

DATENSCHUTZERKLÄRUNG FÜR BRAINY

Stand: 13. April 2026

1. Verantwortlicher und Kontaktdaten

Verantwortlich für die Verarbeitung Ihrer personenbezogenen Daten ist:

Latoo.labs GmbH, FN 565855s, Kraußstraße 16, 4020 Linz, Österreich.

E-Mail: office@latoo.at Website: www.abrainy.com

2. Datenschutzbeauftragter

Unser Datenschutzbeauftragter steht Ihnen für Fragen zum Datenschutz zur Verfügung:

Mag. Kurt Schmid, Kraußstraße 16, 4020 Linz, Österreich

E-Mail: datenschutz@latoo.at

3. Welche Daten wir verarbeiten:

Bei der Nutzung von Brainy verarbeiten wir folgende personenbezogene Daten:

Registrierungs- und Kontodaten:

- Name
- E-Mail-Adresse
- Telefonnummer
- Nutzer-ID
- Authentifizierungsdaten (Passwort in verschlüsselter Form)

Nutzungs- und Telemetriedaten:

- Metadaten zur App-Nutzung (z.B. Nutzungshäufigkeit, Zeitstempel, App-Version)
- Token-/Nutzungszähler (pro Organisation/Account)
- Geräte-/Betriebssystem-/App-Informationen

Inhalte (Auftragsdaten):

- Textliche und sprachliche Eingaben (z.B. Aufzeichnungen, Transkriptionen)
- Von Ihnen erstellte und gespeicherte Inhalte (Dokumente, Dateien, Bilder, Videos)

Inhalte Dritter:

- Informationen über andere Personen, die Sie in Ihren Eingaben erwähnen (z.B. Klienten, Patienten, Mitarbeitenden)

Connector-Daten (nur bei aktivierten Konnektoren):

- Daten, die KI-Agenten über Konnektoren aus Drittdiensten lesen (z. B. E-Mail-Inhalte, Dateiinhalte, Kalendereinträge, CRM-Datensätze)
- Daten, die KI-Agenten in Drittdienste schreiben (z. B. versendete E-Mails, erstellte Dateien)
- Connector-Credentials (OAuth-Tokens, API-Schlüssel) zur Anbindung von Drittdiensten

Filesystem-Daten (nur bei Nutzung des gemeinsamen Dateibereichs):

- Dateien, Ordner und Metadaten, die Sie im gemeinsamen Dateibereich (Nextcloud-Instanz) ablegen oder die KI-Agenten dort bereitstellen

MCP-Server-Daten (nur bei Nutzung von MCP-Servern):

- Daten, die KI-Agenten über Anbieter- oder Kunden-MCP-Server beziehen oder dorthin übermitteln

Aktionsprotokolle von KI-Agenten:

- Protokolle aller durch KI-Agenten ausgeführten Aktionen (Zeitstempel, Tool-Aufrufe, Ergebnisse, verwendete Modelle)
- Protokolle der Aktivierung und Deaktivierung von MCP-Tools

3a. Pflicht zur Bereitstellung und Freiwilligkeit:

- Für die Registrierung und Durchführung des Nutzungsvertrags ist die Bereitstellung von Basis-Kontodaten (z.B. Name, E-Mail-Adresse, Zahlungsangaben) erforderlich. Ohne diese Daten ist eine Nutzung von Brainy nicht möglich.
- Die Nutzung von KI-Modellen der Kategorien „DSGVO“ und „Weltweit“ ist freiwillig. Alle Kernfunktionen der Anwendung stehen auch bei ausschließlicher Nutzung EU-gehosteter Modelle zur Verfügung. Sie können die zulässigen Modell-Kategorien jederzeit mandantenweit einschränken (vgl. Ziff. 4.5). Ebenso ist die Nutzung von Agentic AI Funktionen, Konnektoren und MCP-Servern freiwillig; die Kernfunktionen der Anwendung (Transkription, Dokumentenerstellung) sind auch ohne diese Funktionen nutzbar.

4. Zwecke und Rechtsgrundlagen der Datenverarbeitung

Als B2B-SaaS-Anbieter haben wir eine Doppelrolle: Für die Kernfunktionen von Brainy sind wir Ihr Auftragsverarbeiter, für den Betrieb und die Verbesserung unserer Plattform sind wir Verantwortlicher für eigene Geschäftszwecke.

4.1 Als Ihr Auftragsverarbeiter

Brainy fungiert als **Auftragsverarbeiter** für Ihre berufliche Datenverarbeitung. **Sie sind Verantwortlicher** im Sinne der DSGVO.

