Datenschutz-Mappe

Für Tippfaul · Stand: 27. November 2026 · ohne Konto, ohne Abo

Alles, was eine Praxis, eine Kanzlei oder ein Datenschutzbeauftragter vor einem Test wissen will: wer wer ist, wo eure Daten laufen, wie gelöscht wird und was für Berufsgeheimnis und Gesundheitsdaten gilt.

Auf einer halben Seite

Tippfaul schreibt, was ihr sagt. Dafür geht die Stimme auf einen kurzen Weg. Wer daran beteiligt ist:

Principium e.V.

Der Verein hinter Tippfaul, eingetragen beim Amtsgericht München (VR210441), Sitz in Krün. Er bietet die App an und ist für sie verantwortlich.

Adrian Schmidt

Verkauft die Business-Abos am Computer, unter dem Namen „Tippfaul“. Mit ihm schließt ihr den Vertrag zur Auftragsverarbeitung (AVV).

Hetzner

Ein deutsches Rechenzentrum in Nürnberg. Dort steht der Rechner, auf dem unser Server läuft. Unsere Software darauf nimmt die Aufnahme an und gibt sie weiter, ohne sie zu speichern.

Mistral AI

Eine französische Firma aus Paris. Ihre KI macht aus der Sprache Text und glättet ihn. Wir nutzen nur ihren Zugang für die EU, ohne Speicherung über das Ergebnis hinaus und ohne Training mit euren Daten.

Infomaniak

Ein Anbieter aus Genf in der Schweiz. Wer in der Schweiz verarbeiten lässt, dessen Diktate und Meetings laufen dort statt über Deutschland und Paris.

Was beim Meeting-Protokoll über den Server läuft

Etwa alle fünf Minuten geht ein Abschnitt der Aufnahme verschlüsselt an unseren Server und von dort an Mistral AI (oder Infomaniak, wenn ihr die Schweiz gewählt habt). Zurück kommt Text mit getrennten Sprechern. Am Ende geht dieser Text noch einmal durch, damit dort das Protokoll geschrieben wird. Unser Server speichert dabei weder Audio noch Text, nur welche Abschnitte abgerechnet sind.

Was nicht über den Server läuft und bei euch bleibt:

- Die Aufnahme liegt in Abschnitten auf eurem Gerät, bis der Text da ist. Dann löscht die App sie.
- Transkript, Protokoll und die Namen der Sprecher bleiben auf eurem Computer oder Handy, bis ihr sie löscht.
- Nur wenn ihr in Business das Protokoll an Teilnehmer schickt, geht es verschlüsselt über unseren Server: 30 Tage, ohne Transkript, den Schlüssel haben wir nicht.
- Nur wenn euer Team das Team-Archiv einschaltet, liegen Meetings verschlüsselt bei uns. Den Schlüssel haben nur eure Geräte.

Ehrlich dazu: Ohne Internet gibt es kein Diktat, denn die Spracherkennung läuft nicht auf dem Gerät. Tippen geht weiter.

Was in der Mappe steht

1. Der Vertrag zur Auftragsverarbeitung (AVV)
2. Unterauftragnehmer mit Standort, auch bei Mistral
3. Technische und organisatorische Maßnahmen (TOMs)
4. Logs, Abstürze und Training: unsere schriftliche Aussage
5. Wie gelöscht wird
6. Schweigepflicht (§ 203 StGB) und Gesundheitsdaten (Art. 9 DSGVO)
7. Was die Mappe nicht ist

1. Der Vertrag zur Auftragsverarbeitung (AVV)

Der AVV nach Art. 28 DSGVO steht öffentlich auf dieser Website. Ihr müsst nichts kaufen, um ihn zu lesen oder abzulegen. Er gilt ohne Unterschrift mit jedem Business-Abo, auch in der Testphase. Er regelt Daten, Weisungen, Schweigepflicht, Sicherheit, Unterauftragnehmer, Datenpannen innerhalb von 48 Stunden, Löschung und Kontrollen. Für die Haftung gilt Art. 82 DSGVO, ergänzend die Nutzungsbedingungen. Im PDF dieser Mappe liegt er hinten bei.

Gilt der AVV auch für Plus?

