CRAFTBASE / LEGAL

Data processing agreement (DPA)

This agreement governs Craftbase's processing of personal customer data and includes the related processing details, safeguards, and subprocessor information.

Last updated: 3 September 2026

1 Roles, parties, and scope

1.1 This data processing agreement (DPA) is entered into between Craftbase GmbH, as the provider identified in the Legal Notice, and the customer identified in the main agreement. It supplements the main agreement for the use of Craftbase.

1.2 The DPA is concluded electronically in the account or together with an individual offer. Craftbase records the accepted DPA revision, time, company, and acting person; the accepted revision remains available to the parties.

1.3 The DPA applies where Craftbase processes personal data on the customer's behalf. It covers paid plans, trials, and free accounts from the time Craftbase first processes personal customer data on the customer's behalf.

1.4 The customer generally acts as controller. Where the customer processes personal data on behalf of a third party, Craftbase acts as a further processor within the scope of this DPA; the customer ensures that it may validly engage Craftbase and issue the required instructions.

1.5 Craftbase does not act as processor for activities where it determines its own purposes and means, including its own contract administration, billing, and processing required by law for security or evidence. Those activities are described in the Privacy Policy.

1.6 Annexes 1 to 3 form part of this DPA. For processing on the customer's behalf, this DPA prevails over the Terms and general service description; individually negotiated data-protection arrangements take precedence.

2 Subject matter and duration of processing

2.1 The processing concerns the provision, operation, protection, maintenance, support, and contractual development of the cloud-based Craftbase application, including features subscribed to or activated by the customer.

2.2 Processing begins when Craftbase first processes personal customer data and continues for the term of the main agreement, including the agreed return, export, and deletion process.

2.3 After the main agreement ends, Craftbase processes remaining customer data only as required for the agreed export, deletion, security of backups, a documented instruction, or a legal obligation directly binding on Craftbase.

2.4 Duties intended by their purpose to continue after termination, including confidentiality, protection of existing backups, return, deletion, and evidence duties, remain in effect to the required extent.

3 Nature and purpose of processing

3.1 Processing may include collecting, recording, organising, storing, adapting, retrieving, transmitting, making available, matching, linking, restricting, backing up, restoring, exporting, and deleting personal data.

3.2 Its nature and purpose follow from the main agreement, service description, subscribed features, administrative settings, and the customer's intended use. Annex 1 provides the details.

3.3 Production AI features process customer data only through active use or configuration by an authorised user. Beta and preview features require voluntary activation.

3.4 Craftbase does not use customer data for its own advertising, data trading, or to train its own generally available models or third-party models. An AI provider may process customer data only if it has been validly engaged under this DPA and is named in the current subprocessor list.

4 Documented instructions

4.1 Craftbase processes personal data only on a documented instruction from the customer unless Union or Member State law directly requires Craftbase to process it.

4.2 Documented instructions arise from the main agreement, this DPA, the service description, intended operation of the application, administrative settings, and communications through the account, support system, or in text form.

4.3 The customer identifies persons authorised to give instructions or establishes their authority through account and role administration. Craftbase may reasonably verify that authority where there is doubt.

4.4 Where Craftbase is legally required to process data without an instruction, it informs the customer of that requirement before processing unless the applicable law prohibits that information on important grounds of public interest.

4.5 If Craftbase considers an instruction to infringe data-protection law, it informs the customer without undue delay. Craftbase may suspend the affected operation until the issue is resolved unless an immediately necessary legal or security measure requires otherwise.

5 Customer rights and obligations

5.1 The customer remains responsible for the lawfulness of processing, protection of data subject rights, and legality of its instructions. Within the agreed service, it determines the purposes and means of processing.

5.2 In particular, the customer meets transparency duties, establishes the required legal bases, and assesses the conditions for special categories of personal data under Article 9 GDPR and data under Article 10 GDPR.

5.3 The customer administers users, roles, and permissions according to need, protects credentials, and informs Craftbase without undue delay of suspected misuse or compromised accounts.

5.4 The customer provides the information and cooperation Craftbase requires for contractual processing, handling requests, containing incidents, and meeting statutory duties.

5.5 Under this DPA, the customer may issue instructions, request evidence, initiate handling of data subject requests, and exercise the agreed audit rights. Statutory rights remain unaffected.

6 Craftbase obligations

6.1 Craftbase processes customer data in accordance with this DPA, documented instructions, and applicable data-protection law and ensures that persons entrusted with processing act only within the permitted scope.

6.2 Craftbase maintains the records of processing activities required of processors and provides the competent supervisory authority with information required by law.

6.3 Craftbase assists the customer as set out in clauses 11 to 13 and informs it of circumstances within Craftbase's responsibility that materially affect the customer's data-protection duties.