Rechtsgrundlage: Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Das bedeutet:

- **Sie** bestimmen Zwecke und Mittel der Datenverarbeitung
- **Sie** sind verantwortlich für Rechtsgrundlagen (auch bei Gesundheitsdaten nach Art. 9 DSGVO)
- **Wir** verarbeiten nur auf Ihre dokumentierte Weisung

Ihre Pflichten als Verantwortlicher:

- Abschluss eines Auftragsverarbeitungsvertrags mit uns
- Rechtsgrundlagen für eingegebene Daten (insb. Patientendaten)

- Information und Einwilligung Ihrer Mitarbeitenden/Mandanten/Kunden (falls erforderlich)
- Berufsgeheimnisse und spezielle Compliance-Anforderungen beachten
- Einhaltung beruflicher Schweigepflichten
- Auswahl geeigneter KI-Modelle (EU vs. Nicht-EU) für Ihre Datenarten. **Unsere Empfehlung:** Verwenden Sie für sensible Daten ausschließlich **EU-gehostete KI-Modelle**.

Zwecke der Auftragsverarbeitung:

- Bereitstellung der Brainy-Kernfunktionen gemäß Ihrem Auftrag
- Sprach-zu-Text-Umwandlung Ihrer Audio-Aufzeichnungen
- KI-gestützte Dokumentenerstellung nach Ihren Vorgaben
- Speicherung und Verarbeitung von Audio, Video, Bild- und Textdaten
- Synchronisation zwischen Ihren Endgeräten
- Agentic AI und Konnektoren (nur sofern von Ihnen aktiviert):
 - Betrieb und Ausführung von KI-Agenten in Ihrem Auftrag
 - Herstellen und Aufrechterhalten von Verbindungen zu Drittdiensten über Konnektoren (mittels Nango-Infrastruktur)
 - Lesen und schreiben von Daten in Drittdiensten über Konnektoren auf Ihre Weisung
 - Sichere Verwahrung von Connector-Credentials
 - Bereitstellung eines gemeinsamen Dateibereichs (Nextcloud) für den Datenaustausch zwischen Ihnen und KI-Agenten
 - Bereitstellung von Anbieter-MCP-Servern als standardisierte Agenteninfrastruktur
 - Verarbeitung von Daten, die KI-Agenten über Kunden-MCP-Server beziehen
 - Granulare Steuerung einzelner MCP-Tools (Default-Off: Alle Tools sind standardmäßig deaktiviert und werden erst nach Ihrer expliziten Aktivierung nutzbar)
 - Protokollierung aller Agentenaktionen und Tool-Aktivierungen/-Deaktivierungen
- Erstellung strukturierter Dokumente aus verbalen Aufzeichnungen

Verarbeitete Daten:

- Ihre Audio-Aufzeichnungen und Spracheingaben
- Daraus erstellte Transkriptionen und Dokumente
- Von Ihnen eingegebene und gespeicherte Inhalte
- Inhalte über Dritte (z.B. Patienten, Mandanten, Mitarbeitenden), die Sie erwähnen

4.2 Als Verantwortlicher für unsere eigenen Zwecke

Für den Betrieb und die Verbesserung unserer Brainy Plattform verarbeiten wir Daten für eigene Geschäftszwecke.

Rechtsgrundlagen:

- Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO): Registrierung und Verwaltung Ihres Accounts, Bereitstellung und Betrieb der Anwendung, Support, Abrechnung.
- Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO): Technische Administration, Sicherheits- und Missbrauchsprävention, Stabilität sowie produktbezogene Auswertungen auf Basis anonymisierter oder, wo erforderlich, pseudonymisierter Betriebs-/Telemetriedaten. Ihre Interessen werden durch Datenminimierung, kurze Speicherfristen und Konfigurationsmöglichkeiten gewahrt.

Hinweis zu nicht EU-gehosteten Modellen: Die optionale Nutzung nicht EU-gehosteter KI-Modelle erfolgt ausschließlich auf Ihre dokumentierte Auswahl/Weisung innerhalb der App. Die hierfür erforderlichen Übermittlungen an Anbieter in Drittländern stützen wir auf EU-Standardvertragsklauseln (Art. 46 DSGVO) und zusätzliche Schutzmaßnahmen. Für etwaige Rechtsgrundlagen in Bezug auf von Ihnen eingegebene Daten Dritter (z.B. Patienten-/Mandantendaten) sind Sie als Verantwortlicher zuständig.