Nein. Der AVV gibt es nur mit Business, auch für eine Praxis oder Kanzlei mit nur einer Person. Plus ist das Abo für eine einzelne Person. Dort gilt die Datenschutzerklärung, und Principium e.V.ist selbst verantwortlich für die wenigen Kontodaten. Das Diktat läuft bei Plus technisch genauso wie bei Business: gleicher Weg, keine Speicherung von Audio und Text. Der Unterschied ist der Vertrag. Diktiert ihr Gesundheitsdaten oder Geheimnisse von Mandanten, braucht ihr den AVV und damit Business. Das Gratis-Konto hat ihn ebenfalls nicht.

2. Unterauftragnehmer mit Standort

Diese Dienste berühren eure Daten. Alle sind im AVV (Abschnitt 7) genannt:

Hetzner Online GmbH

Gunzenhausen, Deutschland

Aufgabe: Betrieb unseres Servers.

Wo verarbeitet wird: Rechenzentrum in Nürnberg, Deutschland.

Mistral AI SAS

Paris, Frankreich

Aufgabe: Spracherkennung, Glätten, Schreibaufträge, Protokolle und Sprecher-Erkennung; Diktate und Meetings, die ihr in der Schweiz verarbeiten lasst, gehen stattdessen an Infomaniak.

Wo verarbeitet wird: EU und Europäischer Wirtschaftsraum, keine Speicherung über das Ergebnis hinaus, kein Training.

Infomaniak Network SA

Rue Eugène Marziano 25, 1227 Les Acacias (Genf), Schweiz

Aufgabe: Betrieb unseres Servers in der Schweiz (dort auch die Sprecher-Erkennung von Meetings), Spracherkennung, Glätten, Schreibaufträge und Protokolle, wenn ihr in der Schweiz verarbeiten lasst.

Wo verarbeitet wird: Rechenzentren in der Schweiz (angemessenes Datenschutzniveau, Art. 45 DSGVO), keine Speicherung über das Ergebnis hinaus, kein Training.

Resend, Inc.

San Francisco, USA

Aufgabe: Versand von Anmeldecodes und Einladungen (E-Mail-Adresse, Code), Protokolle an die Teilnehmer eines Meetings (Adresse, Zeitpunkt, Link, kein Inhalt) und, wer es will, Hinweisen auf neue Aufnahmen im Team-Archiv ohne Inhalt.

Wo verarbeitet wird: Rechenzentrum in Irland (EU); EU-US Data Privacy Framework und Standardvertragsklauseln.

Functional Software, Inc. („Sentry“)

San Francisco, USA

Aufgabe: Fehler- und Absturzberichte von Server und Apps, ohne Audio und ohne Text.

Wo verarbeitet wird: EU-US Data Privacy Framework und Standardvertragsklauseln, Löschung nach spätestens 90 Tagen.

Cloudflare, Inc.

101 Townsend St., San Francisco, CA 94107, USA

Aufgabe: Aufbewahrung der nächtlichen Sicherungskopie unserer Datenbank, verschlüsselt mit einem Schlüssel, den nur wir haben.

Wo verarbeitet wird: Rechenzentren in der EU; EU-US Data Privacy Framework und Standardvertragsklauseln, Löschung nach 35 Tagen.

Wo Mistral selbst verarbeitet

Mistral: Mistral AI SAS, Paris, Frankreich (EU). Der Auftragsverarbeitungsvertrag von Mistral ist Teil seiner

Geschäftsbedingungen und gilt ohne Unterschrift.

Wir rufen Mistral nur über seinen EU-Zugang auf (`api.eu.mistral.ai`); nur dort sagt Mistral Rechenzentren in der EU und der EFTA zu. Mistral nennt für diese Verarbeitung:

- **Mistral Compute:** Frankreich
- **Microsoft Azure:** Schweden, Norwegen
- **Google Cloud:** Niederlande, Belgien (die USA nur beim US-Endpunkt, den wir nicht nutzen)
- **CoreWeave:** Europäischer Wirtschaftsraum

Gelesen auf Mistrals Liste am 24. November 2026. Mistral kann sie ändern; die aktuelle Liste steht auf trust.mistral.ai/subprocessors. Mit unserem Konto bei Mistral ist die Speicherung der Eingaben und Ergebnisse (Zero Data Retention) abgeschaltet, und Mistral trainiert nicht mit ihnen. Neue Unterauftragnehmer kündigen wir mindestens vier Wochen vorher per E-Mail an.

