EUNAVIA · DATENSCHUTZ & VERTRAUEN

Wie wir deine Daten schützen.

Das Datenschutz- und Anonymitäts-Konzept hinter den Eunavia-Selbsthilfe- und Begleit-Apps — verständlich erklärt. Maximaler Schutz für die schützenswertesten Daten, die es gibt, ohne Verlust an Funktion und Bedienbarkeit.

Stand Juni 2026 · Selbsthilfe- und Begleit-Apps aus dem Bereich Lebensstil und Wohlbefinden — *kein Medizinprodukt, keine medizinische oder rechtsverbindliche Beratung.*

1 · Worum es geht

Unsere Apps begleiten Menschen in sehr persönlichen Momenten — beim Rauchstopp, beim Loslassen von Alkohol, in Fragen der eigenen Gesundheit und des Wohlbefindens. Das sind die schützenswertesten Daten, die es gibt. Darum ist Datenschutz bei Eunavia kein nachträgliches Feature, sondern das Fundament, auf dem alles steht.

Dieses Dokument fasst zusammen, wie wir diesen Schutz technisch umsetzen — in einfacher Sprache, damit du nachvollziehen kannst, warum du uns vertrauen kannst. Die zentrale Idee ist **Trennung**: Wer du bist und was du über deine Gesundheit einträgst, bewahren wir niemals gemeinsam auf.

> **Die zentrale Spannung — und ihre Auflösung.** „Anonym bleiben" und „sich identifizieren können" (z. B. um einen persönlichen Verlauf wiederherzustellen) widersprechen sich nur scheinbar. Die Lösung ist Trennung: Wer jemand ist, wird getrennt von dem verwahrt, *was* die Person über ihre Gesundheit einträgt. Beide Hälften sind nur über ein anonymes Kürzel verbunden, das allein nichts verrät.

2 · Die acht Leitprinzipien

Diese Grundsätze sind in der Technik unserer Produkte verbindlich verankert.

#	Prinzip	Was es bedeutet
1	**Datensparsamkeit**	Wir erheben nur, was eine sinnvolle Funktion wirklich braucht. Standort, Name & Co. bleiben optional.
2	**Anonym per Default**	Die App funktioniert vollständig ohne Konto. Kein Pflicht-Login, kein echter Name.
3	**Auf dem Gerät zuhause**	Deine Rohdaten bleiben verschlüsselt auf deinem Gerät. Eine Cloud ist optional, nicht die Quelle der Wahrheit.
4	**Identität ↔ Gesundheit getrennt**	Zwei getrennte Tresore, nur über ein anonymes Kürzel verbunden (Split-Identity).
5	**Eine Festung pro App**	Getrennte Datenwelten und Schlüssel je Produkt. Kein gemeinsames Profil über die Apps hinweg.
6	**Verschlüsselung überall**	Verschlüsselt auf dem Gerät, bei der Übertragung und — falls genutzt — in der Cloud.
7	**Du behältst die Kontrolle**	Export mit einem Tap, Löschen mit einem Tap — und Löschen heißt wirklich gelöscht.
8	**Kein Datenhandel, keine Tracker**	Null Werbe-Netzwerke, null fremde Analyse-Dienste. Wir verkaufen deine Daten nicht.

3 · Anonymität und Identifizierung — das Split-Identity-Modell

Menschen sollen anonym bleiben, sich bei Bedarf aber trotzdem wiedererkennen können — und alles soll einfach bleiben. Das gelingt durch zwei strikt getrennte Tresore, von denen keiner den Inhalt des anderen kennt.

Identitäts-Tresor — „Wer du bist"
Kennt, wenn überhaupt, nur einen anonymen Zugang (z. B. Fingerabdruck oder Gesichts-Entsperrung deines Geräts). Keine Gesundheitsdaten. Kein Name, keine E-Mail nötig.

Gesundheits-Tresor — „Was du einträgst"
Speichert deine Einträge, Fortschritte und Verläufe — aber ohne zu wissen, wer du bist. Kein Name, keine E-Mail, kein Gerät. Nur der Inhalt, von der Person gelöst.

`anonymes Kürzel` `— verbindet beide, verrät allein nichts`

Erst beide Hälften zusammen ergäben ein vollständiges Bild — und genau das verhindern wir, indem wir sie getrennt halten. Wer eine Hälfte in die Hände bekäme, hielte nur eine sinnlose Hälfte.

Wiederherstellung ohne E-Mail

Ein verlorenes Gerät darf weder Datenverlust noch eine E-Mail-Pflicht bedeuten. Beim Anlegen erzeugt die App einen persönlichen **Wiederherstellungs-Schlüssel** (z. B. eine merkbare Wortfolge). Damit lässt sich ein optionaler, Ende-zu-Ende verschlüsselter Cloud-Verlauf auf einem neuen Gerät zurückholen — ganz ohne E-Mail-Adresse, und ohne dass ein Server jemals den Klartext sieht.

4 · Eine Festung pro App

Jedes Produkt erhält eine ganz eigene, abgeschottete Datenwelt mit eigenen Schlüsseln. Das ist gelebte Sicherheit durch **Kompartimentierung** — und zugleich ein Datenschutzgewinn, weil ein App-übergreifendes Profil technisch gar nicht erst entstehen kann.

