

Data Processing Agreement — Template

Navigate (Workforce Ascend). Template for review by your counsel. We will also sign your organization's own DPA, data-sharing agreement, or student data privacy terms.

1. Parties and roles

Your organization is the data controller. Workforce Ascend, operating Navigate, is the data processor and processes participant data only on your documented instructions.

2. Subject matter and duration

Processing covers the delivery of workforce program management: participant enrollment, assessment, progression, credentialing, employer referral, and outcomes reporting. Processing lasts for the term of the service agreement and any agreed wind-down period.

3. Categories of data and data subjects

Data subjects are program participants and program staff you invite. Categories processed:

- **Identity and contact:** name, email address.
- **Program data:** cohort membership, assessment responses, readiness scores, lesson progress, credentials issued.
- **Outcome data your staff enter:** employment status, employer, job title, wage, credential, retention checkpoints, employer referrals.
- No Social Security numbers, financial account data, or protected health information are collected, and the platform is not designed to store them.

4. Processor obligations

- Process personal data only on documented instructions from the controller.
- Ensure personnel with access are bound by confidentiality.
- Apply role-based access control, organization-level data isolation, and encryption in transit.
- Assist the controller with data subject access, correction, and deletion requests.
- Notify the controller without undue delay, and within 72 hours of becoming aware, of a personal data breach affecting the controller's data.

5. Subprocessors

Processing relies on managed cloud hosting and database services in the United States, a transactional email provider, and a hosted AI model provider used only for coaching features. A current subprocessor list is provided on request. The controller will be notified before a new subprocessor is engaged and may object.

6. International transfers

Data is hosted in the United States. If the controller requires processing in another region, that must be agreed in writing before contracting.

7. Security measures

- Authentication handled by a managed identity provider; passwords are never stored by Navigate.
- Row-level authorization scoping every record to a single organization.

- Separate administrator, instructor, and participant roles.
- Encryption in transit (TLS) and encryption at rest by the hosting provider.
- Audit of privileged database functions and least-privilege grants.

8. Audit and compliance status

Stated plainly: Navigate has not completed a SOC 2 audit and holds no third-party FERPA attestation or formal WCAG audit. The controller may request written responses to a security questionnaire and reasonable evidence of the controls described above. If a certification is a hard procurement requirement, raise it during scoping.

9. Return and deletion

On termination, the controller may export all participant, outcome, credential, and reporting data as CSV. On written request, Navigate will delete the controller's data within 30 days, except where retention is required by law.

10. Liability and governing law

Liability, indemnities, insurance, and governing law are set out in the master service agreement between the parties and are not modified by this template.

Signature block

Controller: _____

Name/Title: _____ Date: _____

Processor (Workforce Ascend):

Name/Title: _____ Date: _____