftragsverarbeiter ein, für den keine Drittlandübermittlung stattfindet: Scaleway SAS

(Frankreich) speichert unsere verschlüsselten Backup-Kopien (Abschnitt 12.1)

ausschließlich in der EU. Die Backups werden vor dem Upload verschlüsselt; Scaleway erhält zu jedem Zeitpunkt nur Geheimtext.

Die Aktualität der DPF-Zertifizierungen wird regelmäßig über dataprivacyframework.gov

geprüft. Sollte eine Zertifizierung entfallen, stützen wir die Übermittlung

ausschließlich auf Standardvertragsklauseln in Verbindung mit einem Transfer Impact Assessment.

Der dem EU-U.S. Data Privacy Framework zugrunde liegende Angemessenheitsbeschluss ist derzeit Gegenstand eines Verfahrens vor dem Gerichtshof der Europäischen Union. Er bleibt in Kraft. Weil wir uns nicht darauf verlassen können, dass das so bleibt, halten wir für die oben genannten DPF-zertifizierten Anbieter zusätzlich Standardvertragsklauseln und ein dokumentiertes Transfer Impact Assessment als Rückfallebene vor, sodass ein Wegfall des Angemessenheitsbeschlusses für sich genommen keine Übermittlung ohne Garantie zurückließe.

15. Rechte der betroffenen Personen

Im Rahmen der geltenden gesetzlichen Bestimmungen hast du folgende Rechte:

- Auskunft über deine gespeicherten personenbezogenen Daten (Art. 15 DSGVO)
- Berichtigung unrichtiger oder unvollständiger Daten (Art. 16 DSGVO)
- Löschung deiner Daten (Art. 17 DSGVO)

- Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruch gegen die Verarbeitung (Art. 21 DSGVO)

Soweit eine Verarbeitung auf deiner Einwilligung beruht, kannst du sie jederzeit mit Wirkung für die Zukunft widerrufen. Den Widerruf der Cookie-Einwilligung kannst du jederzeit über die Cookie-Einstellungen in der Anwendung vornehmen.

Zudem hast du ein Beschwerderecht bei einer

Datenschutz-Aufsichtsbehörde, insbesondere in dem Mitgliedstaat deines gewöhnlichen Aufenthalts oder des Orts des mutmaßlichen Verstoßes. Die für uns zuständige Aufsichtsbehörde ist:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg
Heilbronner Straße 35, 70191 Stuttgart

Postanschrift: Postfach 10 29 32, 70025 Stuttgart

Telefon: +49 (0) 711 / 615541-0

E-Mail: poststelle@lfdi.bwl.de

Web: www.baden-wuerttemberg.datenschutz.de

Anfragen sind jederzeit über die im Impressum angegebenen Kontaktdaten möglich.

15a. Automatisierte Inhaltsprüfung und menschliche Entscheidungen

Heyblocks setzt eine automatisierte Inhaltsprüfung ein, die hochgeladene Inhalte vor der Verarbeitung gegen unsere Nutzungsregeln prüft (siehe Abschnitt 5.3). Wird ein Inhalt markiert, wird dieser Upload abgelehnt, und dir wird mitgeteilt, warum. Automatisch geschieht darüber hinaus nichts.

Funktionsweise: Ein KI-Modell bewertet den Inhalt und gibt eine Kategorie

(zum Beispiel Gewalt, Hassrede, Kinderschutz, illegale Aktivität, Belästigung oder ein Versuch, das KI-System zu manipulieren) samt kurzer Begründung zurück. Das Modell erhält nur den Inhalt selbst: keine Nutzer-ID, keine Kontodaten, keine E-Mail-Adresse und keine Historie werden an es übermittelt, sodass es dich weder identifizieren noch bewerten kann. Wird nichts markiert, hinterlässt die Prüfung keinerlei Spur.

