DATA PROCESSING ADDENDUM

GrantGenix | Version 1.1 | 21 October 2026

This Data Processing Addendum (the "DPA") forms part of the terms under which Elska Flow Consulting AB (organisation no. 559357-5144, Gripengatan 38, 177 67 Järfälla, Sweden), owner of GrantGenix ("ELSKA"), provides GrantGenix to a customer (the "Customer"), whether under the GrantGenix Terms & Conditions or any other written agreement that incorporates this DPA. It applies to the extent ELSKA processes personal data on behalf of the Customer and sets out the terms required by Article 28 of Regulation (EU) 2016/679 ("GDPR").

1. Roles and scope

1.1 For personal data contained in material that the Customer submits to GrantGenix ("Customer Personal Data"), the Customer is the controller, or a processor acting for its own clients, and ELSKA is the processor, or a sub-processor. Details of the processing are in Annex 1.

1.2 ELSKA acts as an independent controller for account, billing and website-usage data that it holds for its own purposes. That data is described in the GrantGenix Privacy Policy and is outside this DPA.

2. Instructions

2.1 ELSKA shall process Customer Personal Data only on the Customer's documented instructions, which are: this DPA, the agreement under which GrantGenix is provided, and the Customer's use of GrantGenix features. Any further instruction must be in writing and agreed with ELSKA.

2.2 ELSKA shall inform the Customer without undue delay if it believes an instruction infringes data protection law, and may suspend the relevant processing until the Customer confirms or amends it. Where EU or Member State law requires ELSKA to process the data otherwise, ELSKA shall inform the Customer before processing unless the law prohibits it.

3. Customer responsibilities

3.1 The Customer is responsible for having a valid legal basis for submitting Customer Personal Data, for giving any required notices to data subjects, and for the lawfulness of its instructions. Where the Customer acts as a processor for its own clients, it confirms that it has the authorisation of the relevant controller(s) for ELSKA's processing, including the use of the sub-processors in Annex 3.

3.2 The Customer shall not submit special categories of personal data (Article 9 GDPR) or data relating to criminal convictions (Article 10 GDPR) to GrantGenix, and shall minimise the personal data it includes in submitted material.

4. Confidentiality

4.1 ELSKA shall ensure that everyone it authorises to process Customer Personal Data is bound by a duty of confidentiality and processes the data only as needed to provide GrantGenix.

5. Security

5.1 ELSKA shall implement appropriate technical and organisational measures to protect Customer Personal Data as required by Article 32 GDPR, taking into account the risks of the processing. The measures in place at the date of this DPA are described in Annex 2. ELSKA may update them, provided the overall level of protection is not reduced.

6. Sub-processors

6.1 The Customer gives ELSKA general authorisation to use the sub-processors listed in Annex 3.

6.2 ELSKA shall give the Customer at least thirty (30) days' notice (by email or on the GrantGenix website) before adding or replacing a sub-processor. The Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Customer may stop using GrantGenix and ELSKA shall refund any prepaid fees for the period after termination.

6.3 ELSKA shall bind each sub-processor by a written contract imposing data protection obligations no less protective than those in this DPA, and remains responsible to the Customer for the sub-processor's performance of those obligations.

7. International transfers

7.1 ELSKA shall transfer Customer Personal Data outside the EU/EEA only where a transfer mechanism under Chapter V GDPR applies (for example an adequacy decision, or the EU Standard Contractual Clauses together with any required supplementary measures). ELSKA shall document the mechanism used for each sub-processor in Annex 3.

8. Assistance

8.1 Taking into account the nature of the processing, ELSKA shall assist the Customer by appropriate technical and organisational measures in responding to requests from data subjects. If ELSKA receives such a request directly, it shall forward it to the Customer without undue delay and shall not respond to it itself except to acknowledge receipt.

8.2 ELSKA shall assist the Customer in complying with Articles 32 to 36 GDPR (security, personal data breaches, data protection impact assessments and prior consultation), taking into account the information available to ELSKA.

9. Personal data breaches

9.1 ELSKA shall notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, and shall provide the information reasonably available to it to allow the Customer to meet its own notification duties. ELSKA shall take reasonable steps to contain the breach and mitigate its effects.

10. Deletion and return

10.1 On termination or expiry of the Customer's access, ELSKA shall, at the Customer's choice, delete or return Customer Personal Data within thirty (30) days, unless EU or Member State law requires it to be retained. Copies in routine backups are deleted in the ordinary backup cycle. On request, ELSKA shall confirm deletion in writing.

11. Audits and information

11.1 ELSKA shall make available to the Customer the information necessary to demonstrate compliance with Article 28 GDPR. Where that information is not sufficient, the Customer (or an independent auditor bound by confidentiality) may audit ELSKA's compliance with this DPA on thirty (30) days' written notice, at most once in any twelve (12) month period unless a personal data breach has occurred or a supervisory authority requires otherwise. The audit shall be carried out during normal business hours at the Customer's cost, shall not disrupt ELSKA's operations unreasonably, and shall not extend to source code, models, prompts, or the data of ELSKA's other customers.