3. Technische und organisatorische Maßnahmen (TOMs)

Das tun wir für die Sicherheit nach Art. 32 DSGVO. Jede Zeile beschreibt, was auf unseren Servern und in den Apps wirklich eingerichtet ist. Der AVV (Abschnitt 6) nennt dieselben Punkte kürzer.

- **Übertragung:** Alles zwischen App, Website und Server läuft verschlüsselt (TLS, Zertifikat von Let’s Encrypt). Der Server schreibt kein Zugriffsprotokoll, in dem IP-Adressen stünden.
- **Server:** Hetzner Online GmbH, Rechenzentrum Nürnberg; für die Verarbeitung in der Schweiz Infomaniak Network SA, Rechenzentren in der Schweiz. Die Firewall lässt nur Web (80, 443) und Fernwartung (22) durch. Die Fernwartung geht nur mit Schlüssel, die Anmeldung mit

Passwort ist abgeschaltet. Sicherheitsupdates des Betriebssystems laufen automatisch.

- **Rechte der Software:** Unser Server läuft unter einem eigenen Benutzer ohne Anmelderecht, mit einem schreibgeschützten System; schreiben darf er nur in seinen Datenordner. Zugangsdaten zu Diensten liegen in einer Datei, die nur der Systemverwalter lesen kann, nie im Quelltext.
- **Keine Schlüssel in der App:** Die Apps tragen keinen Schlüssel eines KI-Anbieters. Sie sprechen nur mit unserem Server, mit einer anonymen Kennung, die im geschützten Speicher des Geräts liegt (Android Keystore, iOS Schlüsselbund).
- **Datensparsamkeit:** Aufnahmen und Texte werden nur während der Verarbeitung im Arbeitsspeicher gehalten und danach verworfen. Gespeichert werden nur Konto, Plan, gezählte Sekunden und, was ein Team selbst einträgt (Wörter, Textbausteine).
- **Anmeldung und Rollen:** Anmeldung mit Einmal-Code per E-Mail, mit Google oder mit Microsoft. Anmeldungen im Browser speichern wir nur als Prüfsumme. Im Team laden nur Inhaber und Verwaltung ein und entfernen Mitglieder; die Verwaltung sieht nur Minuten, nie Inhalte.
- **Team-Archiv und Protokolle:** Verschlüsselung auf euren Geräten mit AES-256-GCM. Den Schlüssel haben nur eure Geräte, wir nicht.
- **Missbrauchsschutz:** Anfragen werden je Gerät und je Adresse begrenzt. Die Adresse steht dafür nur im Arbeitsspeicher und wird nirgends gespeichert.
- **Sicherung:** Nächtliche Kopie der Datenbank (ohne Audio und Text): 14 Tage auf dem Server, außer Haus nur verschlüsselt, in einem Speicher in der EU mit Löschsperre, 35 Tage. Der Schlüssel liegt nicht auf dem Server.
- **Überwachung:** Alle 15 Minuten prüft eine zweite Stelle, ob Server, Website und Update-Feeds antworten. Der Server meldet selbst, wenn eine Sicherung alt wird, der Platz knapp wird oder der Sprachdienst ausfällt. Abstürze und Fehler gehen ohne Inhalte an Sentry.

- **Menschen:** Zugang zu den Systemen haben nur Personen, die zur Vertraulichkeit verpflichtet sind. Inhalte von Diktaten und Meetings sieht bei uns niemand an. Unterauftragnehmer sind vertraglich auf denselben Schutz verpflichtet.
- **Datenpannen:** Wir melden euch eine Verletzung des Schutzes unverzüglich, spätestens innerhalb von 48 Stunden (AVV Abschnitt 9).