Folgen: Eine Ablehnung verhindert die Verarbeitung dieser einen Datei. Sie schränkt dein Konto nicht ein, und auch wiederholte Ablehnungen schränken es nicht ein; es gibt keine automatische Eskalation und keine automatische Sperrung. Ein markierter Inhalt wird dokumentiert und in eine Warteschlange zur Prüfung durch einen Menschen gestellt. Nur dieser Mensch kann ein Konto einschränken oder sperren, und nur nach Prüfung des Falls; der Grund wird dokumentiert. Ergibt die Prüfung, dass der Inhalt tatsächlich nicht gegen unsere Regeln verstoßen hat, wird der Eintrag als Fehlalarm markiert und der gespeicherte Auszug deines Inhalts gelöscht.

Automatisierte Entscheidungsfindung im Sinne von Art. 22 DSGVO: Wir

vertreten die Auffassung, dass Art. 22 Abs. 1 DSGVO nicht einschlägig ist, weil der automatisierte Teil dieses Verfahrens weder rechtliche Wirkung entfaltet noch eine ähnlich erhebliche Beeinträchtigung darstellt: Sein einziges Ergebnis ist, dass ein einzelner Upload nicht verarbeitet wird. Jede Entscheidung, die dich erheblich betrifft, insbesondere jede Einschränkung deines Kontos, wird von einem Menschen getroffen. Unabhängig davon kannst du jederzeit das Eingreifen einer natürlichen Person erwirken, deinen eigenen Standpunkt darlegen und eine Entscheidung anfechten, indem du an info@heyblockslabs.com schreibst. Dieses Recht unterliegt keiner zeitlichen Begrenzung.

§ 11 Abs. 6 unserer Nutzungsbedingungen sieht zusätzlich ein förmliches Beschwerdeverfahren nach dem Vorbild von Art. 20 des Digital Services Act vor, offen für sechs Monate nach der Entscheidung mit einer Antwort innerhalb von 10 Werktagen.

Beweissicherung in Kinderschutzfällen: Markiert die Prüfung Inhalte in der Kategorie Kinderschutz, kopieren wir die betroffene Datei und das Transkript in einen separaten, zugriffsbeschränkten Speicherbereich, damit das Material für eine Meldung an die zuständigen Behörden verfügbar bleibt. Diese Sicherung ist bewusst von allen automatischen Löschroutinen ausgenommen und überdauert auch einen Löschantrag oder die Löschung des Kontos; Rechtsgrundlage ist Art. 17 Abs. 3 lit. b und e DSGVO. Sie wird gelöscht, sobald das Melde- oder Behördenverfahren abgeschlossen ist, und ohne Rückmeldung der Behörden spätestens nach 90 Tagen. Abschnitt 12 weist dies auch in der Speicherdauertabelle aus.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Sicherheit und Integrität der Anwendung und am Schutz vor rechtswidrigen Inhalten), in Verbindung mit Art. 6 Abs. 1 lit. b DSGVO, soweit die in § 11 unserer Nutzungsbedingungen vereinbarten Inhaltsregeln durchgesetzt werden.

Besondere Kategorien personenbezogener Daten: Die Prüfung zielt nicht darauf ab, ein Merkmal deiner Person im Sinne von Art. 9 Abs. 1 DSGVO festzustellen. Sie bewertet, ob Inhalte gegen unsere Regeln verstoßen, und gibt einen Kategoriencode zurück; sie leitet nicht ab, speichert nicht und bewertet nicht deine ethnische Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, dein Sexualleben oder deine sexuelle Orientierung. Von dir hochgeladene Inhalte können derartige Informationen gleichwohl beiläufig enthalten. Soweit wir einen kurzen Auszug zur Dokumentation eines Verstoßes aufbewahren, ist Rechtsgrundlage dieser Speicherung Art. 9 Abs. 2 lit. f DSGVO (Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen). Für Kategorien, in denen keine menschliche Prüfung vorgesehen ist, wird gar kein Auszug gespeichert. Ein Datenschutzbeauftragter wurde nicht benannt, weil die Voraussetzungen für eine Pflichtbenennung nicht vorliegen: Unsere Kerntätigkeit ist weder die umfangreiche,

regelmäßige und systematische Überwachung betroffener Personen noch die umfangreiche Verarbeitung besonderer Datenkategorien (Art. 37 Abs. 1 DSGVO), und es sind weniger als zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 Abs. 1 BDSG). Wir überprüfen diese Einschätzung, wann immer sich die Verarbeitung ändert.