6.4 Copies of customer data are created only where required for operations, security, recovery, support, or performance of a documented instruction.

6.5 Data-protection communications to Craftbase may be sent to support@craftbase.de. A data protection officer is identified in the contract information only where the appointment and responsibility have been confirmed.

7 Confidentiality and access

7.1 Before access, Craftbase binds all persons who may access customer data to confidentiality or ensures they are subject to an appropriate statutory duty of confidentiality. The obligation continues after their work ends.

7.2 Access is limited to authorised persons, required tasks, and the minimum necessary scope. Permissions are personal and role-based and are withdrawn when the need ends.

7.3 Support and administrative access to customer content occurs only when required for support, maintenance, or security, is limited in purpose and duration, and is logged where technically provided.

7.4 Where Craftbase must disclose customer data under an enforceable authority or court order, it informs the customer in advance where legally permitted and limits disclosure to what the law requires.

8 Security of processing

8.1 Taking account of the state of the art, implementation costs, the nature, scope, context, and purposes of processing, and the risks, Craftbase maintains appropriate technical and organisational measures under Article 32 GDPR.

8.2 Annex 2 describes the control areas and measures applying to this agreement. To protect the systems, security-sensitive operational detail and evidence may be provided confidentially only to authorised customers, auditors, and authorities.

8.3 Craftbase may adapt measures to technical developments and changing risks provided the agreed level of protection is not reduced overall. A material reduction requires a separate lawful basis.

8.4 Craftbase maintains procedures for risk-based assessment of the effectiveness of the measures and appropriate handling of identified material weaknesses. Specific assessment intervals apply only where expressly documented.

8.5 The customer's security contributions, including secure devices, suitable role assignment, and protection of credentials, complement Craftbase's measures but do not transfer Craftbase's statutory duties to the customer.

9 Subprocessors

9.1 The customer grants Craftbase general written authorisation to engage the subprocessors listed in Annex 3 for the services described there.

9.2 Craftbase publishes the current subprocessor list as part of this DPA and retains previous operative list revisions in a traceable form.

9.3 Craftbase generally informs the customer's administrative contact by email at least 30 calendar days before engaging a new or replacement subprocessor and updates the public list.

9.4 The customer may object within the notice period on specific, substantiated data-protection grounds. An objection to changes in general without a connection to the protection of personal data is insufficient.

9.5 The parties first consider a reasonable alternative or configuration. If no appropriate solution is available, either party may terminate the service affected by the change on reasonable notice; further rights under the main agreement and mandatory law remain unaffected.

9.6 Where a security need or emergency requires a faster replacement, Craftbase may shorten the period to what is necessary and informs the customer with reasons as early as possible.

9.7 Craftbase imposes at least equivalent data-protection obligations on each subprocessor and remains responsible to the customer for the subprocessor's contractual performance under Article 28(4) GDPR.

10 International transfers

10.1 Personal data is transferred to a third country or international organisation only on the customer's documented instruction or because of a legal obligation directly binding on Craftbase and in compliance with Chapter V GDPR.

10.2 A legally relevant remote access from a third country also constitutes a transfer. The current Annex 3 describes known processing locations and safeguards used for each service.

10.3 Where required, Craftbase relies in particular on an adequacy decision or appropriate safeguards such as the applicable EU Standard Contractual Clauses and takes account of required transfer assessments and supplementary measures.

10.4 Selection of a German region for regionally configurable core data is not a general promise that all data, metadata, support operations, or subprocessing take place exclusively in Germany.

11 Assistance with data subject rights

11.1 Taking account of the nature of processing, Craftbase assists the customer through available search, access, export, rectification, restriction, and deletion functions and reasonable supplementary assistance with data subject requests.

11.2 The customer assesses identity, legal basis, scope, and exceptions for a data subject request and remains responsible for responding within the applicable period.

11.3 Where a request received directly by Craftbase clearly concerns customer data, Craftbase securely forwards it to the responsible customer contact without deciding its substance and without undue delay, unless Craftbase is legally required to act directly.

11.4 If the customer cannot retrieve the required data through the application, it provides Craftbase with a sufficiently specific documented instruction and the information needed to identify the data.

12 Personal data breaches and further assistance

12.1 Craftbase notifies the customer of a personal data breach affecting customer data within Craftbase's responsibility without undue delay after becoming aware of it.

12.2 The initial notice includes, where available, a description of the incident, affected data and categories of persons, likely consequences, measures taken or proposed, and a contact. Missing information is supplied without undue delay.

12.3 Craftbase takes appropriate steps to contain, investigate, preserve evidence of, and prevent comparable incidents and assists the customer with available information for its risk assessment.

12.4 The customer generally decides on notifications to supervisory authorities and communications to data subjects. Craftbase communicates about customer data only on a documented instruction or under its own mandatory legal obligation.

