Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

Vorlage, Stand 3. November 2026 – keine Rechtsberatung. Diese Vorlage wurde für die confBuild-Plattform erstellt und ist vor der ersten Verwendung durch eine Rechtsanwältin oder einen Rechtsanwalt zu prüfen. Platzhalter in eckigen Klammern sind je Vertrag auszufüllen.

zwischen

[Name des Kunden], [Anschrift] – nachfolgend „Verantwortlicher“ –

und

Daniel Zuidinga, confBuild, Hubertusstr. 68, 52064 Aachen, Deutschland – nachfolgend „Auftragsverarbeiter“ –

§ 1 Gegenstand und Dauer

1. Der Auftragsverarbeiter betreibt die Software-as-a-Service-Plattform confBuild (app.confbuild.com, veröffentlichte Konfiguratoren, Remote-MCP-Server, Cloud Functions) und verarbeitet in diesem Rahmen personenbezogene Daten im Auftrag des Verantwortlichen.
2. Diese Vereinbarung konkretisiert die Pflichten der Parteien aus dem Hauptvertrag (Nutzungsvertrag / AGB confBuild vom [Datum], nachfolgend „Hauptvertrag“).
3. Die Dauer entspricht der Laufzeit des Hauptvertrags. Sie endet mit dessen Beendigung und der Löschung oder Rückgabe der Daten nach § 9.

§ 2 Art und Zweck der Verarbeitung

1. Zweck: Bereitstellung der parametrischen CAD- und Konfigurator-Plattform, Speicherung und Verarbeitung von Projekten, Veröffentlichung von Konfiguratoren, Entgegennahme von Anfragen und Bestellungen von Endkunden des Verantwortlichen, Erzeugung von Stücklisten, Zeichnungen, Angeboten und Exporten, Abrechnung des Abonnements, Support.
2. Art der Verarbeitung: Erheben, Speichern, Verändern, Übermitteln an Unterauftragsverarbeiter nach § 6, Bereitstellen zum Abruf, Löschen.
3. Optionale KI-Funktionen: Ruft ein Nutzer des Verantwortlichen KI-Funktionen auf, werden die dabei eingegebenen Inhalte an den jeweils in der Liste der Unterauftragsverarbeiter genannten KI-Anbieter übermittelt. Der Verantwortliche entscheidet durch Nutzung oder Nichtnutzung der Funktion über diese Übermittlung.

§ 3 Datenkategorien und betroffene Personen

1. Datenkategorien:
    - Konto- und Profildaten (Name, E-Mail-Adresse, Anmeldeverfahren, Rollen, Firmenzugehörigkeit, Adresse, Steuernummer)

    - Projekt- und Konfigurationsdaten einschließlich hochgeladener Dateien, Tabellen, 3D-Modelle, Zeichnungen, Prompts und KI-Ergebnisse
    - Kontaktdaten von Endkunden, die Konfigurationen, Angebotsanfragen, Warenkörbe oder Bestellungen über veröffentlichte Konfiguratoren einreichen (Name, E-Mail, Telefon, Adresse, Firma, Nachricht)
    - Abrechnungsdaten (Plan, Status, Rechnungsadresse, Stripe-Kunden-ID; Zahlungsmittel nur beim Zahlungsdienstleister)
    - Nutzungs-, Protokoll- und Sicherheitsdaten (Zeitstempel, IP-Adresse, Gerät/Browser, Funktionsnutzung, Token-Verbrauch)
    - Kommunikationsdaten aus Support und Benachrichtigungen
2. Betroffene Personen: Mitarbeitende und Beauftragte des Verantwortlichen (Nutzerkonten), Endkunden und Interessenten des Verantwortlichen, Ansprechpartner von Lieferanten, soweit sie in Projekten erfasst werden.

§ 4 Weisungen des Verantwortlichen

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen. Der Hauptvertrag, diese Vereinbarung und die Nutzung der Plattformfunktionen durch den Verantwortlichen gelten als Weisung.
2. Weisungen, die über den Hauptvertrag hinausgehen, sind in Textform an daniel@confbuild.com zu richten. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt; er darf die Durchführung bis zur Bestätigung aussetzen.
3. Weisungsberechtigte Personen des Verantwortlichen: [Name, Funktion]. Empfänger beim Auftragsverarbeiter: Daniel Zuidinga.

§ 5 Pflichten des Auftragsverarbeiters

1. Vertraulichkeit: Alle mit der Verarbeitung befassten Personen sind zur Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht.
2. Technische und organisatorische Maßnahmen nach § 7.
3. Unterstützung des Verantwortlichen bei der Beantwortung von Anträgen betroffener Personen (Art. 12–23 DSGVO). Die Plattform stellt dafür die Selbstbedienungsfunktionen Datenexport (Art. 15, 20) und Kontolöschung (Art. 17) im Bereich „Daten & Datenschutz“ der Einstellungen bereit; Endkundendaten in Anfragen löscht der Verantwortliche über die Anfrage-Inbox.
4. Unterstützung bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 35, 36) mit den dem Auftragsverarbeiter verfügbaren Informationen.
5. Meldung von Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, an [E-Mail des Verantwortlichen] mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar.
6. Datenschutzbeauftragter: Der Auftragsverarbeiter ist nach derzeitigem Stand nicht zur Benennung verpflichtet [zu prüfen]. Ansprechpartner für Datenschutz: daniel@confbuild.com.
7. Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

§ 6 Unterauftragsverarbeiter

1. Der Verantwortliche genehmigt allgemein den Einsatz der in der jeweils aktuellen Liste „Unterauftragsverarbeiter“ (Anlage 2, Download unter app.confbuild.com → Einstellungen → Daten & Datenschutz) genannten Unterauftragsverarbeiter.
2. Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage vor dem Einsatz eines neuen oder dem Austausch eines Unterauftragsverarbeiters per E-Mail an die Kontoadresse. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Kommt keine Einigung zustande, kann jede Partei den Hauptvertrag mit einer Frist von 30 Tagen kündigen.
3. Mit jedem Unterauftragsverarbeiter schließt der Auftragsverarbeiter einen Vertrag, der diesem im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diese Vereinbarung.
4. Übermittlungen in Drittländer erfolgen nur auf Grundlage eines Angemessenheitsbeschlusses, der EU-Standardvertragsklauseln oder einer anderen Garantie nach Art. 46 DSGVO. KI-Anbieter mit Sitz außerhalb des EWR werden nur auf ausdrückliche Nutzung der jeweiligen Funktion durch den Verantwortlichen eingesetzt.

