

RECHTLICHES

Auftragsverarbeitungsvertrag (AVV)

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

zwischen dem Kunden (Verantwortlicher, „Kunde“) und der Baldux GmbH, Erlistrasse 6, 6403 Küssnacht am Rigi, Schweiz (Auftragsverarbeiter, „Baldux“).

Der AVV wird mit Annahme der AGB in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO).

1. Gegenstand, Dauer, Rang

1.1 Baldux bearbeitet personenbezogene Daten im Auftrag des Kunden, um XGait bereitzustellen: Hosting, Speicherung, Datensicherung, Ausführung der Plattformfunktionen, API, Konnektoren, Wartung und, wenn beauftragt, Support und Managed-Leistungen.

1.2 Der AVV gilt, solange Baldux solche Daten bearbeitet, einschliesslich der Export- und Löschfristen nach Vertragsende.

1.3 Bei Widersprüchen geht dieser AVV den AGB in Fragen des Datenschutzes vor. Im Übrigen gelten die AGB.

2. Art und Zweck, Daten, betroffene Personen

2.1 Art und Zweck: Bereitstellung einer konfigurierbaren Geschäftsplattform (Warenwirtschaft, Aufträge, Rechnungen und vom Kunden definierte Prozesse).

2.2 Datenkategorien und betroffene Personen bestimmt der Kunde durch seine Nutzung. Typisch sind Stamm-, Kontakt-, Vertrags-, Bestell-, Rechnungs- und Kommunikationsdaten sowie Nutzungs- und Protokolldaten von Kunden, Lieferanten, Interessenten, Beschäftigten und Nutzern des Kunden.

2.3 Besonders schützenswerte Personendaten (Art. 5 lit. c DSGVO) und besondere Kategorien (Art. 9 DSGVO) verarbeitet der Kunde nur nach gesonderter schriftlicher Vereinbarung.

3. Verantwortung und Weisungen

3.1 Der Kunde ist für die Rechtmässigkeit der Bearbeitung, die Information der betroffenen Personen und die Wahrung ihrer Rechte allein verantwortlich.

3.2 Baldux bearbeitet die Daten nur auf dokumentierte Weisung des Kunden. Weisungen sind die AGB, dieser AVV, die Konfiguration und Nutzung von XGait einschliesslich aller Handlungen über API-Token des Kunden, sowie Anweisungen im Support in Textform oder in einer Zoom-Sitzung.

3.3 Hält Baldux eine Weisung für rechtswidrig, informiert Baldux den Kunden und darf die Ausführung bis zur Klärung aussetzen. Baldux ist nicht verpflichtet, Weisungen rechtlich zu prüfen.

3.4 Muss Baldux Daten aufgrund gesetzlicher Pflicht anders bearbeiten, informiert Baldux den Kunden vorher, soweit das Gesetz dies nicht verbietet.

4. Vertraulichkeit und Sicherheit

4.1 Baldux verpflichtet alle Personen mit Zugriff auf die Daten schriftlich zur Vertraulichkeit.

4.2 Baldux trifft die technischen und organisatorischen Massnahmen nach Anlage 1 (Art. 32 DSGVO, Art. 8 DSG und Art. 1 bis 5 DSV). Baldux darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt.

4.3 Der Kunde ist für die Sicherheit in seinem Verantwortungsbereich zuständig: Benutzerkonten, Rechte, Passwörter, API-Token, die Nutzung angebotener Sicherheitsfunktionen, Endgeräte und die von ihm eingesetzten KI-Assistenten und Drittdienste.

5. KI-Assistenten

5.1 **Bedient der Kunde einen KI-Assistenten mit eigenem Konto**, ist dessen Anbieter ein Dienstleister des Kunden, nicht von Baldux. Der Kunde schliesst mit ihm die nötigen Verträge und verantwortet die Übermittlung.

5.2 **Bedient Baldux einen KI-Assistenten im Auftrag des Kunden**, ist dessen Anbieter ein Unterauftragsverarbeiter von Baldux nach Ziffer 7. Baldux nutzt dafür ausschliesslich

geschäftliche Konten mit Datenschutzvereinbarung, bei denen der Anbieter die Daten nicht zum Training verwendet, und übermittelt nur, was für die Aufgabe nötig ist.

6. Unterstützung des Kunden

6.1 Baldux unterstützt den Kunden mit angemessenen technischen und organisatorischen Mitteln bei Anfragen betroffener Personen, bei der Datensicherheit, bei Meldungen von Verletzungen, bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 32 bis 36 DSGVO, Art. 22 bis 24 DSG).

6.2 Anfragen betroffener Personen leitet Baldux an den Kunden weiter und beantwortet sie nicht selbst.

6.3 Unterstützung, die über die Standardfunktionen der Plattform hinausgeht und nicht durch einen Verstoß von Baldux veranlasst ist, wird mit CHF 299 bzw. EUR 299 pro Stunde abgerechnet.