12.5 Taking account of the nature of processing and information available, Craftbase assists the customer with its obligations under Articles 32 to 36 GDPR, including security, notifications, communications, data protection impact assessments, and prior consultations.

12.6 Ordinary assistance through product functions, documentation, and standard information is included in the SaaS fee. Exceptional customer-specific work may be charged after prior information and agreement; baseline assistance required by law remains unaffected.

13 Evidence and audits

13.1 Craftbase provides the customer with the information required to demonstrate compliance with Article 28 GDPR and contributes to audits required by law.

13.2 Evidence is provided first through this DPA, the TOM documentation, the subprocessor list, standardised information, and available suitable audit reports.

13.3 If that evidence does not resolve substantiated questions, the customer may conduct a supplementary audit itself or through an independent qualified auditor. Audits are announced reasonably, limited to what is necessary, and generally conducted during customary business hours.

13.4 Without a specific cause, one customer audit per calendar year is generally permitted. Additional audits remain possible after a material incident, on substantiated suspicion, following a material change, or under an authority's order.

13.5 Auditors must be bound by confidentiality. Other customers' data, trade secrets, source code, and security-sensitive information are disclosed only where legally required and no equivalent evidence is sufficient.

13.6 Each party generally bears its own audit costs. Craftbase agrees exceptional additional work with the customer in advance; necessary evidence costs are not shifted to the customer where a material Craftbase breach is established.

14 Return, export, and deletion

14.1 During the agreement, the customer may use the export and deletion functions then supported in production. Customer-specific formats or additional data preparation are owed only where separately agreed.

14.2 After a paid main agreement ends, the customer receives restricted read and export access for 30 calendar days. During that period, the customer secures the data and documents it requires.

14.3 Return generally takes place through the supported exports. Different documented instructions are implemented where lawful, technically feasible, and included in the agreed service.

14.4 After the export period, Craftbase deletes or anonymises customer data from production systems under the documented deletion process. This generally includes invoices issued by the customer and other documents unless separate retention has been commissioned or a duty directly binding on Craftbase requires otherwise.

14.5 The customer's statutory retention duties alone do not provide Craftbase with its own authority to retain data after termination. Continued retention on the customer's behalf requires a documented instruction and corresponding contractual basis.

14.6 Data remaining in backups is processed only for recovery and security and is overwritten under the technically defined backup cycles. If a backup is restored, the deletion and restriction rules apply again.

14.7 On request, Craftbase provides reasonable documented confirmation that the regular deletion process has been completed. Any legally permitted or required residual processing is limited to its relevant purpose.

15 Liability, termination, and final provisions

15.1 Liability between the parties is governed by Article 82 GDPR, other mandatory law, and the legally approved liability provisions of the main agreement. Data subject rights and supervisory authority powers are not restricted by this DPA.

15.2 For a material remediable breach of this DPA, the other party may first require cure within a reasonable period. If the breach continues or waiting is unreasonable, the affected service may be terminated for cause.

15.3 Termination of the main agreement also terminates this DPA except where confidentiality, return, deletion, protection of backups, and evidence duties continue by their purpose.

15.4 Material amendments to this DPA are actively agreed by the parties. Editorial clarifications and exclusively protection-enhancing changes may be notified in documented form without retrospectively changing existing rights.

15.5 The TOMs may be changed without renewed consent if the agreed level of protection is maintained overall. Changes to the subprocessor list follow only the procedure in clause 9.

15.6 The governing law and, where validly agreed, jurisdiction specified in the main agreement apply. Mandatory data-protection jurisdiction remains unaffected.

15.7 If a provision of this DPA is invalid or unenforceable, the remaining provisions continue in effect. Applicable law applies in place of the affected provision.

15.8 Only the German version of this DPA is legally binding. This English version and any other translation are provided for information only; if the texts differ, the German version prevails.

Annex 1 Description of processing

A1.1 This Annex specifies the subject matter, duration, nature, and purpose of processing and the types of personal data and categories of data subjects. Only features actually used by the customer apply.

A1.2 The customer may process special categories of personal data only within the intended scope and where the statutory requirements are met. This gives Craftbase no authority to use that data for its own purposes.

A1.3 If the subscribed feature set changes, this Annex applies to processing operations added through the intended use of those features unless a material amendment to the DPA is required.

Processing framework

Subject matter	Provision, operation, security, maintenance, support, and contractual development of the Craftbase SaaS application.
Purposes	Digital organisation of the customer's contact, project, job, scheduling, working-time, communication, documentation, and billing processes.
Duration	Term of the main agreement, including the agreed export and deletion process and technically required backup cycles.

