Zargo

Vertrag zur Auftragsverarbeitung

Stand: 19.11.2026 · Fassung 2026-11-19a

Anlage zu den Nutzungsbedingungen von Zargo. Zum Ablegen auch als PDF.

Parteien

Verantwortlicher ist die Person oder das Büro, das ein Konto bei Zargo führt (im Folgenden „Nutzer").

Auftragsverarbeiter ist Dennis Schrowang, Goldbekufer 27, 22303 Hamburg, E-Mail info@zargo.app (im Folgenden „Zargo").

Der Vertrag wird geschlossen, indem der Nutzer die Nutzungsbedingungen akzeptiert. Eine Unterschrift ist nicht nötig.

1 Gegenstand und Dauer

Zargo speichert und verarbeitet für den Nutzer die Daten, die der Nutzer in seinem Konto ablegt. Soweit darin personenbezogene Daten anderer Personen enthalten sind, geschieht das im Auftrag des Nutzers nach Art. 28 DSGVO.

Der Vertrag gilt, solange das Konto besteht.

2 Art und Zweck der Verarbeitung

Speichern, Anzeigen, Ändern, Exportieren und Löschen der Projektdaten, damit der Nutzer Türen in Grundrissen nummerieren und Türlisten führen kann. Zargo wertet die Daten nicht für eigene Zwecke aus.

3 Art der Daten und betroffene Personen

Daten	Betroffene Personen
Name und Anschrift des Auftraggebers	Bauherren, Auftraggeber
Büro, Anschrift, Bearbeiter, Telefon, E-Mail des Verfassers	Beschäftigte des Nutzers
Name der Person, die einen Änderungswunsch äußert	Auftraggeber, Projektbeteiligte
Raumnamen, Bemerkungen und andere freie Texte	Personen, die der Nutzer dort nennt
Pläne und Logos, soweit sie Angaben zu Personen enthalten (zum Beispiel im Plankopf)	Planverfasser, Bauherren, Projektbeteiligte

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht vorgesehen. Der Nutzer legt solche Daten nicht in Zargo ab.

4 Weisungen

Zargo verarbeitet die Daten nur auf dokumentierte Weisung des Nutzers. Die Weisungen ergeben sich aus diesem Vertrag, den Nutzungsbedingungen und aus der Bedienung der App durch den Nutzer (anlegen, ändern, exportieren, löschen). Weitere Weisungen erteilt der Nutzer per E-Mail.

Hält Zargo eine Weisung für rechtswidrig, teilt Zargo das dem Nutzer mit.

Ist Zargo gesetzlich zu einer anderen Verarbeitung verpflichtet, informiert Zargo den Nutzer vorher, soweit das Gesetz das nicht verbietet.

5 Vertraulichkeit

Zargo wird von einer Einzelperson betrieben. Sie behandelt die Daten vertraulich. Weitere Personen erhalten nur Zugang, wenn sie zur Vertraulichkeit verpflichtet sind.

6 Sicherheit der Verarbeitung

Zargo trifft die technischen und organisatorischen Maßnahmen nach **Anlage 1** (Art. 32 DSGVO). Sie dürfen weiterentwickelt werden, solange das Schutzniveau nicht sinkt.

7 Unterauftragsverarbeiter

Der Nutzer stimmt dem Einsatz der Unterauftragsverarbeiter nach **Anlage 2** zu.

Will Zargo einen weiteren Unterauftragsverarbeiter einsetzen oder einen ersetzen, informiert Zargo den Nutzer mindestens vier Wochen vorher per E-Mail oder in der App. Der Nutzer kann widersprechen. Lässt sich der Widerspruch nicht ausräumen, kann der Nutzer sein Konto löschen und den Vertrag damit beenden.

Zargo verpflichtet Unterauftragsverarbeiter vertraglich auf einen Datenschutz, der diesem Vertrag entspricht. Bei Dienstleistern außerhalb der EU stellt Zargo sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (zum Beispiel durch Standardvertragsklauseln).

8 Rechte der betroffenen Personen

Wendet sich eine betroffene Person an Zargo, verweist Zargo sie an den Nutzer, soweit sich die Anfrage zuordnen lässt. Zargo unterstützt den Nutzer im Rahmen des Möglichen dabei, Anfragen zu Auskunft, Berichtigung, Löschung und Datenübertragbarkeit zu erfüllen. Der Nutzer kann die Daten in der App selbst einsehen, ändern, exportieren und löschen.

