Data Processing Agreement

Viresta AS, trading as GrantWise · Version 1.1 · Effective 17 August 2026

Who needs this agreement. If you use GrantWise purely for your own proposal, you do not need it — the GrantWise Privacy Policy covers you and GrantWise is the controller.

This agreement applies when you use GrantWise **in the course of your business on behalf of someone else**: a consultant reviewing a client's proposal, an accelerator reviewing a portfolio company's application, a university office acting for a research group. In that case you are the **controller** of any personal data in the documents you upload, and GrantWise is your **processor** within the meaning of Article 28 GDPR.

It takes effect without signature when you first use the service in that capacity. Sign the final page only if your procurement process requires an executed copy.

1. Parties

Processor	Viresta AS, organization number 224 664 729, Lokaltunet 18, 1626 Manstad, Norway, registered in the Norwegian Register of Business Enterprises (Foretaksregisteret), trading as GrantWise (“GrantWise”). Responsible person: Samina Shams. Contact: hello@grantwise360.com
Establishment and supervisory authority	Viresta AS is established in Norway, within the EEA, and is subject to the GDPR as incorporated into Norwegian law by the Personal Data Act (personopplysningsloven). Its supervisory authority is Datatilsynet, the Norwegian Data Protection Authority. No representative under GDPR Article 27 is required.
Controller	The business customer that accepts these terms and uploads documents (“Customer”). Where a signed copy is executed, the Customer's legal name and address are as stated on the signature page.

This agreement supplements and forms part of the GrantWise Terms of Service (the “Principal Agreement”). Where they conflict on the processing of personal data, this agreement prevails.

2. Subject matter and duration

Subject matter. Automated pre-submission quality assessment of funding proposals, and delivery of the resulting report.

Duration. For the term of the Principal Agreement, and for each individual review only for as long as that review requires. Processing of an uploaded document ends when the review of it is complete.

3. Nature and purpose of processing

GrantWise receives a proposal document and supporting material, extracts its text in memory, submits that text to a large language model for inference, generates a report, and delivers the report to the email address supplied. Personal data is processed only to provide that service, to secure it, to bill for it, and to meet legal obligations.

4. Categories of data subject

- Individuals named in the uploaded proposal or annexes — typically project team members, principal investigators, company officers and partner contacts.
- The individual submitting the review and receiving the report.

5. Types of personal data

- Names, job titles, professional affiliations, qualifications, biographies and CV content appearing in the uploaded documents.
- Professional contact details appearing in the uploaded documents.
- The submitting person's email address, chosen programme, optional project acronym, and optional organisation type and country.
- Technical data required to operate and secure the service, such as IP address and request timestamps.

Special category data. The service is not designed for and must not be used to process special categories of personal data under Article 9 GDPR, or personal data relating to criminal convictions. The Customer must not upload documents containing such data.

6. GrantWise obligations as processor

1. **Documented instructions.** GrantWise processes personal data only on the Customer's documented instructions. The Customer's instruction is its use of the service: to run the requested review on the documents uploaded. GrantWise will inform the Customer if it believes an instruction infringes data protection law. Where required by law to process beyond those instructions, GrantWise will inform the Customer first unless the law forbids it.
2. **No training.** GrantWise does not use Customer documents, their content, or the resulting reports to train, fine-tune or improve any machine learning model, and its AI provider is contractually bound not to do so with data submitted through the enterprise interface used.
3. **Confidentiality.** Every person authorised to process personal data under this agreement is bound by an obligation of confidentiality.
4. **Security.** GrantWise implements the measures set out in Annex 2.
5. **Subprocessors.** As set out in section 8.
6. **Data subject rights.** If a data subject contacts GrantWise directly about data processed for the Customer, GrantWise will not respond substantively; it will refer them to the Customer and notify the Customer without undue delay. Because uploaded documents are not retained, practical assistance is generally limited to confirming that no copy exists.
7. **Assistance.** Taking into account the nature of processing and the information available, GrantWise will assist the Customer with data protection impact assessments, prior consultation and security obligations under Articles 32 to 36 GDPR.
8. **Breach notification.** GrantWise will notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach affecting data processed for the Customer, with the information then available and updates as investigation proceeds.
9. **Deletion or return.** On termination, and at the Customer's choice, GrantWise deletes or returns personal data processed for the Customer and deletes existing copies unless law requires retention. Because uploaded documents are not stored, this is limited in practice to generated reports and account correspondence.
10. **Audit.** GrantWise makes available the information necessary to demonstrate compliance with this agreement, and allows and contributes to audits, including inspections, by the Customer or an auditor it mandates. Audits are on reasonable notice, no more than once in any twelve-month period unless a breach has occurred or a supervisory authority requires it, during business hours, subject to confidentiality, and at the Customer's cost. GrantWise may satisfy an audit request by providing its subprocessors' current certifications and reports where these address the request.

