Current as of 31 Oct 2025

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") forms part of the RIB General Terms and Conditions ("Main Agreement") entered into by and between RIB and You ("Customer") and is incorporated by reference therein. Under the Main Agreement, the services provided by RIB ("Services") may involve the processing, collection, or storage of personal data on behalf of the Customer. The terms "personal data," "controller," "processor," "data subject," "personal data breach," and "processing" shall have the meanings assigned to them under applicable Data Protection Laws (defined below).

Where RIB acts as a sub-processor on behalf of the Customer, who is itself acting as a processor, this DPA shall be interpreted such that any reference to the controller shall mean the processor, and any reference to the processor shall mean the sub-processor.

1. Definitions

In this DPA, capitalized terms not otherwise defined elsewhere or in the General Terms and Conditions shall have the following meanings:

Controller: means the entity that determines the purposes and means of the processing of Personal Data, and for the purposes of this Agreement means Customer.

Customer Data: means all Personal Data provided by Customer to Processor hereunder, including Customer's organization, structure and meta-data that is Personal Data which may be Processed by Processor for or on behalf of Customer in connection with the Services as described in **Annex 2**.

Data Breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Subjects: means an identified or identifiable natural person as defined by Applicable Data Protection Laws.

Personal Data: means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor: means an entity that processes Personal Data on behalf of the Controller, and for the purposes of this Agreement means RIB Software.

Representative(s): means any director, officer, employee, agent, advisor or consultant of a Party or an Affiliate.

Sub-processor: means an entity (which may be a third-party or Processor Affiliate) appointed by or on behalf of Processor to Process Customer Data.

Supervisory Authority: means an independent public authority which is established by a EU Member State.

2. Scope of the Data Processing Agreement ("DPA")

(a) This agreement lays down the rights and obligations that apply when the Processor [**RIB**] processes personal data on behalf of the Controller [the **Customer**]. The identities and addresses of the parties to this DPA are specified in **Annex 1**.

(b) The agreement has been drawn up with a view to compliance by the parties with applicable data protection law that generally applicable to information technology service providers, especially the Article 28(3) of ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation", or "GDPR")*** that sets specific requirements concerning the content of a data processing agreement.

(c) Controller must comply with all laws and regulations applicable to its use of Application, including laws related to confidentiality of communications, and applicable data protection law. Controller is responsible for determining whether the Application is appropriate for storage and processing of information subject to any specific law or regulation and for using the Application in a manner consistent with Controller's legal and regulatory obligations. Controller is responsible for responding to any request from a third-party regarding Controller's use of the Application.

(d) The duration of the processing depends on the duration of the Main Agreement.

(e) The nature and purpose of the processing, as well as the type of personal data and categories of data subjects are specified in **Annex 2**.

3. The Processor acts on instructions

(a) The Processor processes personal data on documented instructions from the Controller, unless required to do so by applicable data protection law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; see Article 28(3)(a) of GDPR.

(b) The Processor shall immediately inform the Controller by E-Mail or in writing if, in its opinion, an instruction is in violation of the applicable data protection law. The processing according to the instruction in question will be suspended until the Controller either revokes or confirms the instruction in writing (E-Mail is sufficient).

(c) Unless otherwise specified in the General Terms and Conditions, Controller may not provide Processor with any sensitive or special personal data that imposes specific data security or data protection obligations on processer in addition to or different from those specified in the DPA or General Terms and Conditions.

4. Confidentiality

(a) The Processor ensures that the persons authorized to process personal data on behalf of the Controller have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The commitment to confidentiality of employees of the Processor extends beyond the end of possible employment with the Processor.

5. Security of processing

(a) The Processor undertakes to take all appropriate technical and organizational measures and maintain them while processing Customer Data, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the Customer Data, as well as the different likelihood and severity of the risk to the rights and freedoms of the data subjects, in order to ensure a level of protection of Customer Data appropriate to the risk.

(b) The Processor guarantees to establish in particular the technical and organizational measures specified in **Annex 3** to this agreement prior to begin processing of Customer Data and to ensure that processing of Customer Data is carried out in accordance with those measures.