Ebene	Maßnahme	Wirkung
Hosting	Eigenes Projekt/Konto pro App, in der EU-Region	Ein Vorfall bei einer App betrifft keine andere.
Datenbank	Eigene Datenbank und Zugangsdaten pro App	Getrennte Speicher, keine geteilten Schlüssel.
Schlüssel	Eigener Hauptschlüssel pro App, eigener Datenschlüssel pro Person	Ein einzelner Schlüssel öffnet niemals alles.

> **Bewusst kein gemeinsames Nutzerkonto über alle Apps.** Ein zentraler „Eunavia-Account" wäre bequem — aber für Gesundheitsdaten genau das Falsche: Er schüfe einen einzigen Topf, dessen Leck alles offenlegt. Stattdessen bleibt jede App ihre eigene Festung.

5 · Verschlüsselung & „wirklich löschen"

Schutz auf jeder Stufe — und Löschen, das auch in Sicherungskopien wirkt.

Stufe	Schutz	Bewahrt vor
Auf dem Gerät	Starke Verschlüsselung, Schlüssel im sicheren Gerätespeicher	Verlorenes oder gestohlenes Gerät
Bei der Übertragung	Moderne Transportverschlüsselung	Mitlesen im Netz
In der Cloud (optional)	Ende-zu-Ende: der Server sieht nur unlesbaren Geheimtext	Server-Vorfälle, neugierige Betreiber

Löschen, das wirklich löscht

„Recht auf Löschung" wird oft schlecht umgesetzt, weil Daten in Backups überleben. Bei uns gilt: Statt Datensätze mühsam zu suchen, vernichten wir den persönlichen Schlüssel. Ohne ihn wird der gesamte Bestand dieser Person — auch in jeder Sicherungskopie — unwiederbringlich unlesbar. Ein Tap, sofort wirksam.

6 · Notfall ohne Funktionsverlust

Datenschutz darf die Funktion nicht ausbremsen — und es braucht eine schnelle Notfallfunktion. Beides ist kein Widerspruch: Ein lokaler Notfallpfad ist sowohl schneller *als auch* datensparsamer.

- ✓ Die Soforthilfe in kritischen Momenten läuft komplett **offline und ohne Konto**.
- ✓ Wichtige Krisenressourcen (z. B. Notruf- und Hilfsnummern) liegen fest in der App — kein Online-Abruf nötig.
- ✓ Eine optionale Vertrauensperson wird nur lokal hinterlegt; Auslösen ruft direkt an, ohne Umweg über einen Server.
- ✓ Bei Warnzeichen verweist die App freundlich, aber konsequent auf menschliche und ärztliche Hilfe — statt selbst zu „therapieren".

> **Kernaussage.** Weil die wirksamsten Funktionen ohnehin auf dem Gerät laufen, ist die datenschutzfreundliche Architektur zugleich die schnellste und robusteste. Dein Vorteil und der Datenschutz zeigen in dieselbe Richtung.

7 · Was wir niemals tun

- × Deine Daten verkaufen oder an Dritte weitergeben.
- × Werbe- oder Tracking-Dienste in unsere Apps einbauen.
- × Ein gemeinsames Profil über alle Apps hinweg anlegen.
- × Dich zu einer E-Mail-Adresse oder einem Login zwingen.
- × Lebenswichtige Hilfe von einer Internetverbindung abhängig machen.

8 · Nachprüfbar — freiwillige Prüfung

Wir möchten nicht nur sagen, dass deine Daten sicher sind — wir legen unsere Schutz-Architektur offen und setzen auf freiwillige, unabhängige Prüfungen. Pflicht-Zertifizierungen für Medizinprodukte braucht unser nicht-medizinischer Selbsthilfe-Ansatz dafür nicht.

Baustein	Was es belegt
DSGVO-Konformität	Datenschutz-Folgenabschätzung, Verarbeitungsverzeichnis und granulare, jederzeit widerrufbare Einwilligungen — die rechtliche Grundlage für sensible Daten.
Unabhängiger Sicherheits-Test	Penetrationstest auf Basis des OWASP-MASVS — von einer spezialisierten IT-Security-Firma geprüft, nicht nur selbst behauptet.
Freiwilliges Datenschutz-Siegel	Optionales TÜV-/ePrivacy-Siegel für sensible Apps als Vertrauensanker — ohne Pflicht; der Schutz steht auch ohne Siegel.

Eunavia ist noch in der Prototyp-Phase und nicht am Markt — diese freiwilligen Prüfungen sind deshalb noch nicht erfolgt. Wir bauen Datenschutz von der ersten Codezeile an ein und gehen sie Schritt für Schritt an, sobald wir starten — zuerst dort, wo die Daten am sensibelsten sind.

9 · Glossar

Begriff	Bedeutung
Split-Identity	Trennung von „Wer du bist" und „Was du einträgst" in zwei Tresore, verbunden nur durch ein anonymes Kürzel.
Ende-zu-Ende	Verschlüsselung, bei der nur deine Geräte lesen können — der Server speichert ausschließlich unlesbaren Geheimtext.
Crypto-Shredding	Löschen durch Vernichten des Schlüssels — die Daten werden unwiederbringlich unlesbar, auch in Backups.
Passkey	Gerätegebundene, phishing-resistente Anmeldung ohne Passwort und ohne E-Mail (z. B. per Fingerabdruck).
Kompartimentierung	Strikte Trennung in abgeschottete Bereiche, damit ein Vorfall nie alles auf einmal betrifft.