7. Unterauftragsverarbeiter

7.1 Der Kunde genehmigt allgemein den Einsatz von Unterauftragsverarbeitern. Die bei Vertragsschluss eingesetzten stehen in der Liste unter [/unterauftragsbearbeiter](#) (Anlage 2).

7.2 Baldux informiert den Kunden mindestens 30 Tage vor dem Einsatz eines neuen oder dem Wechsel eines Unterauftragsverarbeiters per E-Mail. Der Kunde kann innerhalb von 14 Tagen aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Finden die Parteien keine Lösung, kann jede Partei den betroffenen Teil des Vertrags auf den Einsatzzeitpunkt kündigen. Weitere Rechte hat der Kunde nicht.

7.3 Baldux verpflichtet Unterauftragsverarbeiter vertraglich auf die Pflichten dieses AVV, soweit sie auf deren Leistung anwendbar sind. Bei Standardverträgen grosser Anbieter (etwa Hetzner, AWS, Anthropic, OpenAI, Zoom) gelten deren Datenschutzvereinbarungen als ausreichend, sofern sie Art. 28 DSGVO entsprechen.

8. Übermittlung ins Ausland

Daten werden in Staaten ohne angemessenes Datenschutzniveau nur übermittelt, wenn geeignete Garantien bestehen, insbesondere Standardvertragsklauseln der EU-Kommission mit

Anpassungen für die Schweiz oder eine Zertifizierung nach dem EU-US bzw. Swiss-US Data Privacy Framework. Die Länder stehen in Anlage 2.

9. Verletzung der Datensicherheit

Baldux meldet dem Kunden eine Verletzung der Datensicherheit, die seine Daten betrifft, ohne unangemessene Verzögerung, in der Regel innerhalb von 48 Stunden nach Kenntnis, per E-Mail an die hinterlegte Adresse. Die Meldung enthält, soweit bekannt, Art der Verletzung, betroffene Daten und Personen, wahrscheinliche Folgen und getroffene Massnahmen; fehlende Angaben werden nachgereicht. Ob der Kunde Behörden oder Betroffene informieren muss, entscheidet der Kunde. Die Meldung ist kein Anerkenntnis einer Haftung.

10. Nachweise und Kontrollen

10.1 Baldux stellt dem Kunden die Informationen zur Verfügung, die zum Nachweis der Pflichten aus diesem AVV nötig sind, vorrangig durch die veröffentlichten Seiten [/security](#) und [/unterauftragsbearbeiter](#), Anlage 1 und schriftliche Auskünfte.

10.2 Der Kunde darf Prüfungen einschliesslich Inspektionen durchführen oder durch einen zur Verschwiegenheit verpflichteten, nicht mit Baldux im Wettbewerb stehenden Prüfer durchführen lassen: höchstens einmal pro Jahr, mit 30 Tagen Vorankündigung, während der Geschäftszeiten, ohne Zugriff auf Daten anderer Kunden und ohne Beeinträchtigung des Betriebs. Ohne konkreten Anlass erfolgt die Prüfung durch Dokumente und Fragebögen.

10.3 Der Kunde trägt die Kosten der Prüfung und vergütet den Aufwand von Baldux mit CHF 299 bzw. EUR 299 pro Stunde, ausser die Prüfung deckt einen wesentlichen Verstoß von Baldux auf.

11. Löschung und Rückgabe

Nach Vertragsende kann der Kunde seine Daten 30 Tage lang exportieren. Danach löscht Baldux die Daten der Instanz. Datensicherungen werden im regulären Zyklus von höchstens 5 Wochen überschrieben. Eine gesonderte Löschbestätigung erhält der Kunde auf Anfrage. Gesetzliche Aufbewahrungspflichten von Baldux bleiben vorbehalten.

12. Haftung

Für die Haftung zwischen den Parteien gelten die Beschränkungen der AGB Ziffer 13 auch für Ansprüche aus diesem AVV. Zwingende Haftung gegenüber betroffenen Personen (Art. 82 DSGVO) bleibt unberührt; im Innenverhältnis trägt jede Partei den Anteil, der ihrem Verantwortungsbereich entspricht.

13. Schlussbestimmungen

Rechtswahl und Gerichtsstand richten sich nach den AGB, soweit zwingendes Datenschutzrecht nichts anderes vorschreibt. Änderungen bedürfen der Textform; Anpassungen von Anlage 1 und 2 erfolgen nach Ziffer 4.2 und 7.

Anlage 1: Technische und organisatorische Massnahmen (TOM)

Diese Anlage beschreibt das vereinbarte Mindestniveau. Baldux darf die Massnahmen weiterentwickeln, solange das Schutzniveau insgesamt nicht sinkt (Ziffer 4.2).