6. Engagement of sub-processors

(a) The Customer grants the Processor the general authorization to engage further processors with regard to the processing of Customer Data. The Customer hereby authorizes the engagement of the further processors listed in **Annex 4**.

(b) The Processor will inform the Controller of any intended changes concerning the addition or replacement of further processors, thereby giving the Controller the opportunity to object to such changes within two weeks after receipt of the notification. If the Customer objects, the Controller is entitled to terminate the Main Agreement and this agreement with a notice period of 3 months.

(c) The Processor informs the Controller of the above changes by updating the list of sub-processor on the website or otherwise updated from time to time by the Processor and notified to the Customer.

(d) The Processor will make sure that the same data protection obligations are imposed on sub-processors as those laid down in this data processing agreement via a contract or other legal act under Union or Member State law whereby in particular the appropriate safeguards are provided that the sub-processor will take the necessary technical and organisational measures in such a manner that the processing complies with the requirements of the data protection regulation.

(e) Where the sub-processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the sub-processor's obligations.

7. Transfer of personal data to third countries or international organizations

(a) Processor shall be entitled to process Personal Data, including by using sub-processors, in accordance with this DPA in a third country. Data processing in countries which are neither a Member of the European Union nor a contracting state of the European Economic Area (EEA) (hereinafter referred to as ("third countries") may only take place under the further condition that the requirements of Art. 44 ff. GDPR..

8. Assistance to the Controller

(a) Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

(b) The Processor assists the Controller in ensuring compliance with the Controller's obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the Processor; see Article 28(3)(f) of GDPR.

(c) The processor will immediately inform the controller of any violation of the protection of personal data of which he becomes aware.

9. Monitoring and audits

(a) The Processor makes available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and this agreement and allows and contributes to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller only if:

   a. There has sufficient evidence that Processor failed its compliance with the technical and organizational measures that protect the production systems of the Application;
   b. A personal Data Breach has occurred;
   c. An audit is formally requested by Controller's data protection authority; or
   d. Mandatory applicable data protection law provides Controller with a direct audit right and provided that Controller shall only audit once in any twelve month period unless mandatory applicable data protection law requires more frequent audits.

(b) Controller shall provide at least sixty days advance notice of any audit unless applicable mandatory data protection law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Controller audits shall be limited in time to a maximum of two business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Controller shall provide the results of any audit to Processor.

(c) Controller shall bear the costs of any audit unless such audit reveals a material breach by Processor of this DPA, then Processor shall bear its own expenses of an audit. If an audit determines that Processor has breached its obligations under the DPA, Processor will promptly remedy the breach at its own cost.

10. California Consumer Privacy Act ("CCPA")

(a) If Processor is processing personal data within the scope of the CCPA, Processor makes the following additional commitments to Controller. Processor will process Customer Data and personal data on behalf of Controller and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will Processor sell any such data. These CCPA terms do not limit or reduce any data protection commitments Processor makes to Controller in the DPA, General Terms and Conditions, or other agreement between Processor and Controller.

11. Changes and the notification obligation of the Controller

(a) If a person signs this DPA on behalf of the Controller that person will be regarded as the "representative of the Controller" and information on any changes to the data processing agreement will be submitted to the representative.

(b) It is the obligation of the Controller to notify the Processor if the “representative of the Controller” is changed or the contact information of the representative changes.

12. Deletion and return

(a) Upon termination of the processing services, the processor shall, at the choice of the controller, either delete or return all personal data, as well as documents, other data and generated processing or usage results relating to the contractual relationship, unless there is an obligation to store or retain them under Union or national law. The processor's data shall be irretrievably deleted in accordance with data protection law. An irrevocable physical deletion shall be recorded. This also applies to any data backups at the processor. The processor shall document the deletion in a suitable manner. If there are legal storage obligations, the data must be deleted after the end of the storage obligation. An appropriate deletion concept shall be documented.