§ 7 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der Auftragsverarbeiter hält die in Anlage 1 beschriebenen Maßnahmen ein und entwickelt sie dem Stand der Technik entsprechend fort. Das Schutzniveau darf dabei nicht unterschritten werden.

§ 8 Kontrollrechte

1. Der Verantwortliche kann die Einhaltung dieser Vereinbarung durch Einholung von Auskünften, Vorlage von Nachweisen (Zertifizierungen und Prüfberichte der Infrastrukturanbieter, Beschreibung der TOMs) und, soweit erforderlich, durch Prüfungen nach vorheriger Abstimmung mit einer Frist von 14 Tagen während der üblichen Geschäftszeiten überprüfen, höchstens einmal jährlich, sofern kein konkreter Anlass besteht.
2. Für Infrastruktur der Unterauftragsverarbeiter genügen deren Zertifizierungen (z. B. ISO 27001, SOC 2) und Prüfberichte.

§ 9 Löschung und Rückgabe

1. Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter alle personenbezogenen Daten, sofern der Verantwortliche nicht innerhalb von 30 Tagen die Rückgabe über den Datenexport der Plattform vornimmt. Die Kontolöschung mit 30-tägiger Karenzfrist steht dem Verantwortlichen jederzeit als Selbstbedienung zur Verfügung.
2. Von der Löschung ausgenommen sind Daten, die gesetzlichen Aufbewahrungspflichten unterliegen (insbesondere Rechnungen und Buchungsbelege nach § 147 AO, § 257 HGB); sie werden nach Ablauf der Frist gelöscht und bis dahin pseudonymisiert und gesperrt.
3. Sicherungskopien werden im turnusmäßigen Rotationsverfahren überschrieben; eine gezielte Löschung einzelner Datensätze aus Sicherungen erfolgt nicht, der Zugriff ist auf die Wiederherstellung beschränkt.
4. Der technische Löschablauf ist in der Dokumentation „DSGVO-Selbstbedienung“ beschrieben und wird protokolliert (ohne Personenbezug).

§ 10 Haftung, Schlussbestimmungen

1. Die Haftung richtet sich nach dem Hauptvertrag und Art. 82 DSGVO.
2. Änderungen und Ergänzungen bedürfen der Textform. Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag geht diese Vereinbarung in datenschutzrechtlichen Fragen vor.
3. Es gilt deutsches Recht. Gerichtsstand ist Aachen, soweit zulässig.

Verantwortlicher: Ort, Datum, Unterschrift: _____

Auftragsverarbeiter: Ort, Datum, Unterschrift: _____

Anlage 1 – Technische und organisatorische Maßnahmen

Bereich	Maßnahme
Zutritts-/Zugangskontrolle	Betrieb ausschließlich in Rechenzentren von Google Cloud (ISO 27001, SOC 1/2/3); kein eigener Serverbetrieb mit Kundendaten. Administrativer Zugang nur mit Zwei-Faktor-Authentifizierung über das Google-Konto des Betreibers.
Zugriffskontrolle	Rollenbasierte Berechtigungen (Firestore- und Storage-Sicherheitsregeln je Nutzer, Firma und Rolle; Admin-Rechte nur über signierte Custom Claims). Server-only-Felder (Guthaben, Abrechnung, Löschstatus) sind für Clients schreibgeschützt.
Weitergabekontrolle	Transportverschlüsselung (TLS 1.2+) für alle Verbindungen; signierte, zeitlich befristete Download-Links für Exporte (7 Tage); keine Fremdinhalte von CDNs (eigene Auslieferung aller Bibliotheken).
Eingabekontrolle	Admin-Audit-Log (`adminAuditLog`), Firmen-Audit-Ereignisse, Sicherheitsereignisse mit wöchentlicher Zusammenfassung; Server-Zeitstempel.
Verfügbarkeitskontrolle	Verwaltete, georedundante Dienste (Firestore, Cloud Storage); Release-Prüfung der Hosting-Dateien nach jedem Deployment; Projektversionen in der Anwendung.
Trennungskontrolle	Logische Mandantentrennung über Nutzer-ID und Firmen-ID in allen Pfaden und Regeln; getrennte Emulator-Testprojekte; Produktionsgeheimnisse im Secret Manager.
Pseudonymisierung/Löschung	Automatisierter Löschlauf nach Inventarliste; pseudonymisierte Aufbewahrung gesetzlich erforderlicher Belege; Audit-Ereignisse ohne Personenbezug.
Verfahren zur Überprüfung	Automatisierte Tests der Sicherheitsregeln und des Lösch-/Exportlaufs gegen den Emulator vor jedem Release der betroffenen Komponenten; jährliche Überprüfung der TOMs.

Anlage 2 – Unterauftragsverarbeiter

Siehe „Liste der Unterauftragsverarbeiter“ (separates Dokument, gleicher Stand).

confBuild · Quelle/source: docs/legal/avv-de.md · erzeugt/generated 2026-11-03