Datenschutzerklärung für die App „Forma“

Version 1 – 13.10.2025

Verantwortlicher

- Andre Zimpel (Freiberufler)
- Anschrift: Henriettenstraße 65, 09112 Chemnitz, Deutschland
- E-Mail: hello@useforma.io
- Domain: useforma.io
- Datenschutzbeauftragter: nicht benannt (nicht erforderlich)

Geltungsbereich und Rollen

- Diese Erklärung gilt für die Nutzung der Forma-Plattform (App) und der Marketing-Website.
- Für Plattform-/Kontodaten handeln wir als Verantwortlicher.
- Für Patienten- und Buchungsdaten von Praxen handeln wir als Auftragsverarbeiter; die jeweilige Praxis bleibt Verantwortliche und bestimmt Zwecke/Mittel der Verarbeitung.

Kategorien personenbezogener Daten

- Konten/Organisation/Mitglieder: Name, E-Mail, Rollen, Organisationsdaten (Name, Logo, Kontakt, Adresse, Zeitzonen-Metadaten).
- Sitzungs-/Nutzungsdaten: Session-Token, Laufzeiten, IP-Adresse, User-Agent, Rate-Limit-Metadaten.
- Services/Buchungen: Terminzeiten, Service, Preis/Währung, Status, Puffer/Segmente, Reschedule-Infos.
- Patienten (im Auftrag der Praxis): Identität, Kontakt/Adresse, Buchungskontext; optional Versicherungsstatus/medizinische Angaben; interne Praxisnotizen.
- Kommunikation: OTP-E-Mails, Buchungsbestätigungen/-stornos, ICS-Kalenderdateien (freiwillige Freitext-Nachrichten werden nicht per E-Mail/ICS versendet).
- Produktfeedback/Support: Nachricht, Kategorie, Impact, PagePath, User-Agent.
- Analytics: App-Nutzungsdaten (PostHog – EU), Marketing-Website (Plausible – EU, geplant).

Zwecke der Verarbeitung

- Betrieb und Bereitstellung der Plattform (Auth, Organisation/Mitglieder/Services).
- Termin- und Patientenverwaltung für Praxen (im Auftrag).
- Sicherheit, Stabilität, Missbrauchsvermeidung (Rate-Limiting, Protokollierung technischer Metadaten).
- Produktverbesserung (Feedback, App-Analytics).
- Reichweitenmessung der Marketing-Website (Plausible, geplant).

Rechtsgrundlagen

- Art. 6 Abs. 1 lit. b DSGVO (Vertrag/Anbahnung): Konten, Plattformbetrieb, Buchungsvorgänge.
- Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse): Sicherheit, Stabilität, Produktverbesserung.
- Art. 6 Abs. 1 lit. a DSGVO (Einwilligung): nicht erforderliche Analytics/Komfortfunktionen, sofern eingesetzt.
- Art. 9 DSGVO (besondere Kategorien) bei Patientendaten: Verarbeitung durch die Praxis als Verantwortliche; wir verarbeiten nur weisungsgebunden (regelmäßig Art. 9 Abs. 2 lit. h i. V. m. § 22 BDSG).

Empfänger/Auftragsverarbeiter (Subprozessoren)

Wir geben keine Daten an unabhängige Dritte zu eigenen Zwecken weiter. Zur Leistungserbringung setzen wir Auftragsverarbeiter ein und schließen AV-Verträge; Übermittlungen in Drittländer werden durch geeignete Garantien (insb. EU-SCC) abgesichert.

- Vercel (Hosting/CDN/Serverless)
    - Unternehmen: Vercel Inc., USA; Zweck: App-Hosting, Edge/CDN
    - Region: primär EU-Betrieb möglich; CDN mit globalen PoPs
    - Rechtsinstrumente: AVV; bei Drittlandübermittlungen EU-SCC + zusätzliche Maßnahmen
- Neon (Datenbank)
    - Unternehmen: Neon, Inc., USA; Zweck: Managed PostgreSQL
    - Region: EU (Frankfurt)
    - Rechtsinstrumente: AVV; EU-SCC für etwaige Zugriffe aus Drittländern; Verschlüsselung in Transit/at Rest
- maxcluster (E-Mail, aktuell)
    - Unternehmen: maxcluster GmbH, Deutschland; Zweck: SMTP-Versand
    - Region: EU (Deutschland)
    - Rechtsinstrumente: AVV; keine Drittlandübermittlung
- Resend (E-Mail, Umzug geplant)
    - Unternehmen: Resend, Inc., USA; Zweck: transaktionale E-Mails
    - Region: EU (Irland) konfiguriert
    - Rechtsinstrumente: AVV; bei etwaigen Drittlandübermittlungen EU-SCC + Maßnahmen
- PostHog (App-Analytics)
    - Unternehmen: PostHog, Inc. (USA) / PostHog Limited (UK)
    - Region: EU-Cloud konfiguriert
    - Rechtsinstrumente: AVV; bei Drittlandübermittlungen EU-SCC; UK verfügt über EU-Angemessenheitsbeschluss
- Plausible (Marketing-Website-Analytics, geplant)

    - Unternehmen: Plausible Insights OÜ, Estland
    - Region: EU-Hosting
    - Rechtsinstrumente: AVV; keine Drittlandübermittlung erforderlich

- Wasabi (Objektspeicher, geplant)

    - Unternehmen: Wasabi Technologies, LLC, USA
    - Region: EU-central-2 (Frankfurt) geplant
    - Rechtsinstrumente: AVV; bei Drittlandbezug EU-SCC; Verschlüsselung in Transit/at Rest

Aktuelle Konfiguration: PostHog EU-Region, Resend EU (Irland), Neon EU (Frankfurt), Wasabi EU (Frankfurt, noch nicht aktiv). Änderungen an Subprozessoren/Regionen werden in aktualisierten Fassungen dieser Erklärung ausgewiesen.