Zwecke unserer eigenen Verarbeitung:

- Bereitstellung und Betrieb der Brainy-Anwendung
- Vertragsabwicklung (Registrierung, Abrechnung, Support)
- Technische Administration und Systemsicherheit
- Produktverbesserung und Entwicklung neuer Features
- Fehleranalyse und Qualitätssicherung, Support
- Compliance und rechtliche Verpflichtungen

Verarbeitete Daten:

Kontodaten:

- Name, E-Mail-Adresse, Telefonnummer, optional Profilbild
- Nutzer-ID und Authentifizierungsdaten
- Rechnungs- und Zahlungsinformationen

Technische Daten (eigene Zwecke):

- Modell-/Assistenten-IDs, Zeitstempel, Feature-Flags, Token-/Nutzungszähler pro Organisation/benutzendem Account, Geräte-/App-Versionen
- Fehler-/Performance-Protokolle (z.B. Exception-IDs, Statuscodes; ohne Inhaltsdaten)
- IP-Adressen für Sicherheitszwecke (kurzfristig)

Klarstellung: Inhalte (z.B. „Chatverläufe“, Transkriptionen, Dokumente) werden für eigene Zwecke nicht ausgewertet. Zugriffe auf Inhalte erfolgen nur im Rahmen der Auftragsverarbeitung bzw. im Supportfall auf Ihre Weisung.

Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO):

- Unser Interesse: Sicherer und verbesserter Service
- Erforderlichkeit: Verarbeitung auf Basis anonymisierter oder, wo erforderlich, pseudonymisierter Betriebs-/Telemetriedaten; keine Auswertung von Inhalten
- Ihre Interessen: Wahrung der Vertraulichkeit, kurze Speicherfristen, Konfigurations-/Opt-Out-Möglichkeiten
- Abwägung: Überwiegen unserer Interessen bei beschriebenen Schutzmaßnahmen

4.3 Auftragsverarbeitungsvertrag

Die Einzelheiten der Auftragsverarbeitung sind in unserem separaten Auftragsverarbeitungsvertrag (AVV) geregelt, der folgende Punkte umfasst:

- Detaillierte Weisungen zur Datenverarbeitung
- Technische und organisatorische Maßnahmen (TOMs)
- Unterauftragsverarbeiter und deren Pflichten
- Lösungsmodalitäten und Datenrückgabe
- Unterstützung bei Betroffenenrechten
- Meldepflichten bei Datenschutzvorfällen

Der AVV ist integraler Bestandteil Ihres Nutzungsvertrags. Informationen zu eingesetzten Unterauftragsverarbeitern, zu Standardvertragsklauseln und zu zusätzlichen Schutzmaßnahmen stellen wir auf Anfrage zur Verfügung.

4.4 Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

 **Wichtiger Hinweis für Ärzte, Therapeuten und andere Gesundheitsberufe:**

Bei der Verarbeitung von Gesundheitsdaten über Brainy sind Sie als Auftraggeber verantwortlich für:

- Rechtmäßigkeit nach Art. 9 DSGVO (z.B. Patienteneinwilligung, medizinische Diagnostik)
- Auswahl EU-gehosteter KI-Modelle für maximalen Schutz
- Information Ihrer Patienten über die Nutzung von Brainy
- Einhaltung berufsrechtlicher Vorgaben und ärztlicher Schweigepflicht

Unsere Empfehlung: Verwenden Sie für Gesundheitsdaten ausschließlich mit "EU" gekennzeichnete KI-Modelle.

4.5 Modell-Kategorien und Drittlandverarbeitung

Brainy bietet KI-Modelle in drei Kategorien an: „EU“ (vollständige Verarbeitung in der EU), „DSGVO“ (Speicherung in der EU, Inference-Verarbeitung ggf. auch außerhalb der EU) und „Weltweit“ (derzeit Verarbeitung und Speicherung in den USA). Jedes KI-Modell ist in der Anwendung transparent mit seiner Kategorie gekennzeichnet.

Standardmäßig stehen Ihnen alle verfügbaren KI-Modelle aller Kategorien zur Auswahl. Die Auswahl eines Modells der Kategorie „DSGVO“ oder „Weltweit“ durch Sie oder Ihre autorisierten Nutzer gilt als dokumentierte Weisung zur Verarbeitung gemäß den Bedingungen der jeweiligen Kategorie, einschließlich der damit verbundenen Drittlandübermittlungen.

Nutzen Sie innerhalb eines Workflows Modelle unterschiedlicher Kategorien, wird der gesamte Workflow mit der Kategorie des am weitesten reichenden Modells gekennzeichnet (Prinzip des schwächsten Glieds).

Sie können die zulässigen Modell-Kategorien für Ihre gesamte Organisation jederzeit durch eine einmalige schriftliche Weisung auf „Nur EU“ oder „EU + DSGVO“ einschränken. Nach Umsetzung der Einschränkung werden Modelle ausgeschlossener Kategorien in der Benutzeroberfläche nicht mehr angeboten. Die Einschränkung kann jederzeit durch eine neue Weisung geändert oder aufgehoben werden.