7. Customer obligations as controller

1. The Customer warrants that it has a lawful basis for the processing it instructs, and that it has provided the required transparency information to the individuals whose personal data appears in the documents uploaded.
2. The Customer warrants that it is entitled to disclose those documents to GrantWise, and that doing so does not breach any confidentiality obligation, consortium agreement, non-disclosure agreement or third-party right.
3. The Customer must not upload special category data, criminal-offence data, or personal data of children.
4. The Customer is responsible for the accuracy of the email address supplied. Reports are delivered to that address, and a wrong address is a disclosure that cannot be recalled.

8. Subprocessors

The Customer gives general written authorisation for GrantWise to engage the subprocessors below. GrantWise imposes data protection obligations on each that are no less protective than those in this agreement, and remains fully liable to the Customer for their performance.

Subprocessor	Purpose	Location
Google Cloud / Vertex AI (Google Ireland Ltd / Google LLC)	AI inference; temporary report storage in Firestore	EU (europe-west1, EU multi-region)
Cloudflare, Inc.	Website delivery, DNS, security and DDoS protection	Global edge network
Resend (Plus Five Five, Inc.)	Transactional email delivery of reports and reminders	United States
Stripe, Inc. / Stripe Payments Europe Ltd	Payment processing. Stripe acts as an independent controller for payment data; GrantWise never receives card details.	EU and United States

Not a subprocessor: website analytics. GrantWise uses PostHog (PostHog Cloud EU, Frankfurt) for analytics on grantwise360.com, loaded only for visitors who accept analytics in the cookie banner. PostHog is **not** a subprocessor under this agreement, because it never receives Customer Data: no uploaded document, no document content, no report, no file name and no proposal-derived personal data is sent to it. It processes website visitor data for which GrantWise is the controller in its own right. It is named here so that the boundary is explicit rather than assumed. If that ever changes, it becomes a subprocessor and the notice period below applies.

Changes. GrantWise will give at least 30 days' notice before adding or replacing a subprocessor, by email to the address associated with the Customer's use of the service and by updating grantwise360.com/dpa.html. If the Customer reasonably objects on data protection grounds within that period, it may terminate the Principal Agreement without penalty and receive a pro-rata refund of any prepaid amount for services not yet delivered.

9. International transfers

Viresta AS is established in Norway, within the EEA. Its own processing takes place in Norway, and AI inference and temporary report storage take place in EU regions. Where the Customer is established in the EEA, its disclosure of personal data to GrantWise is therefore not a transfer to a third country and requires no transfer mechanism.

Onward transfers do occur at the subprocessor layer: email delivery and parts of payment processing involve transfer to the United States. For those transfers GrantWise acts as exporter and relies on one or more of: an adequacy decision; the EU–US Data Privacy Framework where the recipient is certified; or the Standard Contractual Clauses adopted by the European Commission in Decision 2021/914, which apply in Norway through the EEA Agreement.

