Technische und organisatorische Massnahmen (Anhang 2, TOM)

Stand: 8. November 2026 · Version 2026-11-06

Vertragspartnerin und Rechnungsstellerin ist die Betreiberin (noowy, Patrice Gobat & Nicolas Affolter (einfache Gesellschaft)); Wichtli ist eine Marke von ihr.

- Datensparsamkeit: nur die nötigen Felder; Voreinstellungen privat.
- Transportverschlüsselung (TLS) für alle Verbindungen; HSTS.
- Speicherung in Cloudflare D1 mit EU-Jurisdiktion.
- Wohnadressen: AES-256-GCM-Verschlüsselung pro Datensatz mit firmenspezifisch abgeleitetem Schlüssel; Schlüssel nur als Worker-Secret, nie im Code.
- Kein Endpunkt liest Adressen aus; entschlüsselt wird nur im Versandexport, jede Entschlüsselung wird protokolliert (wer, wann, ohne Adresse).
- HR und Admins sehen nie, wer wen gezogen hat, keine Fragebogen-Antworten und keine Nachrichten.
- Rollenbasierter Zugriff; Zwei-Faktor-Authentisierung für den Betreiber-Zugang; Anmeldung per Einmal-Link.
- Logs ohne Inhalte und ohne Adressen; Aufbewahrung 30 Tage.
- E-Mails enthalten nie Paare, Namen des Wichtelkinds oder Wichtels und standardmässig keinen Nachrichtentext. Absenderdomain mit SPF, DKIM und DMARC.
- Automatische Löschung nach Ziffer 11; Backups verfallen nach höchstens 30 Tagen.
- Vorfallprozess: eindämmen, bewerten, protokollieren; Protokoll der Verletzungen 2 Jahre.