Für die Drittlandübermittlungen setzen wir EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) und zusätzliche technische und organisatorische Schutzmaßnahmen ein. Für sensible Daten (insbesondere Art. 9 DSGVO) empfehlen wir die ausschließliche Nutzung EU-gehosteter Modelle.

5. Empfänger der Daten

Zur Bereitstellung unserer Dienste nutzen wir folgende Unterauftragsverarbeiter, die Zugriff auf Ihre Daten haben können:

5.1 Unterauftragsverarbeiter (EU-Hosting; Verarbeitung von Inhalten/Auftragsdaten)

- **Microsoft Ireland Operations Ltd.** (Azure Cloud-Services, EU-Standort) - Bereitstellung von EU-gehosteten KI-Modellen
- **Amazon Web Services EMEA SARL (AWS)** (Cloud-Services, EU-Standort) - Bereitstellung von EU-gehosteten KI-Modellen
- **Google Ireland Limited** (KI-Modelle, EU-Standort) - Bereitstellung von EU-gehosteten KI-Modellen
- **FOX Informationstechnologie GmbH** (Hosting der Infrastruktur, EU-Standort) - verantwortlich für das physische Hosting der Applikation und Datenbanken der selbst betriebenen Nextcloud-Instanz (gemeinsamer Dateibereich) sowie der Anbieter-MCP-Server
- **BFL GmbH** (Deutschland) - Bereitstellung von Bild-KI-Modellen („Flux“)

5.1a Unterauftragsverarbeiter mit teilweiser Drittlandverarbeitung (Kategorie „DSGVO“)

- **Microsoft Ireland Operations Ltd.** (Azure OpenAI, Deployment-Typ „Global Standard“) – KI-Modelle, bei denen die Speicherung in der EU erfolgt, die Inference-Verarbeitung jedoch global (einschließlich USA) stattfinden kann. Rechtsgrundlage: EU-Standardvertragsklauseln und zusätzliche Schutzmaßnahmen. Nutzung nur auf Ihre dokumentierte Weisung.

5.1b Unterauftragsverarbeiter für Konnektor-Infrastruktur (nur bei aktivierten Konnektoren)

- **Nango Inc.** (USA, mit EU-Rechenzentrumsoptionen) – Bereitstellung der technischen Infrastruktur für Konnektoren zu Drittdiensten; sichere Verwahrung von Connector-Credentials (OAuth-Tokens, API-Schlüssel); technische Abwicklung von API-Aufrufen. Nango verarbeitet ausschließlich Connector-Credentials und technische Metadaten; Inhalte aus Drittdiensten werden nur transient weitergeleitet und nicht dauerhaft gespeichert. Rechtsgrundlage: EU-Standardvertragsklauseln.

5.2 Unterauftragsverarbeiter (Drittlandverarbeitung; nur bei optionaler Nutzung nicht EU-gehosteter Modelle)

Rechtsgrundlage für Übermittlungen: EU-Standardvertragsklauseln (Art. 46 DSGVO) und zusätzliche Schutzmaßnahmen; Nutzung nur auf Ihre dokumentierte Auswahl/Weisung in der App.

- **OpenAI Inc.** (USA) - Bereitstellung von nicht EU-gehosteten KI-Modellen
- **Perplexity AI Inc.** (USA) – Bereitstellung von nicht EU-gehosteten LLMs
- **Anthropic PBC** (USA)– Bereitstellung von nicht EU-gehosteten LLMs
- **X.AI LLC (USA)** – Bereitstellung von nicht EU-gehosteten LLMs („Grok“)
- **Black Forest Labs Inc. (USA)** - Bereitstellung von nicht EU-gehosteten KI-Modellen („Flux“)
- **Google LLC (USA)** - Bereitstellung von nicht EU-gehosteten LLMs

5.3 Dienstleister für unsere eigenen Zwecke (keine Verarbeitung von Inhalten/Auftragsdaten)

- **Clerk Inc.** – Identitäts- und Zugriffsverwaltung (EU-Standorte, soweit konfiguriert); Rechtsgrundlage: EU-U.S. Data Privacy Framework und/oder EU-Standardvertragsklauseln
- **Functional Software Inc. d/b/a Sentry** – Fehlerüberwachung/Anwendungsdiagnose (EU-Standorte, soweit konfiguriert); Rechtsgrundlage: EU-Standardvertragsklauseln

Klarstellung: Diese Dienstleister verarbeiten Konto-/Betriebs-/Telemetriedaten für Betrieb und Sicherheit; Auftragsdaten/Inhalte werden nicht übermittelt (Einsatz mit Maskierung/Redaction und restriktiver Konfiguration).

