

DATA PROCESSING AGREEMENT (DPA)

1. Background and Purpose

The Processor provides the service Kvorrum, a digital platform for organisational governance, document management and communication, to the Controller under a separate services agreement (the “Main Agreement”).

In connection with the provision of the service, the Processor processes personal data on behalf of the Controller. This Agreement governs such processing in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (“GDPR”), Article 28.

2. Definitions

“Personal Data” means any information that can be attributed, directly or indirectly, to a natural person and that is processed by the Processor within the scope of the service.

“Data Subjects” means the natural persons whose personal data is processed, typically the Controller’s employees, board members and other users of the platform.

“Sub-processor” means a third party engaged by the Processor to carry out certain processing on behalf of the Controller.

3. Subject Matter and Purpose of the Processing

The Processor processes personal data solely in order to provide the Kvorrum platform in accordance with the Main Agreement. The processing is carried out on the instructions of, and on behalf of, the Controller. The Processor does not process the personal data for its own purposes.

To the extent that the Controller uses the additional service Contract Insights, the Processor’s personnel also process the documents that the Controller submits for manual review. Such processing is carried out on the Controller’s instructions and solely to perform the commissioned assignment.

To the extent that the Controller uses the automatic reading function in the Contract Tracker module, the contract documents that the Controller uploads there are processed for automated reading with AI support. The reading is performed by the Processor’s Sub-processor Google (Vertex AI / Gemini) within the EU/EEA, for the purpose of suggesting structured data from the document. The processing is carried out on the Controller’s instructions and solely to perform the commissioned assignment. The reading does not constitute automated decision-making under Article 22 of the GDPR; the suggested data takes effect only once a user at the Controller has reviewed and confirmed it. Apart from the storage of the document that already takes place in the service, the reading function does not store any additional copy of the document’s content; only the suggested structured data, together with the associated source quotations, is processed further.

To the extent that the Controller orders the import of existing contracts, the Processor's authorised personnel upload the documents provided by the Controller and have them read in the same way as for automatic reading in Contract Tracker. The Processor's personnel review the suggested data before the contracts are entered into the Controller's part of the service. The processing is carried out on the Controller's instructions and solely to perform the commissioned assignment.

The service sends emails to users through the Processor's Sub-processor for email delivery (see section 5). The emails relate to invitations to the service and reminders of contract deadlines.

Categories of Data Subjects: Employees, board members, elected representatives and other users at the Controller.

Categories of personal data: Name, email address, role and title, room membership, login IP address, login timestamps, names of trusted devices (operating system and browser), information on who has created or amended records in the service and when, content of support tickets, technical error information when errors occur in the service (user ID, organisation, timestamp, error message, page in the service, app version and browser type), and the content of the documents and minutes that the Controller stores in the service. Where applicable, special categories of personal data under Article 9 of the GDPR may be present in the content that the Controller stores or submits. The Controller is responsible for ensuring that there is a legal basis for the processing of such data.

Nature of the processing: Storage, display, search, export, backup, email delivery, logging of technical errors for troubleshooting and support, manual review (for Contract Insights and import), automated reading with AI support (for Contract Tracker and import) and deletion of the above data through the platform's functions.

4. Processor's Obligations

4.1 Instruction-based processing. The Processor processes personal data only in accordance with documented instructions from the Controller, unless Union or Swedish law requires otherwise. In that case, the Processor informs the Controller before the processing begins, unless the law prohibits such notification.

4.2 Confidentiality. The Processor ensures that personnel with access to the personal data are bound by confidentiality undertakings and have received the necessary data protection training.

4.3 Technical and organisational security measures. The Processor implements appropriate technical and organisational measures to protect the personal data against unauthorised access, loss or destruction, in accordance with Article 32 of the GDPR. The measures include, among other things:

- Encryption of data in transit (TLS) and at rest (AES-256 via Google Cloud)
- Role-based access control within the platform
- Authentication via Firebase Authentication with two-step verification (TOTP)

- Regular backups to an encrypted storage device at the Processor's premises in Sweden
- Automated deletion of personal data in accordance with the documented data retention policy (see Appendix 2A)

4.4 Assistance to the Controller. The Processor assists the Controller, to the extent possible and reasonable, in fulfilling its obligations regarding:

- Data Subjects' rights (access, rectification, erasure, restriction, portability and objection)
- Security incidents under Articles 33 and 34 of the GDPR
- Data protection impact assessments (DPIA) under Article 35 of the GDPR

4.5 Notification of a personal data breach. The Processor notifies the Controller without undue delay, and no later than 48 hours, after becoming aware of a personal data breach affecting the Controller's data.