Bereich	Massnahmen
Governance	Benannte Verantwortung für Informationssicherheit und Datenschutz; dokumentierte Betriebs- und Sicherheitsvorgaben; regelmässige Überprüfung wesentlicher Risiken.
Trennung der Kunden	Eine Instanz je Kunde: eigene Maschine, eigene Datenbank, eigener Datenbankbenutzer, eigener Hauptschlüssel. Eine verschlüsselte Kopie jedes Hauptschlüssels liegt für die Wiederherstellung im Verwaltungssystem von Baldux. Keine kundenübergreifende Datenbank.
Zugriffskontrolle in der Anwendung	Personengebundene Konten; rollenbasierte Rechte, serverseitig durchgesetzt; Least Privilege und Need-to-know; Entzug bei Wegfall des Bedarfs. Passwörter ausschliesslich als scrypt-Hash. Drosselung der Anmeldewege.
Administrativer Zugang	Server ausschliesslich über SSH-Schlüssel; Passwort-Anmeldung und Root-Login per Passwort abgeschaltet. Datenbank nicht öffentlich erreichbar.

Bereich	Massnahmen
Sitzungssicherheit	Sitzungs-Cookies HttpOnly und SameSite=Lax, in Produktion Secure mit __Host-Präfix; Sitzungsablauf; Herkunftsprüfung schreibender Anfragen.
Transportverschlüsselung	TLS für alle Zugriffe von aussen und für administrative Zugänge; Zertifikate je Instanz automatisch bezogen und erneuert.
Secrets	Hinterlegte Zugangsdaten mit AES-256-GCM unter dem Hauptschlüssel der Instanz verschlüsselt; Schlüssel getrennt vom Quellcode; je Instanz eigene Werte.
Infrastruktur	Gehärtete Basiskonfiguration, minimale offene Dienste, Trennung administrativer und produktiver Zugänge.
Sichere Entwicklung	Review vor dem Zusammenführen von Änderungen; Bewertung von Abhängigkeiten und Schwachstellen; getrennte Entwicklungs- und Produktionsumgebungen; keine Kundendaten in Testumgebungen.
Patch-Management	Bewertung sicherheitsrelevanter Updates; priorisierte Behebung kritischer Schwachstellen; Ausrollen über versionierte Images je Instanz.
Protokollierung	Fachliche Änderungen über einen Ereignisstrom mit Audit-Spur; sicherheitsrelevante Anmeldeereignisse gesondert; Logs liegen auf der Instanz; das Verwaltungssystem von Baldux ruft davon nur allgemeine Betriebskennzahlen ab, vor allem für die Preisberechnung und, auf Anfrage des Kunden, für den Support; Webserver-Zugriffsprotokolle werden automatisch rotiert.
Datensicherung und Wiederherstellung	Tägliche Sicherung der Datenbank auf Host-Ebene; Aufbewahrung 7 Tage täglich plus 4 Wochen wöchentlich; Verschlüsselung vor dem Verlassen des Servers; Übertragung per SFTP auf getrennten Offsite-Speicher; Wiederherstellung nach dokumentiertem Verfahren.
Vorfallmanagement	Verfahren für Erkennung, Bewertung, Eindämmung, Behebung, Wiederherstellung und Benachrichtigung des Kunden nach Ziffer 9.
Upload-Schutz	Uploads als nicht vertrauenswürdig behandelt: Grössenbegrenzung, Auslieferung mit bereinigtem MIME-Typ, keine Ausführung auf dem Server; Ablage in der Datenbank der Instanz.

Bereich	Massnahmen
KI-Assistenten	Externe KI-Assistenten, die Baldux bedient, laufen nur über geschäftliche Konten ohne Training; die dafür angelegten Zugänge widerruft Baldux nach der Aufgabe.
API-Sicherheit	Authentisierte Schnittstellen mit Rollen- und Rechteprüfung; Durchsatzgrenzen je Aufrufer; Begrenzung der Anfragegrösse; Eingabevalidierung.
Unterauftragsverarbeiter	Prüfung vor Einsatz, vertragliche Bindung, öffentlich geführte Liste, Transferprüfung für Drittländer.
Personal	Vertraulichkeitsverpflichtungen; Zugriff nur für die jeweilige Aufgabe; Entzug der Zugänge beim Ausscheiden.
Löschung	Definierte Löschroutinen für produktive Daten, Konten, Backups und Secrets; Backups laufen nach dem Rotationszyklus aus.
Wiederanlauf	Instanzen werden aus versionierten Images und dokumentierten Abläufen neu aufgesetzt; Wiederanlauf aus dem Backup ist Teil des Verfahrens.

Anlage 2: Unterauftragsverarbeiter

Liste unter [/unterauftragsbearbeiter](#) in der jeweils gültigen Fassung.