4. Logs, Abstürze und Training: unsere schriftliche Aussage

- **Server-Logs:** Sie enthalten nur: Zeitpunkt, Art des Ereignisses, den Anfang der anonymen Kennung (nicht die ganze), Sekunden, Zahlen wie die Menge an Zeichen und Status. Nie Audio, nie Text, nie E-Mail-Adressen, keine IP-Adressen. Sie werden höchstens 30 Tage aufbewahrt.
- **Abstürze und Fehler:** Die Apps schicken nur Art des Fehlers, Programmzeilen, App- und Systemversion und die grobe Geräteklasse. Der Server übernimmt nur, was ein festes Schema erlaubt; Sätze, Adressen, Nummern und Schlüssel fliegen heraus. Der Server meldet seine eigenen Fehler ohne Kennung, ohne IP-Adresse und ohne Inhalte. Alles geht an Sentry (EU-Region), Löschung dort nach spätestens 90 Tagen.
- **Training:** Mit euren Daten wird nichts trainiert, weder von uns noch von Mistral. Es gibt einen Aufnahmemodus, mit dem wir das Diktat verbessern. Er ist für jedes Konto aus und lässt sich nur für ein Konto einschalten, dessen Inhaber ausdrücklich zugestimmt hat; in Kundenkonten ist er aus. Was er aufnimmt, liegt nur auf unserem Server, nicht in Logs, Sentry oder Sicherungen.
- **Speicherung bei Mistral:** Mit unserem Konto ist die Speicherung von Eingaben und Ergebnissen bei Mistral abgeschaltet (Zero Data Retention). Wir nutzen nur den EU-Zugang.

- **Löschung:** Wann was gelöscht wird, steht im nächsten Abschnitt. Auf Wunsch löschen wir alles auch per E-Mail.

5. Wie gelöscht wird

Aufnahmen und Texte	Werden bei uns nie gespeichert. Der Server verwirft sie nach der Verarbeitung, die App löscht die Aufnahme, sobald der Text da ist, und Mistral speichert nicht über das Ergebnis hinaus.
„Meine Daten löschen“ in der App	Sofort: die zufällige Kennung und die gezählten Sekunden aller Monate. Danach gilt die Kennung nicht mehr.
Kennung, die nie oder ein Jahr lang nicht benutzt wurde	Löscht der Server nach 365 Tagen von selbst, mit den Sekunden.
Konto löschen oder Team auflösen	Sofort. In den nächtlichen Sicherungen sind die Daten nach höchstens 35 Tagen weg.
Protokolle an Teilnehmer	30 Tage, dann gelöscht. Nach dem Löschen eures Kontos innerhalb von zehn Minuten.

Einträge im Team-Archiv	Löscht, wer sie angelegt hat; bei freigegebenen auch Inhaber und Verwaltung. Löst ihr das Team auf, räumt der Server sie kurz danach weg. Sicherungen: höchstens 35 Tage.
Anmeldecodes	Höchstens 15 Minuten.
Fehler- und Absturzberichte	Ohne Audio und ohne Text. Löschung bei Sentry nach spätestens 90 Tagen.

Auf Wunsch löschen wir alles auch auf eine E-Mail an hallo@tippfaul.app hin. Die Sicherungen: eine nächtliche Kopie der Datenbank, 14 Tage auf dem Server und verschlüsselt 35 Tage in der EU. Audio und Texte stehen nicht darin, weil wir sie nicht speichern.

6. Schweigepflicht und Gesundheitsdaten

Berufsgeheimnis nach § 203 StGB

Seid ihr Ärztin, Psychotherapeut, Apothekerin, Anwältin, Notar, Steuerberaterin, Wirtschaftsprüfer oder arbeitet ihr in einer Beratungsstelle, dürft ihr fremde Geheimnisse nur an Personen weitergeben, die an eurer Arbeit mitwirken (§ 203 Abs. 3 StGB). Der AVV (Abschnitt 5) macht uns dazu, auch als Vereinbarung nach § 43e BRAO und § 62a StBerG:

- Wir schweigen über alle fremden Geheimnisse, die wir erfahren, auch nach dem Ende des Vertrags.
- Uns ist bekannt, dass nach § 203 Abs. 4 StGB bestraft wird, wer als mitwirkende Person ein Geheimnis unbefugt offenbart oder weitere

Personen heranzieht, ohne sie zur Geheimhaltung zu verpflichten.

- Inhalte von Diktaten und Meetings sieht bei uns niemand an. Sie laufen automatisch durch.
- Wir ziehen nur Personen heran, die es für die Leistung braucht, und verpflichten jeden Unterauftragnehmer vertraglich auf denselben Schutz.
- Inhalte verarbeiten wir nur in Deutschland und der EU und, wenn ihr es wählt, in der Schweiz.