4.6 Deletion on termination. When the Main Agreement terminates, the Controller retains access to the service for thirty (30) days in accordance with the Main Agreement in order to retrieve its data. Thereafter, the Processor deletes all customer data within thirty (30) days from the expiry of the access period, unless the Parties have agreed otherwise in writing or legislation requires continued storage. Copies in backups are deleted as the backups are purged in accordance with Appendix 2A.

4.7 Audit. The Processor provides the information required for the Controller to be able to verify that the obligations under this Agreement are fulfilled. The Controller, or an auditor appointed by it, is entitled to carry out an audit with reasonable advance notice (at least 30 days' notice) and at the Parties' joint expense.

5. Sub-processors

The Processor has the Controller's general authorisation to engage Sub-processors. The Processor currently engages the following Sub-processors:

Sub-processor	Service	Region
Google LLC / Google Cloud Platform	Firebase Firestore (database), Firebase Authentication (login), Firebase Storage (files), Cloud Functions (server logic), Firebase App Check (protection against automated abuse), Vertex AI / Gemini (AI-assisted reading of uploaded contract documents)	EU/EEA. Firestore: europe-north2 (Stockholm); Storage: europe-north1 (Finland); Functions/Vertex AI: europe-west1 (Belgium); App Check (reCAPTCHA Enterprise): global service that may process data outside the EU/EEA, including in the USA (SCCs)
Plus Five Five, Inc. (Resend)	Email delivery: invitations to the service and reminders of contract deadlines. Processes the recipient's email address and the content of the message.	Emails are sent from the EU (Ireland, eu-west-1). Resend is a US company and may process data in the USA. The transfer is made under the EU-US Data Privacy

		Framework and the European Commission's standard contractual clauses (SCC)
--	--	--

The Processor notifies the Controller in writing at least 30 days in advance of any addition or replacement of the Processor's Sub-processors. Additions or replacements of Sub-processors' own sub-processors are notified to the Controller without undue delay after the Processor becomes aware of them. The Controller has the right to object to any such change. The Processor is responsible for the Sub-processor's performance of data protection obligations to the same extent as for its own.

6. Transfers to Third Countries

The Processor endeavours to ensure that personal data is processed within the EU/EEA. Storage of the Controller's data and all AI-assisted reading takes place within the EU/EEA. Email delivery is carried out via the Sub-processor Resend from its EU region (Ireland). Because Resend is a US company, the recipient's email address and the content of the message may also be processed in the USA. Such transfer is made under the European Commission's adequacy decision for the EU-US Data Privacy Framework and the European Commission's standard contractual clauses (SCC), which form part of the Processor's data processing agreement with Resend. Firebase App Check (Google reCAPTCHA Enterprise), which protects the service against automated abuse, is a global service without a data location commitment. Technical information about the user's browser and device may therefore be processed by Google outside the EU/EEA, including in the USA. Such transfer is made under the European Commission's standard contractual clauses (SCC) in accordance with Google Cloud's Data Processing Addendum. To the extent that other Sub-processors handle data in countries outside the EU/EEA, this takes place under standard contractual clauses or another valid transfer tool under Chapter V of the GDPR.

7. Liability and Limitation

Each Party is liable for damage arising as a result of its breach of the GDPR or this Agreement. The Processor's total liability to the Controller under this Agreement is limited to an amount equal to twelve (12) months' fees under the Main Agreement, unless there is gross negligence or wilful misconduct.

8. Term

This Agreement applies for the same period as the Main Agreement and terminates automatically when the Main Agreement terminates, unless mandatory law provides otherwise.

9. Governing Law and Disputes

This Agreement is governed by Swedish law. Disputes arising out of or in connection with this Agreement shall first be resolved through negotiation. If negotiation does not lead to a

resolution within 60 days, the dispute shall be settled by a court of general jurisdiction, with Helsingborg District Court as the court of first instance.

DATA RETENTION PERIODS

Personal data processed within the service is deleted as follows:

Category	Retention period	Action
Active members	During the term of the agreement and the subsequent 30-day access period	Deleted within 30 days after the access period has expired
Archived members	1 year from the date of archiving	The data is deleted automatically
Login IP and trusted devices of archived members	Immediately upon archiving	The fields are reset automatically
Login IP of active members	90 days after last login	The field is reset automatically
Expired and used invitations	90 days after the invitation was created, when it has been used, archived or expired	The data is deleted automatically
Items in the trash (documents, contracts, licences, meetings, votes)	30 days after the item was moved to the trash	The item and associated files are deleted automatically
Closed support tickets	2 years after last amendment	The ticket is deleted automatically
System log (audit log)	2 years	The log entry is deleted automatically
Error logs (technical errors in the service)	90 days from when the error occurred	The log entry is deleted automatically
Backups	All copies from the last 30 days; thereafter one copy per month for 12 months	Older copies are deleted automatically

Purging is carried out by automated scheduled functions that run daily. Each run is logged for traceability.