Trust, Privacy & Data Protection

An overview of how GrantsMate approaches institutional data stewardship.

Research institutions work with valuable, confidential, and sometimes sensitive information. GrantsMate is designed with institutional data stewardship in mind. We aim to use customer information only as needed to provide, support, secure, and improve the services selected by each institution, subject to the applicable customer agreement.

Our approach at a glance

- Customers control what institutional data is provided and who may access it.
- GrantsMate does not sell Customer Data or use it for targeted advertising.
- The platform uses tenant-aware access controls designed to separate each institution's private data.
- AI-enabled features are used to deliver requested functionality, with contractual data-use boundaries available for institutional customers.
- Specific security, retention, deletion, hosting, and support commitments are documented in the applicable agreement.

Customer control

- **Institutional choice.** Each customer determines the data it provides, the users it authorizes, and the GrantsMate features it enables.
- **Purpose-focused processing.** Customer Data is processed to operate, support, secure, and administer the selected services and as otherwise described in the applicable agreement.
- **Customer-specific terms.** Data residency, retention, deletion, export, support access, and other institution-specific requirements may be addressed through an order form, data processing addendum, or security exhibit.

Clear data-use boundaries

- **No sale of Customer Data.** GrantsMate does not sell Customer Data or share it with another customer without the data owner organization's explicit permission.
- **No targeted advertising.** Customer Data is not used to deliver targeted or cross-context behavioral advertising.
- **AI model training.** Under GrantsMate's standard institutional approach, Customer Content is not used to train, fine-tune, or improve general-purpose or shared AI models unless the customer expressly authorizes that use in writing.
- **Service providers.** GrantsMate may use cloud, AI, search, storage, monitoring, authentication, and other service providers to deliver the platform. The providers used may vary by feature, configuration, and customer agreement.

Security-minded platform design

- **Tenant-aware access.** GrantsMate uses role-based and tenant-aware controls designed to limit users and tenant administrators to the institutional environment they are authorized to access.
- **Layered safeguards.** The platform is designed to use a combination of cloud infrastructure protections, access controls, encryption capabilities, secrets management, monitoring, logging, and operational safeguards appropriate to the services provided.
- **Limited administrative access.** Access by GrantsMate personnel is intended to be limited to authorized business purposes such as support, maintenance, security, troubleshooting, legal compliance, and customer-authorized operations.
- **Ongoing development.** Security practices and platform controls evolve as GrantsMate's services, infrastructure, and customer requirements develop. Current contractual commitments are set out in the applicable customer documents.

Responsible use of AI

- **Feature-specific processing.** AI-enabled features may process a user's question, relevant funding information, selected document excerpts, or other context needed to provide the requested response.
- **Human review.** AI-generated recommendations, summaries, and responses may be incomplete or inaccurate and should be reviewed by qualified institutional personnel before they are used for funding, compliance, legal, or administrative decisions.
- **Institutional configuration.** Available AI providers and controls may vary by deployment and enabled module. Customer-specific requirements should be documented before deployment.

Retention, deletion, and regulated information

- **Retention and deletion.** Retention, export, deactivation, and deletion practices depend on the customer agreement, system configuration, operational requirements, legal obligations, and backup lifecycle.
- **Regulated or highly sensitive data.** Unless expressly authorized by GrantsMate in writing, customers should not submit protected health information, payment-card data, classified or controlled unclassified information, export-controlled technical data, or other specially regulated information. Customers are responsible for ensuring that the information they submit is appropriate for use with the service. GrantsMate cannot accept responsibility for regulated or highly sensitive information submitted without prior written authorization.
- **Education records.** Use involving personally identifiable information from student education records should be addressed through an institution-specific agreement before such information is submitted.

Questions about institutional data protection?

Institutional customers and prospective partners may contact **team@grantsmate.ai** to discuss data-processing requirements, security documentation, subprocessors, or customer-specific safeguards.

About this page. This page is a general, non-technical overview of GrantsMate's approach and is not a contract, security certification, warranty, or complete privacy notice. Features and controls may vary by product, deployment, configuration, and customer agreement. Binding commitments are contained only in an executed agreement, order form, data processing addendum, or security exhibit. This page does not expand or modify those documents.