9 Unterstützung des Nutzers

Zargo unterstützt den Nutzer mit den vorhandenen Informationen bei dessen Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung).

10 Verletzungen des Schutzes personenbezogener Daten

Wird Zargo eine Verletzung des Schutzes der Daten des Nutzers bekannt, informiert Zargo den Nutzer unverzüglich per E-Mail an die Adresse des Kontos. Die Mitteilung nennt, soweit bekannt, Art und Umfang der Verletzung, die wahrscheinlichen Folgen und die ergriffenen Maßnahmen.

11 Löschung und Rückgabe

Der Nutzer kann seine Daten jederzeit exportieren und löschen. Mit „Konto löschen" werden alle Projekte, Dateien und Einstellungen des Kontos entfernt. Ersetzte Dateien werden frühestens nach 12 Stunden entfernt. In Datensicherungen enthaltene Daten werden mit deren Ablauf gelöscht; aufbewahrt werden die letzten acht wöchentlichen Sicherungen, also rund zwei Monate (Anlage 1).

Gesetzliche Aufbewahrungspflichten bleiben unberührt.

12 Nachweise und Kontrollen

Zargo stellt dem Nutzer auf Anfrage die Informationen zur Verfügung, die nötig sind, um die Einhaltung dieses Vertrags nachzuweisen. Dazu gehören die Beschreibung der Maßnahmen in Anlage 1 und die Nachweise der Unterauftragsverarbeiter.

Reichen diese Informationen im Einzelfall nicht aus, kann der Nutzer nach vorheriger Abstimmung eine Überprüfung durchführen oder durchführen lassen. Sie findet zu üblichen Geschäftszeiten und ohne Störung des Betriebs statt und erstreckt sich nicht auf Daten anderer Nutzer.

13 Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis zwischen Nutzer und Zargo gelten die Regelungen der Nutzungsbedingungen.

14 Schlussbestimmungen

Bei Widersprüchen zwischen diesem Vertrag und den Nutzungsbedingungen geht dieser Vertrag in Fragen des Datenschutzes vor. Es gilt deutsches Recht.

Anlage 1 – Technische und organisatorische Maßnahmen

Stand: 19.11.2026. Beschrieben ist der tatsächliche Stand.

Speicherort und Trennung

- Datenbank und Dateispeicher liegen in einem Rechenzentrum in Frankfurt am Main.

- Entwicklung und Echtbetrieb sind getrennte Umgebungen. Im Echtbetrieb gibt es keine Testkonten und keine Testdaten.

Zugriff auf die Daten der Nutzer

- Jedes Projekt gehört einem Konto. Die Datenbank prüft bei jedem Lesen und Schreiben selbst, ob das angemeldete Konto Zugriff hat (Zugriffsregeln je Zeile auf jeder Tabelle und im Dateispeicher).
- Geschrieben wird ausschließlich über festgelegte Datenbankfunktionen, nicht direkt in die Tabellen.
- Dateien liegen in einem nicht öffentlichen Speicher. Es gibt keine öffentlichen Verweise auf Pläne.
- Nach jeder Änderung an der Datenbankstruktur prüft ein automatischer Test mit zwei fremden Konten, dass keines Daten des anderen lesen, ändern oder löschen kann.

Anmeldung

- Anmeldung mit einem 6-stelligen Einmal-Code per E-Mail (15 Minuten gültig), wahlweise zusätzlich mit Passwort (mindestens 10 Zeichen, nur als nicht umkehrbarer Prüfwert gespeichert).
- Schutz vor automatisiertem Missbrauch durch eine Sicherheitsprüfung (Cloudflare Turnstile) und durch Obergrenzen für Anmeldeversuche und versendete Codes.

Übertragung und Verschlüsselung

- Alle Verbindungen sind verschlüsselt (HTTPS, wird erzwungen).
- Datenbank und Dateien sind beim Dienstleister auf den Datenträgern verschlüsselt gespeichert.
- Sicherheits-Kopfzeilen der App erlauben nur Verbindungen zur eigenen Adresse, zur Datenbank und zur Sicherheitsprüfung; fremde Skripte und das Einbetten in fremde Seiten sind gesperrt.