Für Österreich gilt dasselbe in einem Satz; für die Schweiz (Art. 321 StGB) steht der Zusatz in Abschnitt 13 des AVV.

Gesundheitsdaten nach Art. 9 DSGVO

In einem Diktat in der Praxis kommen Gesundheitsdaten vor, die besondere Kategorie nach Art. 9 DSGVO. Wir verarbeiten sie nur, um daraus Text zu machen, und speichern sie nicht. Die Rechtsgrundlage dafür, dass ihr sie diktiert, müsst ihr als Verantwortliche selbst haben, bei der Behandlung meist Art. 9 Abs. 2 lit. h DSGVO. Das entscheiden wir nicht für euch. Bei einer Datenschutz-Folgenabschätzung und bei Meldungen helfen wir (AVV, Abschnitt 8).

Tippfaul schreibt auf, was ihr sagt. Es ist kein Medizinprodukt, stellt keine Diagnose und schlägt keine Therapie vor. Prüft Dosierungen und Zahlen, bevor ihr einen Text ablegt.

7. Was die Mappe nicht ist

- Kein Prüfbericht und kein Zertifikat eines Dritten. Hier steht, was wir tun, und ihr könnt es mit dem AVV und der Datenschutzerklärung abgleichen.
- Keine Verarbeitung nur auf eurem Rechner. Das Diktat läuft über Server, wie oben beschrieben.

- Keine Rechtsberatung für euren Betrieb. Ob Tippfaul bei euch passt, entscheidet ihr oder euer Datenschutzbeauftragter.

Fragen und Wünsche für diese Mappe an hallo@tippfaul.app.

Vertrag zur Auftragsverarbeitung

Für Tippfaul Business · Stand: 14. Oktober 2026

Nutzt ihr Tippfaul Business, verarbeiten wir personenbezogene Daten in eurem Auftrag. Dieser Vertrag regelt das nach Art. 28 DSGVO. Er gilt mit dem Abschluss eines Business-Abos als vereinbart, auch während der Testphase, und läuft so lange wie das Abo. Zum Ablegen könnt ihr diese Seite als PDF speichern oder drucken, oder die Datenschutz-Mappe mit dem AVV als PDF laden.

1. Die Parteien

Verantwortlicher ist die Firma oder Person, die das Business-Abo abschließt („ihr“). Auftragsverarbeiter ist Adrian Schmidt, „Tippfaul“, Adalbert-Stifter-Straße 4, 82494 Krün („wir“), erreichbar unter hallo@tippfaul.app.

2. Gegenstand, Art und Zweck

Wir stellen euch Tippfaul bereit: Diktat am Computer, Aufnahme und Protokoll von Meetings, Konten und Team-Verwaltung, auf Wunsch ein Ende-zu-Ende verschlüsseltes Team-Archiv. Dafür machen wir aus Aufnahmen Text, zählen die genutzten Minuten, verwalten euer Team und rechnen ab. Andere Zwecke verfolgen wir mit euren Daten nicht.

3. Welche Daten, wessen Daten

- **Nur während der Verarbeitung, nie gespeichert:** Aufnahmen von Diktaten und Meetings, der daraus erzeugte Text, markierter Text für einen Schreibauftrag, die eigene Wortliste und die Art des Textfelds.

- **Gespeichert, solange das Konto besteht:** E-Mail-Adressen, Plan, Geräte-Kennungen und genutzte Sekunden pro Monat; im Team der Name des Teams, die Zahl der Plätze und zu jedem Mitglied E-Mail-Adresse, Rolle und ob die Einladung angenommen ist; Team-Wörter und Textbausteine, die eure Verwaltung einträgt; bei Meetings nur, welcher Abschnitt abgerechnet ist; Kunden- und Abo-Nummer bei Stripe.
- **Gespeichert, wenn ihr Protokolle an die Teilnehmer schickt:** das Protokoll eines Meetings (ohne Transkript), auf dem Computer verschlüsselt, 30 Tage lang. Den Schlüssel speichern wir nicht; er steht nur im Link der Mail. Zu jeder Empfängeradresse speichern wir eine Prüfsumme, die Adressen selbst nicht.
- **Gespeichert, wenn ihr das Team-Archiv einschaltet:** Meetings und, wer es will, Diktate (Transkript, Protokoll, Namen der Sprecher), Ende-zu-Ende verschlüsselt auf euren Geräten. Den Schlüssel haben nur eure Geräte und euer Wiederherstellungsschlüssel, wir nicht. Lesbar für uns sind nur Konto, Team, Art, Größe, Zeitpunkt und ob ein Eintrag fürs Team freigegeben ist.
- **Kurz gespeichert:** Anmeldecodes höchstens 15 Minuten, Anmeldungen im Browser als Prüfsumme bis zu ihrem Ablauf.