Types of personal data

Master and contact data	Names, business contact details, addresses, contacts, and customer, supplier, and project assignments.
User and workforce data	Account, authentication, role, permission, working-time, time-account, holiday, and absence data.
Project and job data	Projects, sites, tasks, appointments, services, materials, statuses, reports, acceptances, and custom fields.
Communications and files	Messages, notes, photos, attachments, plans, evidence, and other content submitted by the customer.
Business and document data	Quotes, invoices, payment references, document templates, corrections, exports, and associated history information.
Usage and security data	Technical usage, device, access, error, change, security, and log data to the extent processed on the customer's behalf.

Categories of data subjects

Workforce	Employees, management, apprentices including minors, interns, freelancers, and other customer users.
Business contacts	Customers, prospects, suppliers, subcontractors, business partners, and their contacts.
Project participants	Clients, planners, site managers, project contacts, and other persons assigned by the customer to a job or project.
Other persons	Other persons whose data the customer lawfully records in Craftbase through its intended use.

Special data and limitations

Health-related data	The intended absence type sickness may contain a limited health reference. Diagnoses and detailed medical information are not intended.
Other Article 9 data	Other special categories are not intended without an express agreement, a suitable feature, and confirmed safeguards.
Article 10 data	Data relating to criminal convictions and offences is not intended without an express agreement and confirmed safeguards.
Location data	GPS or comparable location data is covered only once a specific activated product function provides for and documents that processing.

Annex 2 Technical and organisational measures

A2.1 The following control areas describe the contractually required level of protection. Craftbase implements the measures according to risk and the technical architecture used at the relevant time.

A2.2 Individual measures may be replaced with equivalent or more effective measures. The overall level of protection must not be reduced.

A2.3 Further technical evidence, configurations, and audit material are provided confidentially to authorised recipients where required as evidence and compatible with protecting the systems.

Data-protection organisation and confidentiality

Responsibility	Responsibilities for data protection and information security are assigned and material processing operations are documented.
Personnel	Authorised persons are bound by confidentiality before access and receive awareness appropriate to their tasks.

Physical protection and cloud infrastructure

Infrastructure	Production systems use suitable cloud infrastructure; physical data-centre protection is contractually delegated to the infrastructure provider and made auditable.
Work environment	Access from work environments is limited through organisational and technical requirements to authorised persons and devices.

Identity and access control

Authentication	Access is personal; authentication and protective mechanisms reflect the risk and the relevant administrative privilege.
Permissions	Roles and rights follow the need-to-know principle and are adjusted or withdrawn when tasks change or the need ends.

Tenant separation and data access

Separation	Customer data is logically separated by tenant and permissions; access is checked within the intended application context.
Support	Support and administrative access is purpose-specific, limited to what is required, and logged where technically provided.

Transmission and storage

Transmission protection	Personal data in transit is protected against unauthorised access and alteration through technical safeguards appropriate to the risk.
Storage protection	Storage, access, and administrative interfaces are secured according to the protection need and technical architecture; specific methods are evidenced in confidential security documentation.

Logging and incident handling

Traceability	Security-relevant administrative and technical events are recorded to the intended extent and protected against unauthorised alteration.
Incidents	Detected security incidents are assessed, contained, documented, and handled under the defined notification and escalation process.

Availability, backup, and recovery

Availability	Operational and recovery measures reflect risk and the agreed service; a fixed availability or recovery time applies only if expressly agreed.
Backups	Required backups are protected, used only for their purpose, and overwritten under technically documented cycles; recovery procedures are assessed appropriately.

Development, changes, and providers

Software lifecycle	Security and privacy requirements are considered according to risk in development, testing, deployment, and change; identified relevant weaknesses are addressed appropriately.
Providers	Subprocessors are assessed for data protection and security before use, contractually bound, and monitored according to risk.

Annex 3 Subprocessors and transfer information

A3.1 This Annex lists subprocessors confirmed for processing on the customer's behalf. A service may process customer data only after its role, service, and required transfer information have been assessed and documented.

A3.2 Changes are announced under clause 9 and published as a new dated list revision. Previous operative list revisions are retained as evidence.

A3.3 Region information applies only to services that can be configured regionally. Different support, metadata, or further subprocessing is governed by the service-specific contract and transfer information.

Google Cloud and Firebase

Provider	Google Cloud and Firebase services.
Services	Cloud infrastructure, Firebase Authentication, Firebase Data Connect, and other Google or Firebase operational services actually configured.
Purpose	Hosting, data processing, authentication, operations, security, troubleshooting, and technical support for the Craftbase application.
Data	Customer data under Annex 1 and technical account, authentication, usage, security, and log data, depending on the service used.
Processing locations	Germany, particularly Frankfurt, for core data configured for that region; individual services, support operations, and further subprocessors may involve other locations.
Transfer safeguard	For processing outside the EEA, the mechanisms validly agreed for the relevant service under Chapter V GDPR apply.