Klarstellung interne Systembestandteile: Der Anbieter betreibt Nextcloud als eigenverantwortlich gehostete Open-Source-Software auf der FOX IT-Infrastruktur; Nextcloud GmbH (Softwareanbieter) erhält keine Kundendaten und ist kein Unterauftragsverarbeiter. Ebenso erhalten MCP-Protokoll-Entwickler (z. B. Anthropic PBC als Spezifikationsherausgeber) keine Kundendaten. Kunden-MCP-Server sind Infrastruktur des Nutzers und kein Unterauftragsverarbeiter des Anbieters.

6. Datenverarbeitung außerhalb der EU

6.1 EU-gehostete Dienste

Unsere primären Produktivsysteme sind auf EU-Rechenzentren ausgerichtet; planmäßige Übermittlungen in Drittländer erfolgen hierbei nicht. In Ausnahmefällen kann es zu unterstützungsbedingten Remote-Zugriffen aus Drittländern kommen. In solchen Fällen stellen wir geeignete Garantien gemäß Kapitel V DSGVO (z.B. Standardvertragsklauseln) sicher.

6.2 Nicht-EU-gehostete Dienste (optional)

Wenn Sie in der App nicht EU-gehostete KI-Modelle auswählen, werden die hierfür erforderlichen Daten an Anbieter in Drittländern übermittelt und dort verarbeitet. Wir verwenden dafür EU-Standardvertragsklauseln (Art. 46 DSGVO) und zusätzliche Schutzmaßnahmen. Bitte beachten Sie, dass in einigen Drittländern (z.B. USA) ein gegenüber der EU niedrigeres Datenschutzniveau besteht und Behördenzugriffe möglich sind. Die Nutzung nicht EU-gehosteter Modelle ist optional; für sensible Daten empfehlen wir die ausschließliche Nutzung EU-gehosteter Modelle.

Wenn Sie Konnektoren zu Drittdiensten aktivieren, werden Connector-Credentials und technische Metadaten über die Infrastruktur von Nango Inc. (USA) verarbeitet. Die Übermittlung erfolgt auf Basis von EU-Standardvertragsklauseln. Inhalte aus Drittdiensten (Connector-Daten) werden durch Nango nur transient weitergeleitet und nicht dauerhaft gespeichert.

7. Speicherdauer

Wir speichern Ihre personenbezogenen Daten nur so lange, wie es für die Erfüllung der oben genannten Zwecke erforderlich ist:

- **Kontodaten:** Für die Dauer Ihres Nutzungsverhältnisses und danach für die Dauer gesetzlicher Aufbewahrungsfristen.
- **Aufzeichnungen und Transkriptionen:** Gemäß der in Ihrem Produkttarif vereinbarten Speicherfristen. Diese beträgt maximal ein Jahr ab Erstellung.
- **KI-Verarbeitungsdaten:** Anbieterabhängig begrenzte Speicherfristen, typischerweise bis zu 30 Tage.
- **Sicherheits-/Zugriffsprotokolle** (inkl. IP-Adressen): Bis zu 30 Tage, verlängert, wenn es für die Aufklärung sicherheitsrelevanter Vorfälle erforderlich ist.
- **Fehler-/Performance-Protokolle** (z.B. Sentry): Bis zu 90 Tage, ausschließlich zu Diagnose-/Stabilitätszwecken, ohne Inhaltsdaten.
- **Nutzungs-/Tokenmetriken und Abrechnungsdaten:** Bis zu 24 Monate zur Nachvollziehbarkeit und Abrechnung; anschließend Aggregation/Anonymisierung. Hinweis: Backups werden im Rahmen regulärer Zyklen überschrieben; eine selektive Löschung in laufenden Sicherungen erfolgt nicht.
- **Connector-Credentials:** Unverzüglich, spätestens 72 Stunden nach Deaktivierung des Konnektors oder nach Vertragsende.
- **Connector-Aktionsprotokolle** (Audit-Logs): 90 Tage.
- **MCP-Tool-Aktivierungs-/Deaktivierungsprotokolle:** Für die Dauer des Vertragsverhältnisses zuzüglich 90 Tage.
- **Filesystem-Daten (Nextcloud):** Nach Vertragsende 30 Tage Übergabefrist (Export möglich), danach unwiderrufliche Löschung

Nach Ablauf der Speicherfrist oder bei Beendigung Ihres Nutzungsverhältnisses werden Ihre Daten gelöscht oder anonymisiert, sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

8. Ihre Rechte als betroffene Person

Unsere Doppelrolle bei Betroffenenrechten

Je nach Art Ihrer Daten haben Sie unterschiedliche Ansprechpartner für die Ausübung Ihrer Rechte:

8.1 Als unser direkter Nutzer (Kontodaten, Metadaten):

Wir sind Verantwortlicher → Sie wenden sich direkt an uns

8.2 Als Ersteller von Inhalten (Audio, Dokumente):

Sie sind Verantwortlicher, wir Auftragsverarbeiter → Wir unterstützen Sie bei der Rechtsdurchsetzung

8.1 Ihre Rechte als direkter Nutzer

Für Ihre Kontodaten, Nutzungsstatistiken und technischen Daten sind wir direkt zuständig:

Auskunftsrecht (Art. 15 DSGVO)

Was wir Ihnen mitteilen:

- Welche Kategorien personenbezogener Daten wir über Sie verarbeiten
- Zwecke der Verarbeitung und Rechtsgrundlagen
- Empfänger oder Kategorien von Empfängern
- Geplante Speicherdauer
- Ihre Rechte (Berichtigung, Löschung, etc.)
- Bei Drittlandübermittlung: geeignete Garantien

Recht auf Berichtigung (Art. 16 DSGVO)

Unrichtige Daten korrigieren lassen:

- E-Mail-Adresse, Namen, Telefonnummer
- Fehlerhaft gespeicherte Nutzungsstatistiken
- Verfahren: Korrektur binnen 5 Werktagen

Recht auf Löschung (Art. 17 DSGVO)

Löschung verlangen, wenn:

- Daten für ursprüngliche Zwecke nicht mehr erforderlich
- Daten unrechtmäßig verarbeitet wurden
- gesetzliche Löschpflichten bestehen

Recht auf Einschränkung (Art. 18 DSGVO)

Verarbeitung einschränken bei:

- Bestrittener Richtigkeit (während Prüfung)
- Unrechtmäßiger Verarbeitung (statt Löschung)
- Nicht mehr benötigten Daten (die Sie für Rechtsansprüche brauchen)

Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Strukturierte Datenausgabe:

- Ihre Kontodaten in JSON/CSV-Format
- Nutzungsstatistiken und Einstellungen
- Nicht übertragbar: Von Ihnen erstellte Inhalte (siehe 8.2)

Widerspruchsrecht (Art. 21 DSGVO)

Widerspruch bei berechtigtem Interesse:

- Produktverbesserung auf Basis anonymisierter Daten
- Direktmarketing (falls zutreffend)
- Prüfung: Ob unsere Interessen überwiegen

Widerruf der Einwilligung (Art. 7 Abs. 3 DSGVO) und Deaktivierung von Nicht-EU-Modellen

- Soweit eine Verarbeitung auf Einwilligung beruht (z.B. Newsletter/Marketing), können Sie diese jederzeit mit Wirkung für die Zukunft widerrufen. Die Rechtmäßigkeit bis zum Widerruf bleibt unberührt.
- Unabhängig davon können Sie die verfügbaren Modell-Kategorien für Ihre Organisation jederzeit einschränken, indem Sie per schriftlicher Weisung die Stufe „Nur EU“ oder „EU + DSGVO“ festlegen (vgl. Ziff. 4.5). Einzelne Nutzer können zudem bei jeder Verarbeitungshandlung ein EU-gehostetes Modell auswählen.

8.2 Rechte bezüglich Ihrer erstellten Inhalte

Für Audio-Aufzeichnungen, Transkriptionen und Dokumente:

Sie sind Verantwortlicher, wir unterstützen Sie

Bei Betroffenenanfragen von Mitarbeitenden/Patienten/Mandanten/Dritten:

Unser Unterstützungsservice:

Technische Unterstützung bei:

- Identifikation betroffener Daten in Ihrem Account
- Export von Daten für Auskunftersuchen
- Technische Löschung oder Einschränkung
- Berichtigung in gespeicherten Dokumenten

Ihre Verantwortung als Auftraggeber:

Sie entscheiden über:

- Rechtmäßigkeit der ursprünglichen Datenerhebung
- Rechtsgrundlagen für die Verarbeitung (bes. Art. 9 DSGVO)

- Abwägung zwischen Betroffenenrechten und anderen Interessen
- Antwort an den Betroffenen

Verfahren bei Drittanfragen:

1. Betroffener wendet sich an Sie (als behandelnden Arzt/Anwalt/etc.)
2. Sie prüfen Berechtigung und rechtliche Zulässigkeit
3. Sie beauftragen uns mit technischen Maßnahmen
4. Wir setzen binnen 48h um (Werktage)
5. Sie antworten dem Betroffenen direkt

8.3 Verfahren und Fristen

Kontaktaufnahme:

E-Mail: datenschutz@latoo.at

Post: Latoo.labs GmbH, Datenschutz, Kraußstraße 16, A-4020 Linz

Unsere Bearbeitungsfristen:

- Standard: 1 Monat ab Antragseingang
- Komplexe Fälle: Verlängerung um 2 Monate (mit Begründung)
- Technische Unterstützung: 48 Stunden (Werktage)
- Eilfälle: Nach Absprache beschleunigt

Erforderliche Angaben:

Für eine effiziente Bearbeitung benötigen wir:

- Ihren vollständigen Namen und E-Mail-Adresse
- Konkrete Beschreibung Ihres Anliegens
- Bei Drittbetroffenen: Nachweis der Berechtigung
- Identitätsnachweis bei sensiblen Anfragen

Kostenfreiheit:

Grundsätzlich kostenfrei, Ausnahmen:

- Bei offensichtlich unbegründeten Anträgen
- Bei exzessiven Wiederholungen
- Kosten werden vorab mitgeteilt

8.4 Besondere Situationen

Bei Drittlandverarbeitung (US-Services):

Eingeschränkte Rechtsdurchsetzung möglich

- Löschung bei US-Anbietern nicht technisch verifizierbar
- Auskunft über US-Verarbeitung nur begrenzt möglich
- Lösung: Wechsel zu EU-Services empfohlen

Bei Löschung/Account-Schließung:

Vollständige Datenrückgabe möglich

- Export aller Ihrer Daten vor Löschung
- 30 Tage Karenzzeit für Datenrückgabe
- Danach unwiderrufliche Löschung

Bei Geschäftsgeheimnissen/Berufsgeheimnissen:

Besondere Sorgfalt bei:

- Patientendaten (ärztliche Schweigepflicht)
- Mandantendaten (anwaltliches Berufsgeheimnis)
- Verfahren: Verschlüsselte Kommunikation, gesonderte Prüfung

8.5 Beschwerdeweg

Falls Sie mit unserer Bearbeitung nicht zufrieden sind:

1. Direkter Kontakt: datenschutz@latoo.at
2. Eskalation: Geschäftsführung office@latoo.at
3. Aufsichtsbehörde: Österreichische Datenschutzbehörde (siehe Punkt 9)
4. Rechtlicher Weg: Zivilrechtliche Ansprüche vor österreichischen Gerichten

Wir bemühen uns stets um einvernehmliche Lösungen und schnelle, unbürokratische Hilfe.

9. Beschwerderecht bei der Aufsichtsbehörde

Sie haben das Recht, Beschwerde bei einer Datenschutzaufsichtsbehörde einzulegen. Die für uns zuständige Aufsichtsbehörde ist:

Österreichische Datenschutzbehörde, Barichgasse 40–42, 1030 Wien, Österreich.

Telefon: +43 1 52 152-0

E-Mail: dsb@dsb.gv.at Website: www.dsb.gv.at

10. Automatisierte Entscheidungsfindung und Profiling

Brainy nutzt KI-Technologien zur Verarbeitung von Sprache in Text und zur Generierung strukturierter Dokumente. Hierbei handelt es sich nicht um automatisierte Entscheidungen im Sinne des Art. 22 DSGVO, da keine rechtlichen Wirkungen oder ähnlich erhebliche Beeinträchtigungen für Sie entstehen.

11. Besonderheiten der KI-Nutzung

11.1 EU-gehostete KI-Modelle

Diese Modelle werden mit dem Zusatz "EU" gekennzeichnet und bieten ein höheres Datenschutzniveau, da die Verarbeitung innerhalb der EU erfolgt.

11.2 Nicht-EU-gehostete KI-Modelle

Die Nutzung nicht EU-gehosteter KI-Modelle ist optional und erfolgt nur auf Ihre dokumentierte Auswahl/Weisung in der App. Wir empfehlen, keine sensiblen personenbezogenen Daten über diese Modelle zu verarbeiten. Sie können jederzeit bei jeder Verarbeitungshandlung ein EU-gehostetes Modell auswählen. Darüber hinaus können Sie die zulässigen Modell-Kategorien für Ihre Organisation jederzeit mandantenweit einschränken (vgl. Ziff. 4.5).

11.3. EU AI Act (Verordnung (EU) 2024/1689)

Wir richten uns nach den Vorgaben des EU AI Act. Brainy ist in der Regel als KI-System mit begrenztem Risiko anzusehen. Je nach konkretem Einsatzbereich beim Kunden kann jedoch eine Einordnung als Hochrisiko-KI nach Anhang III der Verordnung in Betracht kommen (z.B. Personalwesen/Einstellung, Bildung/Eignungsprüfung, kritische Infrastrukturen).