Drittlandübermittlungen

- Personenbezogene Daten werden überwiegend innerhalb der EU/des EWR verarbeitet.
- Durch global verteilte CDN-/Edge-Infrastrukturen (z. B. Vercel) können technische Übermittlungen in Drittländer erfolgen; hierfür nutzen wir EU-Standardvertragsklauseln und zusätzliche Schutzmaßnahmen (TLS, Verschlüsselung at rest, Zugriffsminimierung).

Cookies und ähnliche Technologien

- Erforderlich (App): Auth/Session-Cookies für sichere Anmeldung und Betrieb (keine Einwilligung erforderlich).
- App-Analytics (PostHog): EU-Region, datensparsam; je nach Konfiguration ggf. einwilligungsbedürftig.
- Marketing-Website (Plausible, geplant): datenschutzfreundliche, in der Regel cookie-lose Reichweitenmessung.
- Nicht erforderliche Funktionen (sofern aktiviert) kannst du ablehnen; die Kernfunktionen der App bleiben nutzbar.

E-Mail/ICS

Wir versenden OTP-E-Mails sowie Buchungsbestätigungen/-stornos mit ICS-Kalenderdateien. Inhalte werden minimiert (keine Diagnosen/medizinischen Details; keine freien Nachrichteninhalte). Bestätigungen enthalten typischerweise: Name, Service, Therapeut:in, Datum/Uhrzeit, Ort, ggf. Preis.

Speicherdauern

- Sessions: 7 Tage.
- Konten/Organisations-/Betriebsdaten: bis zur Löschung/Beendigung des Vertragsverhältnisses bzw. solange gesetzliche Pflichten entgegenstehen.
- App-Logs/Rate-Limit-Daten: für technisch erforderliche Zeiträume.
- Patienten-/Buchungsdaten (Praxisverantwortung): Speicherung nach Weisung/Fristen der Praxis; Löschung auf Weisung oder nach Vertragsende.

Sicherheit der Verarbeitung (TOMs – Kurzüberblick)

- Transportverschlüsselung (TLS) für App/APIs; Provider-seitige Verschlüsselung at rest (DB/Storage), wo verfügbar.
- Rollen-/Berechtigungskonzept (RBAC), Least-Privilege, restriktive Secret-/Schlüsselverwaltung, MFA für Adminzugänge empfohlen.
- Backup/Restore (z. B. DB-Snapshots), Monitoring/Alarmierung, grundlegende Audit-Logs.
- Härtung/Patching, regelmäßige Abhängigkeits-Updates, defensives Fehler-/Log-Handling (keine PHI in Logs).
- Datenminimierung in E-Mails/ICS; kein Versand sensibler Gesundheitsdetails.

Betroffenenrechte (DSAR)

Du hast Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch sowie Widerruf von Einwilligungen.

- Anfragen zu Plattform-/Kontodaten: hello@useforma.io.
- Anfragen zu Praxis-/Patientendaten: direkt an die jeweilige Praxis (diese ist Verantwortliche).
  Wir beantworten Anfragen in der Regel innerhalb eines Monats (Art. 12 Abs. 3 DSGVO).

Widerspruchsrecht (Art. 21 DSGVO)

Soweit wir Daten auf Grundlage berechtigter Interessen verarbeiten, kannst du aus Gründen, die sich aus deiner besonderen Situation ergeben, Widerspruch einlegen.

Automatisierte Entscheidungen/Profiling

Finden nicht statt.

Kinder

Die App richtet sich nicht gezielt an Minderjährige; Buchungen erfolgen durch oder im Auftrag Sorgeberechtigter über die Praxis.

Änderungen

Wir aktualisieren diese Erklärung bei Bedarf. Gültig ist die jeweils veröffentlichte Version (Version 1 – 13.10.2025).

Aufsichtsbehörde/Beschwerderecht

Du hast das Recht, dich bei einer Datenschutzaufsichtsbehörde zu beschweren. Zuständig am Sitz des Verantwortlichen ist die Landesbeauftragte/der Landesbeauftragte für den Datenschutz des Freistaates Sachsen.

Kontakt

- Verantwortlicher: Andre Zimpel, Henriettenstraße 65, 09112 Chemnitz, Deutschland
- E-Mail: hello@useforma.io

Soll ich dir zusätzlich eine kurze HTML-Version generieren (für `app/(marketing)/privacy/page.tsx`) und eine PDF-freundliche Markdown-Datei, die du in `public/legal/privacy-v1-de.pdf` rendern kannst?