Betroffen sind eure Beschäftigten und alle, die ihr ins Team einladet, außerdem Menschen, deren Stimme in einem Diktat oder Meeting zu hören ist oder über die ihr diktiert, etwa Patientinnen und Mandanten, und die Teilnehmer, denen ihr ein Protokoll schickt.

In Diktaten und Meetings können auch besondere Kategorien personenbezogener Daten vorkommen (Art. 9 DSGVO), etwa Gesundheitsdaten in einer Praxis. Für sie gilt dasselbe wie für alle Inhalte oben: Wir verarbeiten sie nur, um daraus Text zu machen, und speichern sie nicht.

4. Weisungen

Wir verarbeiten die Daten nur nach euren Weisungen. Sie stehen in diesem Vertrag und in dem, was ihr in Tippfauleinstellt und auslöst. Weitere Weisungen gebt ihr per E-Mail. Halten wir eine Weisung für rechtswidrig, sagen wir euch das sofort. Müssen wir Daten aufgrund eines Gesetzes anders verarbeiten, sagen wir es euch vorher, soweit das Gesetz es erlaubt.

5. Vertraulichkeit und Berufsgeheimnis

Zugriff auf die Systeme haben nur Personen, die zur Vertraulichkeit verpflichtet sind. Auf Inhalte kann niemand zugreifen, weil wir Aufnahmen nicht speichern und Texte nur im Team-Archiv, Ende-zu-Ende verschlüsselt, ohne dass wir den Schlüssel haben. Protokolle an die Teilnehmer liegen bei uns nur verschlüsselt; den Schlüssel speichern wir nicht.

Seid ihr an ein Berufsgeheimnis gebunden, etwa nach § 203 StGB als Ärztin, Psychotherapeut, Apothekerin, Anwältin, Notar, Steuerberaterin, Wirtschaftsprüfer oder Beratungsstelle, gilt zusätzlich, auch als Vereinbarung nach § 43e BRAO, § 62a StBerG und den entsprechenden Regeln anderer Berufe:

- Wir wirken an eurer beruflichen Tätigkeit mit (§ 203 Abs. 3 StGB). Wir verpflichten uns, über alle fremden Geheimnisse zu schweigen, die wir dabei erfahren, auch nach dem Ende des Vertrags.
- Uns ist bekannt: Wer als mitwirkende Person ein fremdes Geheimnis unbefugt offenbart, wird nach § 203 Abs. 4 StGB mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer weitere Personen heranzieht, ohne dafür zu sorgen, dass sie zur Geheimhaltung verpflichtet sind.
- Von fremden Geheimnissen verschaffen wir uns nur Kenntnis, soweit es für unsere Leistung nötig ist. Inhalte von Diktaten und Meetings sieht

bei uns niemand an; sie laufen automatisch durch.

- Weitere Personen ziehen wir nur heran, soweit es für die Leistung nötig ist: wer bei uns Zugang zu den Systemen hat, und die Unterauftragsverarbeiter aus Abschnitt 7. Alle sind in Textform zur Verschwiegenheit verpflichtet; wer bei uns arbeitet, kennt die strafrechtlichen Folgen.
- Inhalte von Diktaten und Meetings verarbeiten wir nur in Deutschland und der EU und, wenn ihr es wählt, in der Schweiz.
- Dasselbe gilt, wenn ihr nach österreichischem Recht an eine Verschwiegenheitspflicht gebunden seid. Für die Schweiz steht das Berufsgeheimnis in Abschnitt 13.