Where the Standard Contractual Clauses nonetheless apply between the parties — for example where the Customer is established outside the EEA and the Clauses are the agreed mechanism — Module Two (controller to processor) is incorporated by reference and completed as follows: clause 7 (docking) applies; clause 9 option 2 (general written authorisation) applies with the 30-day notice period in section 8; clause 11 does not include the optional independent dispute resolution body; clause 17 selects the law of Ireland; clause 18(b) selects the courts of Ireland. Ireland is selected because clause 17 requires the law of an EU Member State and Norway, as an EEA state, does not qualify; that choice governs the Clauses only and does not displace the Norwegian governing law in section 10. Annexes I, II and III of the Clauses are populated by sections 2 to 5, Annex 2 and section 8 of this agreement respectively.

10. Liability, term and governing law

Each party's liability under this agreement is subject to the limitations and exclusions in the Principal Agreement, except where a limitation is not permitted by applicable data protection law. This agreement terminates automatically when the Principal Agreement ends, save for provisions that by their nature survive. It is governed by Norwegian law, in line with the Principal Agreement, and the agreed venue is Søndre Østfold tingrett, except that where the Standard Contractual Clauses apply, the law specified in section 9 governs those Clauses and nothing here limits data subject rights under them or under the GDPR as incorporated into Norwegian law by the Personal Data Act (personopplysningsloven).

Annex 1 — Processing summary

Subject matter	Automated pre-submission assessment of funding proposals

Duration	Term of the Principal Agreement; per document, only for the duration of the review
Nature and purpose	Text extraction, AI inference, report generation, report delivery
Personal data	As listed in section 5
Data subjects	As listed in section 4
Retention	Uploaded documents: not stored. Generated report and delivery email: up to 7 days. Version registry: scores, non-reversible fingerprints and short finding summaries, containing no proposal text. Payment records: as required by law.

Annex 2 — Technical and organisational measures

1. **Data minimisation by architecture.** Uploaded documents are held in memory for the duration of the review and are never written to a document database or object store. This is the primary security control: data that is not stored cannot be breached, exfiltrated or wrongly retained.
2. **Encryption.** TLS for all data in transit. Encryption at rest for the temporary report store and all subprocessor storage.
3. **Access control.** Least-privilege service accounts per service. Credentials held in a managed secret store, never in source code or configuration files. Administrative endpoints require a separate access token.
4. **Regional processing.** AI inference and temporary report storage are configured to EU regions.
5. **Retention limits enforced in code.** Generated reports carry an expiry timestamp and are deleted automatically; retention is not left to manual housekeeping.
6. **Content-redacted logging.** Operational logs record timing, status, error category and cost. Proposal text, report text, evidence quotations and prompt bodies are excluded from logs by design.
7. **Input validation.** File type and size validation before extraction; limits on decompressed size and parse time to resist archive-bomb and resource-exhaustion attacks.
8. **Rate limiting and abuse controls** on public endpoints.
9. **Segregation.** Analytics and benchmark records are irreversibly separated from identity and contain no proposal or report text.
10. **Change control.** Continuous integration runs the full test suite, including a booted-server smoke test, on every change before deployment.
11. **Resilience.** Managed, replicated cloud infrastructure with provider-level redundancy. Because customer documents are not retained, there is no customer-document backup to restore or to leak.
12. **Personnel.** Access limited to personnel who need it, each under a confidentiality obligation.

Signature

This agreement is effective without signature when the Customer uses the service in the capacity described in the opening panel. Complete and sign the Controller column only if an executed copy is required, then send it to hello@grantwise360.com. A countersigned copy will be returned.

Controller (Customer)	Processor (GrantWise)
Legal entity name _____	Legal entity name Viresta AS
Organization number _____	Organization number 224 664 729
Registered address _____ _____	Registered address Lokaltunet 18 1626 Manstad, Norway
Signature _____	Signature _____
Name and title _____	Name and title Samina Shams, Responsible Person
Date _____	Date _____

Questions: hello@grantwise360.com · Terms of Service: grantwise360.com/terms.html · Privacy Policy: grantwise360.com/privacy.html · Legal Notice: grantwise360.com/legal-notice.html