(b) Prior to the termination of the contractual services, the processor may only delete data that are no longer required with the prior consent of the responsible party. Consent to deletion can also be given by agreement of the contractual parties to a deletion concept.

(c) The Processor may keep documentations, which serve as evidence of the orderly and accurate processing of Customer Data, also after the termination of the agreement.

The following Annexes form an integral part of this Agreement:

- Annex 1 “parties of this contract“
- Annex 2 “Purpose, type and extent of the processing of Customer Data, types of personal data and categories of data subjects”
- Annex 3 “technical and organisational Measures”
- Annex 4 “Approved subcontractors”

Annex 1 parties of this contract

Provisions on data protection and data security for commissioned data processing

concluded between

Customer

also referred to as the "controller", and

RIB

also referred to as "Processor"

(Both jointly referred to as “Parties”)

Annex 2: Purpose, type and extent of the processing of Customer Data, types of personal data and categories of data subjects

The Processor processes the following personal data on behalf of the Customer in order to provide the services specified in each case:

1. Subject matter of processing

a. Processes personal data for customers to provide them with tools that allow them to collaborate on construction projects. Personal data of customer employees, customer clients, customer suppliers, and customer business partners may be processed as a part of providing this cloud service to customers. Data will be processed by created, stored, archived, retrieved, transformed, deleted, and aggregated within the system. The system will also collect personal data associated with the usage of the system for operational and security purposes, as well as for use in improving the system.

b. Furthermore, the subject matter of the processing arises from RIB’s General Terms and Conditions (hereinafter referred to as “**Agreement**”), to which this refers to.

2. Categories of data subjects:

- System user/contact person (type of personal data see 3 i)
- Customers (business customers) (type of personal data see 3 ii)
- Customers (consumers) (type of personal data see 3 ii)
- Prospective Customers (type of personal data see 3 ii)
- Employees of service providers and/or vendors (type of personal data see 3 ii)

3. Type of personal data

(1) System user/contact person Data

Master data, such as

- Personal master data (e.g. name, last name)
- Communication data (e.g. address, telephone, e-mail, fax)
- Profile picture, if the user uploads

Transaction data, such as

- Account Information (e.g. user account, last login)
- Access Data (e.g. Login name/data, location)
- Other behavioural data associated with usage of the system, if the user uploads

(2) Customer Application data

Master data, such as:

- Personal master data (e.g. name, last name)
- Communications data (e.g. address, telephone, e-mail, fax)
- Other data/documents at the customer’s discretion, e.g.
    - ➢ Staff information: name, salary, role

- ➢ Approval e-signatures
- ➢ Contract master data (contractual relationship, product or contractual interests)
- ➢ Customer/client history (business customer)
- ➢ Contract billing information and payment information (business customer)
- ➢ Planning and control data

Transaction data, at the Customer's discretion, e.g.

- Account statements (Statement information)
- Invoices (Account and Payment info)

Sensitive data processed (if applicable) and restrictions or safeguards applied that take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions (including access only for staff who have undergone specific training), records of access to the data, restrictions on onward transfers or additional security measures.

4. Purposes:

Purposes described herein including the provision of Products, Professional Services and Support Services.

5. Duration of the processing

The Term of the Agreement, or as required to make relevant Customer Personal Data available to Customer, or such other period as required by applicable law including Applicable Data Protection Legislation, whichever is longer.

6. Nature of data processing

- Collection
- Recording
- Storage
- Organization
- Retrieval
- Use
- Disclosure by transmission or otherwise making available
- Erasure
- Destruction

ANNEX 3 TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 5 and 6(d) of the DPA:

1. Safeguards. RIB at all times shall maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, availability, and integrity of (i) Customer's Confidential Information that it maintains or transmits and (ii) logon credentials and computing equipment and devices used, or capable of being used, for remote access to any network or system that is operated by or on behalf of Customer.

