

Data Processing Agreement

How Astra FP&A LLC protects and handles your district's data. This is the text published at <https://astraarpa.ai/dpa>.

1. Parties and scope

This Data Processing Agreement (“DPA”) is part of the Terms of Service (or other signed agreement) between Astra FP&A; LLC (“Provider”) and the Customer. It applies whenever Provider processes personal information contained in Customer Data on the Customer’s behalf in providing Astra FP&A; K-12. Terms not defined here have the meanings in the Terms.

If this DPA conflicts with the Terms on the protection of personal information, this DPA controls.

2. Roles and instructions

The Customer controls its Customer Data and decides why and how it's processed. Provider processes it only on the Customer's documented instructions, which are the Terms, this DPA and the Customer's use of the Service's features, and acts as the Customer's service provider (or “processor”) under applicable privacy law. Provider will tell the Customer if it believes an instruction breaks the law.

Provider will not sell or share Customer Data; will not retain, use or disclose it for any purpose other than providing the Service; will not combine it with personal information from other sources except as the Service requires; and will not use it to train AI models.

3. What is processed

Purpose	Providing, securing and supporting the Service: hosting, calculating, building files and answering questions with the AI analyst.
People concerned	The Customer's Users (employees and contractors who use the Service).
Personal information	Users' names, work email addresses, roles, sign-in records and activity records, and the questions they ask the AI analyst.
Customer Data	Summarized financial, enrollment, personnel-cost and program data, documents, and brand materials. By design this data contains no records about individual people.
Duration	The subscription term, plus the return and deletion period in section 10.

4. Records about individual people

The Customer agrees not to provide records about individual students, employees or others, including education records, Social Security numbers, dates of birth, health information, financial account numbers, or individual pay or financial aid. Salary data must be summarized so every row covers at least five people. The Service scans uploads and refuses files that appear to contain such information.

If such information nonetheless reaches the Service, Provider will protect it under this DPA, will not use it except to remove it, and will delete it promptly after discovering it or on the Customer's request, notifying the Customer where it discovers it.

FERPA. To the extent Provider receives any personally identifiable information from education records, Provider acts as a “school official” with a legitimate educational interest under 34 C.F.R. § 99.31(a)(1)(i)(B), is under the Customer's direct control for the use and maintenance of those records, and will not re-disclose them except as FERPA allows.

5. Provider personnel

Provider limits access to Customer Data to personnel who need it to provide or support the Service, who are bound by confidentiality obligations, and who are trained on their security and privacy responsibilities. Provider staff don't view Customer Data except to provide support the Customer asks for, to keep the Service secure, or as the law requires.

6. Security measures

Provider maintains administrative, technical and physical safeguards appropriate to the risk, including reasonable safeguards under New York's SHIELD Act and similar laws. They include:

- **Encryption:** TLS for data in transit; encryption at rest for the database and backups through the hosting provider.
- **Tenant isolation:** each college's data is separated in the database by row-level security, so one college's queries can't reach another's data.
- **Authentication:** passwords stored as salted hashes; session tokens stored as hashes; passkeys and authenticator-app two-step verification, which a college can require for all its Users.
- **Access control:** roles (owner, analyst, viewer) with owner-controlled area permissions enforced on the server; the AI analyst can't read areas a User's role doesn't include.
- **Personal-information screening:** uploads are scanned and refused if they appear to contain personal information.
- **Logging:** uploads, restatements, role and permission changes, and assumption changes are recorded with who made them and when.
- **Least privilege:** production access is limited to authorized personnel using individual accounts with two-step verification.
- **Resilience:** automated database backups and the ability to restore them.
- **Vulnerability management:** dependencies are kept current, security fixes are prioritized, and independent penetration testing is performed at least yearly.

Provider may update these measures as long as the update doesn't lower the overall level of protection.

7. Subprocessors

The Customer authorizes Provider to use the subprocessors below. Provider has written contracts with each that protect Customer Data at least as well as this DPA, and remains responsible for their performance.

Subprocessor	Purpose	Data	Location
Render Services, Inc.	Application hosting, database and backups	All Customer Data and account data	United States
Anthropic, PBC	AI model behind the AI analyst	Questions, page context and the calculated results needed to answer them	United States
Google LLC (Google Workspace)	Company email for support and notices	Contact details and support correspondence	United States

Provider will update this list and notify account owners at least 30 days before a new subprocessor processes Customer Data. The Customer may object on reasonable data-protection grounds; if the parties can't resolve the objection, the Customer may end the affected subscription and receive a refund of prepaid fees for the remaining term.

8. Security incidents

Provider will notify the Customer without undue delay, and in any case within 72 hours, after confirming a breach of security that leads to unauthorized access to or disclosure, alteration or loss of Customer Data. The notice will describe what happened, the data and Users affected (as far as known), the steps taken, and a contact for more information, and Provider will update it as it learns more.

Provider will take reasonable steps to contain and fix the incident, cooperate with the Customer's investigation and any notices the Customer must give, and, where the incident was caused by Provider's breach of this DPA, reimburse the reasonable costs of notices the law requires. Notifying the Customer isn't an admission of fault.

9. Requests and assistance

If Provider receives a request from a person about their personal information in Customer Data, it will refer the person to the Customer and won't respond directly unless the Customer asks or the law requires. Provider will help the Customer respond to such requests, and to government or regulator inquiries, as reasonably needed. If Provider receives a legal demand for Customer Data, it will notify the Customer before disclosing, where the law allows, so the Customer can seek protection.

10. Return and deletion

When the subscription ends, the Customer may export its data for 30 days. Provider then deletes Customer Data from the Service within 60 days and from backups as they are overwritten, within 35 days after that, unless the law requires keeping it. On request, Provider will confirm deletion in writing.

11. Security reviews

Provider will answer the Customer's reasonable security questionnaires (such as the HECVAT) once a year and after a security incident, and will share its most recent independent security assessment or audit report, when available, under confidentiality. If those don't reasonably answer the Customer's questions, the parties will agree on a further review at a mutually agreed time, at the Customer's cost, no more than once a year.

12. Data location

Provider and its subprocessors store and process Customer Data in the United States. Provider won't move Customer Data outside the United States without the Customer's written consent.

13. General

This DPA lasts as long as Provider processes Customer Data. Each party's liability under it is subject to the limits in the Terms. Questions about this DPA: privacy@astrafpa.ai. To report a security concern: security@astrafpa.ai.

Colleges that need a signed copy, or their own data protection addendum reviewed, can write to legal@astrafpa.ai.