12. Liability

12.1 Each party's liability under this DPA is subject to the limitations and exclusions in the agreement under which GrantGenix is provided. Nothing in this DPA limits a data subject's rights under Article 82 GDPR or liability that cannot be limited by law.

13. Term, precedence and governing law

13.1 This DPA applies from the date the Customer first submits Customer Personal Data and continues for as long as ELSKA processes Customer Personal Data on the Customer's behalf.

13.2 If this DPA conflicts with any other terms on the processing of personal data, this DPA prevails. In all other respects the agreement under which GrantGenix is provided prevails.

13.3 This DPA is governed by Swedish law. Disputes are resolved in accordance with the dispute resolution provisions of the agreement under which GrantGenix is provided.

Annex 1 — Details of the processing

Item	Description
Subject matter	Provision of GrantGenix, an AI-assisted tool that evaluates funding proposals.
Duration	For as long as the Customer has access to GrantGenix, plus the deletion period in clause 10.
Nature and purpose	Receiving, storing, analysing and evaluating material submitted by the Customer; generating evaluation reports; support; security and abuse prevention.
Types of personal data	Names, contact details, job titles, affiliations, and biographical or professional information about individuals mentioned in submitted proposals and documents; account login details of the Customer's users.
Categories of data subjects	The Customer's staff and users; applicants, consortium partners and other individuals named in submitted proposals.
Special categories	None. Customers must not submit special category data (clause 3.2).
Frequency	Continuous, for as long as the Customer uses GrantGenix.

Annex 2 — Technical and organisational measures

Measure	Description
Access control	Accounts are created only by an ELSKA administrator; each user has unique login credentials; access to Customer Personal Data is limited to the personnel described in clause 4.1 and the Personnel row below.
Encryption	All connections to the Platform use TLS 1.2 or higher, with HTTP traffic automatically redirected to HTTPS. Passwords are hashed using PBKDF2-SHA-256 (600,000 iterations, per-user salt); plaintext passwords are never stored or logged. Password verification uses constant-time comparison to prevent timing-based attacks.
Segregation of customer data	Customer data is scoped by account and role at the application layer: each user's queries return only records belonging to their own account, enforced server-side. Administrator accounts follow the same rule: they see only the proposals they upload or evaluate themselves, and only usage counts for other accounts. Access to the underlying database at the hosting level is restricted to a named ELSKA technical administrator and is used only for maintenance and incident response.
Logging and monitoring	Audit logging captures login events, role changes, deactivations, key assignments and other administrative actions, each recorded with timestamp, actor and IP address. Additional abuse-prevention controls include anomaly detection (for example, flagging an unusually high number of distinct IP addresses for one user) and a cap of five versions per proposal for non-admin users.

Measure	Description
Backups and recovery	The application database is backed up weekly to encrypted storage; backups are retained for 35 days before they cycle out.
Personnel	Confidentiality undertakings for everyone with access to Customer Personal Data.
Retention	No historical customer data is retained beyond the periods set out in the Privacy Policy and clause 10.
Incident response	Suspected incidents are investigated as part of routine security monitoring. Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, ELSKA notifies the Swedish supervisory authority (IMY) within 72 hours and notifies affected users without undue delay, in accordance with Articles 33 and 34 GDPR (see also clause 9 of this DPA).

Annex 3 — Authorised sub-processors

Sub-processor	Service	Location	Transfer mechanism
Anthropic, PBC	AI model processing (Claude API); default provider	United States, with EU regional processing where available	EU–US Data Privacy Framework (where self-certified) and/or the European Commission's Standard Contractual Clauses (2021/914)
OpenAI	AI model processing (GPT models); only where selected by the Customer	United States	EU–US Data Privacy Framework (where self-certified) and/or the European Commission's Standard Contractual Clauses (2021/914)
Mistral AI	AI model processing (Mistral models); only where selected by the Customer	European Union	Not applicable (processing within the EU/EEA)
Railway Corp.	Hosting of the evaluation platform (evaluate.grantgenix.com) and persistent storage of Customer Personal Data (SQLite + Volume)	European Union (Netherlands region); the provider is established in the United States	European Commission's Standard Contractual Clauses (2021/914)

Anthropic does not use API inputs or outputs to train its models by default, and retains inputs and outputs for up to 30 days for trust-and-safety purposes only, after which they are deleted. Anthropic is the default AI provider; OpenAI and Mistral AI process Customer Personal Data only where the Customer selects them for an evaluation. All transfers to processors outside the EEA are supplemented by technical measures including encryption in transit (TLS 1.2 or higher). An up-to-date list of sub-processors is available on request at info@grantgenix.com; ELSKA will notify the Customer in advance of material changes in accordance with clause 6.2.