6. Sicherheit

Wir schützen die Daten mit diesen technischen und organisatorischen Maßnahmen (Art. 32 DSGVO):

- Server in Deutschland und, für die Verarbeitung in der Schweiz, in der Schweiz, Übertragung nur verschlüsselt (TLS).
- Aufnahmen und Texte werden nach der Verarbeitung verworfen. Protokolle des Servers enthalten nur Ereignis, den Anfang einer Kennung, Sekunden und Status, nie Inhalte und keine Zugriffsprotokolle mit IP-Adressen.
- Zugang zum Server nur mit Schlüssel, Anmeldung mit Passwort abgeschaltet; eine Firewall lässt nur Web und Fernwartung durch; Zugangsdaten zu Diensten liegen nur in einer geschützten Datei auf dem Server.
- Anmeldung mit Einmal-Code per E-Mail, mit Google oder mit Microsoft; Anmeldungen im Browser speichern wir nur als Prüfsumme.
- Rollen im Team: Nur Inhaber und Verwaltung laden ein und entfernen Mitglieder. Die Verwaltung sieht pro Mitglied nur die Minuten des Monats, nie Inhalte.

- Team-Archiv: Verschlüsselung auf euren Geräten mit AES-256-GCM, gebunden an Team, Eintrag und Art; der Schlüssel verlässt ein Gerät nur verschlüsselt (Wiederherstellungsschlüssel, Kopplungscode für 10 Minuten). Zugriff nur für aktive Mitglieder, freigegebene Einträge fürs Team, alle anderen nur für die Person.
- Nächtliche Sicherung der Datenbank, außer Haus nur verschlüsselt; die Sicherungen werden nach spätestens 35 Tagen gelöscht.

Wir passen die Maßnahmen dem Stand der Technik an. Das Schutzniveau sinkt dabei nicht.

7. Unterauftragsverarbeiter

Ihr seid einverstanden, dass wir diese Dienste einsetzen:

- **Hetzner Online GmbH** (Gunzenhausen, Deutschland): Betrieb unseres Servers. Rechenzentrum in Nürnberg, Deutschland.
- **Mistral AI SAS** (Paris, Frankreich): Spracherkennung, Glätten, Schreibaufträge, Protokolle und Sprecher-Erkennung; Diktate und Meetings, die ihr in der Schweiz verarbeiten lasst, gehen stattdessen an Infomaniak. EU und Europäischer Wirtschaftsraum, keine Speicherung über das Ergebnis hinaus, kein Training.
- **Infomaniak Network SA** (Rue Eugène Marziano 25, 1227 Les Acacias (Genf), Schweiz): Betrieb unseres Servers in der Schweiz (dort auch die Sprecher-Erkennung von Meetings), Spracherkennung, Glätten, Schreibaufträge und Protokolle, wenn ihr in der Schweiz verarbeiten lasst. Rechenzentren in der Schweiz (angemessenes Datenschutzniveau, Art. 45 DSGVO), keine Speicherung über das Ergebnis hinaus, kein Training.
- **Resend, Inc.** (San Francisco, USA): Versand von Anmeldecodes und Einladungen (E-Mail-Adresse, Code), Protokolle an die Teilnehmer eines Meetings (Adresse, Zeitpunkt, Link, kein Inhalt) und, wer es will, Hinweisen auf neue Aufnahmen im Team-Archiv ohne Inhalt.

Rechenzentrum in Irland (EU); EU-US Data Privacy Framework und Standardvertragsklauseln.

- **Functional Software, Inc. („Sentry“)** (San Francisco, USA): Fehler- und Absturzberichte von Server und Apps, ohne Audio und ohne Text. EU-US Data Privacy Framework und Standardvertragsklauseln, Löschung nach spätestens 90 Tagen.
- **Cloudflare, Inc.** (101 Townsend St., San Francisco, CA 94107, USA): Aufbewahrung der nächtlichen Sicherungskopie unserer Datenbank, verschlüsselt mit einem Schlüssel, den nur wir haben. Rechenzentren in der EU; EU-US Data Privacy Framework und Standardvertragsklauseln, Löschung nach 35 Tagen.

Bezahlung über Stripe und Anmeldung mit Google oder Microsoft laufen bei diesen Diensten als eigene Verantwortliche, nicht in unserem Auftrag. Einen neuen Unterauftragsverarbeiter kündigen wir mindestens vier Wochen vorher per E-Mail an. Ihr könnt aus wichtigem datenschutzrechtlichem Grund widersprechen; finden wir keine Lösung, könnt ihr das Abo zum Wechsel kündigen. Wir verpflichten jeden Unterauftragsverarbeiter vertraglich auf denselben Schutz wie hier.