Zugang des Betreibers

- Die Konten bei den Dienstleistern sind mit Zwei-Faktor-Anmeldung geschützt.
- Der Schlüssel mit vollem Zugriff auf die Datenbank liegt nur auf dem Rechner des Betreibers. Er steht weder im Quelltext noch in der ausgelieferten App; das wird bei jedem Bauen automatisch geprüft.
- Auf Inhalte von Nutzern greift der Betreiber nur zu, wenn es für Betrieb, Fehlersuche oder auf Wunsch des Nutzers nötig ist.

Nachvollziehbarkeit

- Ein Änderungsprotokoll hält fest, welches Konto wann was an einem Projekt geändert hat. Änderungen derselben Angabe kurz hintereinander werden zu einem Eintrag zusammengefasst; je Projekt bleiben höchstens 5.000 Einträge, die ältesten entfallen.

Verfügbarkeit und Wiederherstellung

- Speichern geschieht in einem Zug: Ein Speichervorgang wird ganz oder gar nicht übernommen. Gleichzeitige Änderungen aus zwei Fenstern überschreiben einander nicht.

- Datensicherung: Einmal pro Woche sichert der Betreiber Datenbank und Dateien auf einen eigenen Rechner in Deutschland, nicht bei einem weiteren Dienstleister. Nach jeder Sicherung wird geprüft, ob sie vollständig ist. Aufbewahrt werden die letzten acht Sicherungen (rund zwei Monate), ältere werden gelöscht. Zwischen zwei Sicherungen können bis zu sieben Tage liegen. Der Dienstleister der Datenbank erstellt im derzeitigen Tarif keine eigene Sicherung.
- Wiederherstellung: Das Zurückspielen einer Sicherung ist beschrieben, aber Handarbeit und nicht automatisiert. Es ist für den Fall eines Datenverlusts im Betrieb gedacht, nicht für das Zurückholen einzelner Stände.

Schutz vor Überlastung und Missbrauch

- Je Konto gelten Grenzen für Projekte, Pläne, Türen und Speicher. Die Datenbank setzt sie selbst durch, nicht nur die Oberfläche. Dazu kommen technische Obergrenzen je Projekt und je Datensatz.
- Ein Skript des Betreibers zeigt die Auslastung von Datenbank und Dateispeicher und warnt ab 70 Prozent. Es gibt dabei nur Zahlen aus, keine Inhalte.

Datensparsamkeit

- Die Auswertung der Pläne geschieht im Browser des Nutzers. Pläne werden an keinen weiteren Dienst geschickt.
- Das Anzeigebild eines PDF-Plans berechnet der Browser des Nutzers; es wird nicht beim Dienstleister gespeichert.
- Einmal geladene Plan-Dateien hält der Browser des Nutzers auf dessen Gerät vor (höchstens 300 MB). Beim Abmelden werden sie dort entfernt.
- Kein Tracking, keine Analyse-Werkzeuge.

Anlage 2 – Unterauftragsverarbeiter

Unterauftragsverarbeiter	Aufgabe	Ort der Verarbeitung	Grundlage bei Übermittlung außerhalb der EU
Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapur 049513	Datenbank, Anmeldung, Dateispeicher	Frankfurt am Main (Rechenzentrum von Amazon Web Services als weiterem Unterauftragsverarbeiter)	Standardvertragsklauseln
Brevo SAS, 106 boulevard Haussmann, 75008 Paris, Frankreich	Versand der Mails mit dem Anmelde-Code (verarbeitet nur die E-Mail-Adresse des Kontos)	EU	nicht erforderlich

Unterauftragsverarbeiter	Aufgabe	Ort der Verarbeitung	Grundlage bei Übermittlung außerhalb der EU
Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	Auslieferung der App, DNS, Sicherheitsprüfung (verarbeitet IP-Adressen und Verbindungsdaten, keine Projektinhalte)	weltweites Netz	Data Privacy Framework EU–USA, Standardvertragsklauseln

---

Zargo ist eine Dokumentationshilfe und prüft keine Brandschutz-, Rettungsweg- oder Barrierefreiheitsanforderungen.