

Compliance-Übersicht

Datenhaltung, Verschlüsselung, Zugriffsschutz und Auftragsbearbeitung bei Formsly, zusammengestellt für Datenschutz-, IT- und Beschaffungsstellen. Alle Angaben sind in der referenzierten Compliance-Dokumentation (Abschnitt 06) hinterlegt.

 **Zürich**

Sämtliche Systeme und Backups werden bei Exoscale in Zürich (eu-central-2) betrieben. Die Daten verbleiben in der Schweiz.

AES-256-GCM

Formularantworten werden auf Applikationsebene verschlüsselt gespeichert. Optional ist Ende-zu-Ende-Verschlüsselung verfügbar.

DSG-konform

AVV, ToMs, DSFA und Löschkonzept sind dokumentiert und unter Abschnitt 06 referenziert.

Mandantentrennung

Row-Level Security ist auf allen Datenbanktabellen aktiv und trennt die Daten der Kunden auf Datenbankebene.

DATENHALTUNG & HOSTING01

- Infrastruktur:** Applikation, Datenbank, Datei-Storage und verschlüsselte Backups werden vollständig bei Exoscale in Zürich (eu-central-2) betrieben. Die Infrastruktur ist nach ISO 27001, 27017 und 27018 zertifiziert.
- Eigenbetrieb:** Datenbank (PostgreSQL), Authentifizierung und Storage werden auf eigenen Servern betrieben. Die Datenverarbeitung erfolgt ausschliesslich auf der Exoscale-Infrastruktur.
- Nicht eingesetzte Dienste:** Für Formular- und Kundendaten werden keine US-Cloud-Infrastruktur, kein Cloudflare und keine CDN-Spiegelung ausserhalb der Schweiz verwendet.

VERSCHLÜSSELUNG02

- Übertragung:** Alle Verbindungen sind TLS-verschlüsselt.
- Speicherung:** Formularantworten werden auf Applikationsebene mit **AES-256-GCM** verschlüsselt gespeichert.
- Ende-zu-Ende-Verschlüsselung (optional):** In den Plänen Professional und Business werden Antworten bereits im Browser mit **ECIES P-256 + AES-256-GCM** verschlüsselt. Die privaten Schlüssel verbleiben beim Kunden; eine Entschlüsselung durch Formsly ist technisch nicht möglich.

ZUGRIFF & AUTHENTIFIZIERUNG03

- Authentifizierung:** Zwei-Faktor-Authentifizierung (TOTP) und Passkeys (WebAuthn) werden unterstützt. Für geschützte Bereiche ist die zweite Stufe technisch erzwungen (AAL2).
- Mandantentrennung:** Row-Level Security (PostgreSQL) ist auf allen Tabellen aktiv und wirkt auch bei direktem Datenbankzugriff.
- Spam-Schutz:** Öffentliche Formulare verwenden ALTCHA (Proof-of-Work). Tracking-Dienste von Drittanbietern kommen nicht zum Einsatz.

AUFBEWAHRUNG & LÖSCHUNG04

- Formularantworten:** Die Löschfristen sind pro Formular konfigurierbar. Die Löschung erfolgt automatisiert gemäss dokumentiertem Lösch- und Aufbewahrungskonzept.
- Kontodaten:** Die Löschung erfolgt 30 Tage nach Kontoschliessung. Auskunft- und Löschbegehren werden innert 30 Tagen umgesetzt.
- Besonders schützenswerte Personendaten:** Deren Verarbeitung ist gemäss AGB ausgeschlossen (Art. 5 lit. c DSG).

AUFTRAGSBEARBEITER & DATENTRANSFERS05

ANBIETER	ZWECK	STANDORT
Exoscale	Hosting, Storage, Backups	Zürich, CH
Infomaniak	Transaktions-E-Mails	Genf, CH
Stripe	Nur Abrechnungsdaten, keine Formulardaten	USA · SCC + DPA
Google, Zapier	Optionale Integrationen. Die Aktivierung erfolgt nur durch den Kunden (Opt-in); bei E2EE technisch nicht verfügbar	USA · SCC, Opt-in

DOKUMENTE & NACHWEISE06

Auftragsbearbeitungsvertrag (AVV)

formsly.ch/avv

Technische & organisatorische Massnahmen

formsly.ch/toms

Sicherheitsarchitektur (Whitepaper)

formsly.ch/sicherheit

DSFA, Verarbeitungsverzeichnis, Incident-Response-Plan

[auf Anfrage \(NDA\)](#)