8. Unterstützung

Wir helfen euch, Anfragen von Betroffenen zu beantworten, etwa auf Auskunft oder Löschung. Vieles geht direkt inTippfaul: Mitglieder löschen ihr Konto selbst, die Verwaltung entfernt Mitglieder. Ebenso unterstützen wir euch bei Sicherheit, Meldungen von Datenpannen und Datenschutz-Folgenabschätzungen (Art. 32 bis 36 DSGVO).

9. Datenpannen

Erfahren wir von einer Verletzung des Schutzes eurer Daten, informieren wir euch unverzüglich, spätestens innerhalb von 48 Stunden, mit allem, was ihr für eine Meldung an die Aufsichtsbehörde braucht.

10. Ende des Vertrags

Endet das Abo, bleiben Konten und Team bestehen, bis ihr sie löscht: mit „Konto löschen“ oder indem der Inhaber das Team auflöst. Dann löschen wir die Daten sofort; in den Sicherungen sind sie nach höchstens 35 Tagen weg. Aufnahmen gibt es nicht zurückzugeben, weil wir sie nicht speichern; das Team-Archiv könnt ihr vorher im Browser lesen, kopieren und herunterladen. Auf Wunsch löschen wir alles auch auf eine E-Mail hin.

11. Nachweise und Kontrollen

Wir geben euch alle Informationen, die ihr braucht, um die Einhaltung dieses Vertrags nachzuweisen. Kontrollen vor Ort stimmen wir vorher ab; sie finden höchstens einmal im Jahr statt, außer es gibt einen konkreten Anlass.

12. Sonstiges

Für die Haftung gilt Art. 82 DSGVO, ergänzend gelten die Nutzungsbedingungen. Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes vor. Mehr zur Verarbeitung steht in der Datenschutzerklärung.

13. Zusatz für die Schweiz

Habt ihr euren Sitz in der Schweiz oder gilt für eure Daten das Schweizer Datenschutzgesetz (DSG), gilt zusätzlich:

- Dieser Vertrag ist auch der Vertrag über die Bearbeitung durch einen Auftragsbearbeiter nach Art. 9 DSG. Verweise auf die DSGVO gelten, soweit das DSG anwendbar ist, als Verweise auf die entsprechenden Regeln des DSG.

- Zuständige Aufsichtsbehörde ist insoweit der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB), Feldeggweg 1, 3003 Bern.
- Daten geben wir nur in Staaten bekannt, deren Datenschutz der Bundesrat als angemessen anerkannt hat (Anhang 1 der Datenschutzverordnung, darunter Deutschland und die anderen Staaten der EU und des EWR), oder mit Standardvertragsklauseln, die der EDÖB anerkannt hat (Art. 16 Abs. 2 lit. d DSG). Lasst ihr Diktate und Meetings in der Schweiz verarbeiten, verlassen deren Aufnahmen und Texte die Schweiz nicht; nur Protokolle, die ihr per Mail an Teilnehmer schickt, gehen verschlüsselt über unseren Server in Deutschland.
- Berufsgeheimnis: Wir und alle, die bei uns Zugang zu den Systemen haben, behandeln eure Daten vertraulich und sind dazu verpflichtet. Jeden Unterauftragsverarbeiter verpflichten wir vertraglich zur Vertraulichkeit. Seid ihr an ein Berufsgeheimnis gebunden, etwa nach Art. 321 StGB als Anwältin, Notar, Ärztin oder Revisor, oder an eine andere berufliche Schweigepflicht (Art. 62 DSG), etwa im Treuhandwesen, handeln wir als eure Hilfsperson und wahren dieses Geheimnis wie ihr. Aufnahmen speichern wir ohnehin nicht, Texte nur im Team-Archiv, Ende-zu-Ende verschlüsselt, ohne dass wir sie lesen können.
- Verletzungen der Datensicherheit melden wir euch unverzüglich, wie in Abschnitt 9 beschrieben, damit ihr eure Pflichten gegenüber dem EDÖB erfüllen könnt.