2. Secure Destruction. When required under this Agreement and in any case when any of Customer's Confidential Information is no longer needed by RIB to perform the Services, the media on which such Confidential Information is stored or recorded shall be destroyed as follows: (i) paper, film, or other hard copy media shall be shredded or destroyed such that the Confidential Information cannot be read or otherwise cannot be reconstructed; and (ii) electronic media shall be cleared, purged, or destroyed consistent with NIST Special Publication 800 88, Guidelines for Media Sanitization, such that the Customer's Confidential Information cannot be retrieved.

3. Subcontractors. Any disclosure of Customer's Confidential Information to an independent contractor or agent of RIB Subcontractor (each, a "**RIB Subcontractor**") shall be pursuant to a written agreement between RIB and such RIB Subcontractor containing restrictions and conditions on the use and disclosure of Customer's Confidential Information intended to provide the safeguards contemplated in Section 1 of this Schedule. RIB shall take reasonable steps to ensure that the acts or omissions of its RIB Subcontractors would not breach the terms of the Agreement if done by RIB, including making reasonable inquiry of such RIB Subcontractors regarding their ability to comply with the foregoing obligations and taking reasonable steps to monitor such compliance.

4. Security Incident. RIB shall report to Customer in writing any Security Incident (as hereinafter defined) involving or materially threatening Customer's Confidential Information, other than a Security Incident that involves an actual or reasonably suspected Data Breach reported pursuant to Section 6 of this Scheudle, within 30 days of RIB's discovery thereof. For purposes hereof, "Security Incident" means (i) the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information that is maintained in or processed, transmitted, or received a facility at which RIB or any RIB Subcontractor provides services pursuant to the Agreement or (ii) the interference with system operations of the foregoing, in each case other than events that are trivial, routine, do not constitute a material threat to the security of such information, and do not result in unauthorized access to or use or disclosure of such information (such as typical pings and port scans).

5. Encryption of PII.

   a. "***PII***" means Customer's Confidential Information that (i) is personally-identifiable information of an individual, (ii) reasonably might be used (alone or in combination with other information) to identify an individual or to obtain personally-identifiable information of an individual, or (iii) the unauthorized use or disclosure of which would violate any law or regulation or would give rise to an obligation of notification to such individual or any governmental body.

   b. RIB shall render all Customer Data and any PII in transmission unusable, unreadable, or indecipherable by encryption using an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Such algorithmic process shall comply with the requirements of Federal Information Processing Standards (FIPS) 140, Security Requirements for Cryptographic Modules, including, as appropriate, standards described in NIST Special Publication 800 52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, NIST Special Publication 800 77, Guide to IPsec VPNs, NIST Special Publication 800 113, Guide to SSL VPNs, or other standards that are FIPS 140 validated.

c. With regard to Customer Data and PII stored on laptop computers, mobile devices, external hard drives, and removable media, RIB shall, and with respect to PII otherwise stored RIB shall use reasonable efforts to, render all PII in storage unusable, unreadable, or indecipherable by encryption using an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Such algorithmic process shall be consistent with the National Institute of Standards and Technology (NIST) Special Publication 800 111, Guide to Storage Encryption Technologies for End User Devices.

6. Data Breach.

a. "**Data Breach**" means any use or disclosure of Customer's Confidential Information not expressly authorized under, or in breach of, the terms and conditions of the Agreement or in violation of applicable law.

b. Without unreasonable delay and in no case later than 10 days after discovery of an actual or reasonably suspected Data Breach, RIB shall notify Customer of an actual or reasonably suspected Data Breach, such notice to describe the circumstances of the Data Breach, including without limitation, to the extent known, (i) a brief description of what happened, including the date of the Data Breach and the date of the discovery of the Data Breach, (ii) a description of the types of data that were involved in the Data Breach, and (iii) a brief description of what RIB is doing to investigate the Data Breach, to mitigate harm from the Data Breach, and to protect against any further Data Breaches.

c. RIB shall conduct such further investigation and analysis as is reasonably required or reasonably requested by Customer and promptly shall advise Customer of additional information pertinent to the Data Breach that RIB obtains.

d. For purposes hereof, an actual or reasonably suspected Data Breach shall be deemed discovered by RIB as of the first day on which such actual or reasonably suspected impermissible use or disclosure is known to RIB or, by exercising reasonable diligence, would have been known to RIB, and RIB shall be deemed to have knowledge of an impermissible use or disclosure if such impermissible use or disclosure is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the impermissible use or disclosure) who is an employee, agent, or independent contractor of RIB.

e. RIB shall take all actions reasonably necessary, and shall cooperate with Customer as reasonably requested, to mitigate, to the extent practicable, any harmful effect of a Data Breach.