Unsere Rolle (Anbieter/Provider):

Wir erfüllen die einschlägigen Anbieterpflichten (u.a. Transparenz, Dokumentation, Cybersicherheit) nach Maßgabe der anwendbaren Fristen.

Ihre Rolle (Nutzer/Betreiber):

Im Standardfall eines Systems mit begrenztem Risiko sind Sie als Betreiber insbesondere für die bestimmungsgemäße Nutzung des Systems gemäß der bereitgestellten Dokumentation sowie für die Sicherstellung einer ausreichenden KI-Kompetenz Ihrer Nutzer verantwortlich. Sollten Sie eine Nutzung als Hochrisiko-System beabsichtigen, gelten die weitergehenden gesetzlichen Betreiberpflichten.

Details:

Risikoklassifizierung, Pflichtenverteilung und Compliance-Maßnahmen sind in unserer AI Act Compliance Notice beschrieben, sowie in der AVV, soweit datenschutzrechtliche Aspekte betroffen sind.

Über wesentliche Änderungen oder neue Pflichten informieren wir innerhalb der Anwendung.

11.4 Agentic AI, Konnektoren und MCP-Server

Brainy bietet Agentic AI Funktionen, die es KI-Agenten ermöglichen, eigenständig Aufgaben auszuführen und über Konnektoren oder MCP-Server mit externen Systemen zu interagieren. Diese Funktionen sind optional und stehen nur in bestimmten Paketen zur Verfügung.

Konnektoren: Über Konnektoren kann Brainy sich im Ihrem Auftrag mit Drittdiensten verbinden (z. B. E-Mail, Dateispeicher, Kalender). Die technische Infrastruktur wird über Nango Inc. bereitgestellt. Sie entscheiden, welche Drittdienste verbunden werden und welche Zugriffsberechtigungen erteilt werden. Connector-Credentials werden verschlüsselt gespeichert.

MCP-Server: KI-Agenten können über MCP-Server auf Werkzeuge und Datenquellen zugreifen. Der Anbieter stellt eigene MCP-Server bereit (Anbieter-MCP-Server); Sie können zusätzlich eigene MCP-Server integrieren (Kunden-MCP-Server).

MCP-Tool-Steuerung (Default-Off): Alle Werkzeuge (Tools) eines MCP-Servers sind standardmäßig deaktiviert. Ein KI-Agent kann ein Tool erst nutzen, nachdem Sie oder ein autorisierter Administrator das Tool explizit aktiviert haben. Jede Aktivierung und Deaktivierung wird revisionssicher protokolliert. Diese Voreinstellung dient dem Schutz Ihrer Daten (Datenschutz durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 Abs. 2 DSGVO).

Transparenz: Für jedes MCP-Tool wird die vom MCP-Server bereitgestellte Beschreibung angezeigt. Bei Anbieter-MCP-Servern gewährleistet der Anbieter die Richtigkeit dieser Beschreibung. Bei Kunden-MCP-Servern stammt die Beschreibung vom externen Server und ist von Ihnen eigenständig zu verifizieren.

Protokollierung: Alle durch KI-Agenten ausgeführten Aktionen werden protokolliert und sind für Sie in der Anwendung einsehbar. Die Protokolle werden für mindestens 90 Tage aufbewahrt.

Weitere Details zu Ihren Pflichten bei der Nutzung von Agentic AI Funktionen finden Sie in unseren AGB (§ 6.8) sowie im Auftragsverarbeitungsvertrag (AVV).

12. Technische und organisatorische Sicherheitsmaßnahmen

Zum Schutz Ihrer personenbezogenen Daten haben wir umfangreiche technische und organisatorische Maßnahmen implementiert:

- Verschlüsselung bei Übertragung (TLS/SSL) und Speicherung
- Rollenbasiertes Berechtigungskonzept
- Regelmäßige Sicherheitsaudits und Penetrationstests
- Redundante Systeme und regelmäßige Backups
- Pseudonymisierung von Daten, wo technisch sinnvoll
- Dokumentierte Prozesse zur Behandlung von Datenschutzvorfällen

13. Änderungen dieser Datenschutzerklärung

Wir behalten uns vor, diese Datenschutzerklärung zu aktualisieren, um rechtlichen Anforderungen zu entsprechen oder Änderungen unserer Dienste abzubilden. Die aktuelle Version finden Sie in ihrem Benutzerprofil unter „Nutzungs- und Datenschutzbestimmungen“

Bei wesentlichen Änderungen werden wir Sie über die Anwendung oder per E-Mail informieren.

14. Fragen zum Datenschutz

Bei Fragen zum Datenschutz bei Brainy kontaktieren Sie uns bitte unter:

datenschutz@latoo.at

Latoo.labs GmbH

FN 565855s

Kraußstraße 16

4020 Linz

Österreich