

RECHTLICHES

Security & Trust

Version 1.0 · gültig ab 01.10.2026 · xgait.com/security/v1.0

Die vertraglich zugesagten Massnahmen stehen als Anlage 1 im [AVV](#).

Jeder Kunde bekommt eine eigene Instanz — eigene Maschine, eigene Datenbank, eigene Schlüssel. Es gibt keine gemeinsame Kundendatenbank, aus der ein Filterfehler fremde Daten sichtbar machen könnte. Eine verschlüsselte Kopie jedes Hauptschlüssels liegt für die Wiederherstellung in unserem Verwaltungssystem.

Bereich	Umsetzung
Identität und Zugriff	Rollen und Rechte serverseitig durchgesetzt; personengebundene Konten; Passwörter ausschliesslich als script-Hash; gedrosselte Anmeldewege
Sitzungen	Cookies HttpOnly, SameSite=Lax, Secure mit __Host-Präfix; Herkunftsprüfung schreibender Anfragen
Administrativer Zugang	nur per SSH-Schlüssel; Datenbank nicht öffentlich erreichbar
Verschlüsselung	TLS für alle Verbindungen; hinterlegte Zugangsdaten mit AES-256-GCM verschlüsselt
Datensicherung	täglich, verschlüsselt vor dem Verlassen des Servers, getrennter Speicher, 7 Tage plus 4 Wochen
Missbrauchsschutz	Durchsatzgrenzen je Aufrufer; Begrenzung der Anfragegrösse; Schutz gegen Credential Stuffing
Uploads	Grössenbegrenzung, bereinigter MIME-Typ, keine Ausführung auf dem Server
Protokollierung	Änderungsprotokoll je Datensatz; Anmeldeereignisse; Logs liegen auf der Instanz, unser Verwaltungssystem ruft nur allgemeine Betriebskennzahlen ab

Bereich	Umsetzung
Entwicklung	Review vor dem Zusammenführen; Bewertung von Abhängigkeiten; getrennte Umgebungen; keine Kundendaten in Tests
KI-Assistenten	bei Managed-Leistungen nur geschäftliche Konten ohne Training; die dafür angelegten Zugänge werden nach der Aufgabe widerrufen

Zertifizierungen: XGait ist derzeit nicht nach ISO 27001 oder SOC 2 zertifiziert. Wir nennen hier nur Nachweise, die tatsächlich bestehen.

Sicherheitsmeldungen an service@xgait.com. Tests gegen produktive Systeme nur mit vorheriger schriftlicher Freigabe.