7. Third-party Reports.

a. In the event that RIB obtains any third-party assessment of the design and/or effectiveness of its information security management program (such as, without limitation, a SOC 2 report prepared by a Certified Public Accountant) or achieves any third-party certification of its information security management program (such as, without limitation, certification under ISO 27001), RIB promptly thereupon shall deliver to Customer a copy of such assessment report or certificate or, at RIB's election, notify Customer thereof and permit Customer or, subject to the execution of a confidentiality and security agreement reasonably acceptable to RIB, Customer's designee to review the same at RIB's offices or via a secure online collaboration session).

b. Any such report delivered pursuant to this section will be deemed the Confidential Information of RIB.

c. If any such report includes any findings that RIB materially fails to comply with the applicable standards or includes any material test exceptions, RIB shall use reasonable efforts to remedy such noncompliance promptly. If RIB fails to deliver to Customer evidence of such remedy reasonably satisfactory to Customer within 45 days following such report, or if RIB fails to provide any report or certificate when required pursuant to this paragraph, then any provision of this Agreement to the contrary notwithstanding, Customer may terminate this Agreement without penalty upon written notice to RIB given any time thereafter until such evidence or such report or certificate (as the case may be) is so delivered.

8. Cyber Insurance.

a. RIB shall procure and maintain, at its sole expense, from an insurance company having an A.M. Best rating of "A-" or better and with a financial size category of at least Class VII or, if such ratings are no longer available, with comparable ratings from a generally recognized insurance rating agency, insurance coverage for the unauthorized acquisition, access, use, physical taking, release, distribution, or disclosure of personal information, identity theft, and breaches by third parties and employees, for costs and expenses arising from or relating to an unauthorized disclosure or use of Customer Data or any use or disclosure of Customer Data in breach of the terms and conditions of this Agreement or in violation of applicable law, including such costs and expenses of notification, fraud alert and credit monitoring, mitigation of damages, consultants, forensic investigation, and legal expenses, such policy to include, at a minimum, (A) third-party coverage for data privacy and computer network security breaches, internet and electronic media liability, and professional services liability, (B) first-party business interruption coverage in the event of a network security breach, (C) first-party cyber extortion coverage for threats against data and identity theft, (E) liability coverage for claims related to computer viruses or other malicious code, (F) liability coverage for claims related to theft or destruction of data, and (G) reimbursement for expenses notification of, and costs associated with credit monitoring for, parties affected by a security breach, costs for investigating and managing a security breach, and data privacy regulatory fines and penalties, with limits of not less than $5,000,000 as an annual aggregate ("**Cyber Insurance**").

b. Upon its procurement of the foregoing insurance and thereafter upon Customer's request from time to time, and upon any replacement of or material change to any policy required under this Agreement, RIB shall furnish Customer with certificates or other proof of each such policy reasonably satisfactory to Customer. RIB shall notify Customer within three business days following any cancellation, or receipt of notice of cancellation, of any such policy.

c. The requirements as to the types and limits of insurance coverage to be maintained by RIB pursuant to this Agreement, and any approval or waiver of said insurance by Customer, is not intended to, and shall not, limit or qualify in any manner the liabilities and obligations otherwise assumed by RIB pursuant to this Agreement, including without limitation provisions relating to indemnification. The procurement and maintenance of insurance required under this Agreement shall not limit or affect any liability that RIB may have by virtue of this Agreement or otherwise.

Annex 4 “Approved sub-processors”

The Controller agrees to the commissioning of the following sub-processors, but only under the condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR.

- Sub-processors list for RIB 4.0