15b. Meldungen rechtswidriger Inhalte (Art. 16 DSA)

Über unser Meldeformular (heyblocks.app/report) kann uns jede Person Inhalte melden, die sie für rechtswidrig hält. Das ist ausdrücklich auch ohne Nutzerkonto möglich, weil Art. 16 der Verordnung (EU) 2022/2065 (Digital Services Act) das so verlangt. Melden ist damit einer der wenigen Fälle, in denen wir Daten von Personen verarbeiten, die unseren Dienst gar nicht nutzen.

Verarbeitete Daten: Name und E-Mail-Adresse der meldenden Person, die angegebene URL, die Art des behaupteten Verstoßes, die Begründung im Freitext sowie Zeitpunkt und Vorgangsnummer der Meldung. Bei Meldungen zu Darstellungen sexuellen Kindesmissbrauchs (Art. 3 bis 7 der Richtlinie 2011/93/EU) sind Name und E-Mail-Adresse nicht erforderlich; solche Meldungen können anonym abgegeben werden.

Zweck: Bearbeitung der Meldung, Eingangsbestätigung und Mitteilung der Entscheidung an die meldende Person (Art. 16 Abs. 4 und 5 DSA), Begründung gegenüber der von einer Maßnahme betroffenen Person (Art. 17 DSA), Erkennung missbräuchlicher Meldungen sowie Nachweis der ordnungsgemäßen Bearbeitung.

Rechtsgrundlage: Art. 6 Abs. 1 lit. c DSGVO (rechtliche Verpflichtung aus Art. 16 DSA) sowie Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Abwehr missbräuchlicher Meldungen und an der Nachweisbarkeit unserer Entscheidungen).

Speicherdauer: 12 Monate ab Eingang der Meldung, danach automatisierte Löschung. Wird die Meldung an Behörden weitergeleitet oder ist ein Verfahren anhängig, speichern wir sie, solange dies zur Rechtsverteidigung erforderlich ist (Art. 17 Abs. 3 lit. e DSGVO). Wird das Konto der betroffenen Person gelöscht, entfernen wir die Verknüpfung zu diesem Konto; der Meldevorgang selbst bleibt als Nachweis bestehen, weil er die Daten der meldenden Person betrifft und nicht die der gelöschten Person.

Empfänger: Der Inhalt einer Meldung wird der von der Maßnahme betroffenen Person in der Begründung nach Art. 17 DSA mitgeteilt, soweit dies zur Erklärung der Entscheidung erforderlich ist. Die Identität der meldenden Person geben wir dabei nicht weiter, außer wenn dies gesetzlich zwingend ist. Bei Verdacht auf eine Straftat, die eine Gefahr für das Leben oder die Sicherheit einer Person begründet, informieren wir die zuständigen Strafverfolgungsbehörden (Art. 18 DSA).

16. Newsletter

Wir bieten derzeit keinen Newsletter an. Sollte künftig ein Newsletter angeboten werden, wird er ausschließlich auf Grundlage deiner ausdrücklichen Einwilligung versandt. Die optionalen Karteikarten-Erinnerungs-E-Mails (Abschnitt 7.8) sind kein Newsletter; auch sie werden ausschließlich auf Grundlage deiner ausdrücklichen Einwilligung versandt.

17. Änderungen dieser Datenschutzerklärung

Wir behalten uns vor, diese Datenschutzerklärung anzupassen, um sie an geänderte rechtliche Anforderungen oder neue Funktionen anzupassen. Die aktuelle Fassung ist stets in der Anwendung abrufbar.

Diese Datenschutzerklärung wird auf Deutsch und Englisch bereitgestellt. Maßgeblich ist die deutsche Fassung; die englische Fassung dient der Verständlichkeit.