Data Processing Agreement pursuant to Art. 28 GDPR

Template, version 3 November 2026 – not legal advice. This template was drafted for the confBuild platform and must be reviewed by a lawyer before first use. Placeholders in square brackets are completed per contract. In case of doubt the German version prevails.

between

[Customer name], [address] – hereinafter the "Controller" –

and

Daniel Zuidinga, confBuild, Hubertusstr. 68, 52064 Aachen, Germany – hereinafter the "Processor" –

§ 1 Subject matter and duration

1. The Processor operates the software-as-a-service platform confBuild (app.confbuild.com, published configurators, remote MCP server, cloud functions) and processes personal data on behalf of the Controller in that context.
2. This agreement specifies the parties' obligations under the main contract (confBuild terms of use dated [date], the "Main Contract").
3. The term equals the term of the Main Contract. It ends with its termination and the deletion or return of the data pursuant to § 9.

§ 2 Nature and purpose of the processing

1. Purpose: provision of the parametric CAD and configurator platform, storage and processing of projects, publication of configurators, receipt of enquiries and orders from the Controller's end customers, generation of bills of material, drawings, quotes and exports, subscription billing, support.
2. Nature: collection, storage, alteration, transfer to subprocessors under § 6, making available for retrieval, erasure.
3. Optional AI features: when a user of the Controller invokes an AI feature, the content entered is transmitted to the AI provider named in the subprocessor list for that feature. The Controller decides on that transfer by using or not using the feature.

§ 3 Categories of data and data subjects

1. Data categories:
    - account and profile data (name, e-mail address, sign-in method, roles, company membership, address, tax id)
    - project and configuration data including uploaded files, sheets, 3D models, drawings, prompts and AI results

    - contact data of end customers who submit configurations, quote requests, carts or orders through published configurators (name, e-mail, phone, address, company, message)
    - billing data (plan, status, billing address, Stripe customer id; payment instruments only at the payment provider)
    - usage, log and security data (timestamps, IP address, device/browser, feature usage, token consumption)
    - communication data from support and notifications
2. Data subjects: employees and agents of the Controller (user accounts), end customers and prospects of the Controller, supplier contacts recorded in projects.

§ 4 Instructions of the Controller

1. The Processor processes personal data only on documented instructions of the Controller. The Main Contract, this agreement and the Controller's use of the platform features constitute instructions.
2. Instructions beyond the Main Contract are given in text form to daniel@confbuild.com. The Processor informs the Controller without delay if, in its opinion, an instruction infringes data protection law and may suspend execution until confirmation.
3. Persons authorised to issue instructions: [name, role]. Recipient at the Processor: Daniel Zuidinga.

§ 5 Obligations of the Processor

1. Confidentiality: all persons engaged in the processing are bound to confidentiality or subject to a statutory duty of confidentiality.
2. Technical and organisational measures pursuant to § 7.
3. Assistance with requests of data subjects (Art. 12–23 GDPR). The platform provides the self-service functions data export (Art. 15, 20) and account deletion (Art. 17) under "Data & privacy" in the settings; end-customer data in enquiries is deleted by the Controller through the request inbox.
4. Assistance with data protection impact assessments and prior consultations (Art. 35, 36) with the information available to the Processor.
5. Notification of personal data breaches without undue delay and at the latest within 48 hours after becoming aware, to [Controller e-mail], with the information under Art. 33(3) GDPR as far as available.
6. Data protection officer: the Processor is currently not obliged to appoint one [to verify]. Privacy contact: daniel@confbuild.com.
7. The Processor maintains a record of processing activities pursuant to Art. 30(2) GDPR.

§ 6 Subprocessors

1. The Controller gives general authorisation for the subprocessors named in the current "Subprocessor list" (Annex 2, download at app.confbuild.com → Settings → Data & privacy).

2. The Processor informs the Controller at least 30 days before engaging a new or replacing a subprocessor by e-mail to the account address. The Controller may object within that period in text form for important data protection reasons. If no agreement is reached, either party may terminate the Main Contract with 30 days' notice.
3. The Processor imposes on each subprocessor essentially the same data protection obligations as those in this agreement.
4. Transfers to third countries take place only on the basis of an adequacy decision, the EU standard contractual clauses or another safeguard under Art. 46 GDPR. AI providers established outside the EEA are used only on the Controller's express use of the respective feature.

§ 7 Technical and organisational measures (Art. 32 GDPR)

The Processor maintains the measures described in Annex 1 and develops them in line with the state of the art without lowering the level of protection.

§ 8 Audit rights

1. The Controller may verify compliance by requesting information, evidence (certifications and audit reports of the infrastructure providers, description of the measures) and, where necessary, audits agreed in advance with 14 days' notice during normal business hours, at most once per year unless there is a specific reason.
2. For subprocessor infrastructure, their certifications (e.g. ISO 27001, SOC 2) and audit reports suffice.

§ 9 Deletion and return

1. After termination of the Main Contract the Processor deletes all personal data unless the Controller retrieves them within 30 days through the platform's data export. Account deletion with a 30-day grace period is available to the Controller as self-service at any time.
2. Data subject to statutory retention obligations (in particular invoices and accounting records under § 147 AO, § 257 HGB) are excluded from deletion; they are deleted after the retention period and pseudonymised and blocked until then.
3. Backups are overwritten in the regular rotation; individual records are not deleted from backups, and access to backups is limited to restoration.
4. The technical deletion process is described in the "GDPR self-service" documentation and is logged without personal reference.

§ 10 Liability, final provisions

1. Liability is governed by the Main Contract and Art. 82 GDPR.
2. Amendments require text form. In case of conflict between this agreement and the Main Contract, this agreement prevails in data protection matters.
3. German law applies. Place of jurisdiction is Aachen where permissible.

Controller: place, date, signature: _____

Processor: place, date, signature: _____

Annex 1 – Technical and organisational measures

Area	Measure
Physical and system access	Operation exclusively in Google Cloud data centres (ISO 27001, SOC 1/2/3); no self-operated servers with customer data. Administrative access only with two-factor authentication through the operator's Google account.
Data access	Role-based permissions (Firestore and Storage security rules per user, company and role; admin rights only through signed custom claims). Server-only fields (credits, billing, deletion state) are read-only for clients.
Transfer control	Transport encryption (TLS 1.2+) for all connections; signed, time-limited download links for exports (7 days); no third-party CDN content (all libraries served from the platform).
Input control	Admin audit log (`adminAuditLog`), company audit events, security events with weekly summary; server timestamps.
Availability	Managed, geo-redundant services (Firestore, Cloud Storage); hosting file check after every release; project versions inside the application.
Separation	Logical tenant separation by user id and company id in all paths and rules; separate emulator test projects; production secrets in Secret Manager.
Pseudonymisation / deletion	Automated deletion run based on the data inventory; pseudonymised retention of legally required records; audit events without personal reference.
Review procedure	Automated tests of the security rules and of the deletion/export run against the emulator before each release of the affected components; annual review of the measures.

Annex 2 – Subprocessors

See "Subprocessor list" (separate document, same version).

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