Alignify

Alignify Compliance Overview

Last Updated: 4/30/2025

---

1. Overview

Alignify is committed to protecting user privacy, maintaining data security, and supporting compliance with applicable regulations including FERPA, GDPR, and U.S. higher education standards. This document outlines our data handling, privacy, security, and compliance practices for institutions evaluating or implementing Alignify.

2. Hosting and Infrastructure

- - Cloud Environment: Alignify is hosted in a secure, U.S.-based cloud environment using Amazon Web Services (AWS).
- - Data Residency: All customer data is stored and processed within the United States.
- - Uptime: Infrastructure is monitored 24/7 and maintained with 99.9% uptime standards.

3. Data Security

- - Encryption:
-   - Data is encrypted in transit (TLS 1.2 or higher)
-   - Data is encrypted at rest using AES-256
- - Authentication:
-   - Role-based user access controls
-   - Optional two-factor authentication (2FA) support
- - Audit Logging: Activity logs track user actions, permissions changes, and data access for security review.

4. FERPA & Educational Records

Alignify is built to support compliance with the Family Educational Rights and Privacy Act (FERPA):

- - Institutions retain full ownership and control over student data.
- - Data is not shared, sold, or accessed by Alignify for non-operational purposes.
- - Privacy-by-design principles are embedded into development workflows.

5. GDPR (Where Applicable)

Although Alignify is U.S.-based, we honor privacy rights consistent with the EU General Data Protection Regulation (GDPR):

- - Users may request access to, correction of, or deletion of personal data.

- - Institutional customers are considered "data controllers" and Alignify acts as a "data processor."
- - Data Processing Agreements (DPAs) are available for clients upon request.

6. Access Controls and Permissions

- - Admin users can manage user roles, program access, and data visibility.
- - Permissions can be customized for faculty, coordinators, institutional researchers, and reviewers.
- - Export access is limited by role and recorded in audit logs.

7. Data Retention and Portability

- - Institutions can define their data retention and archival policies within the platform.
- - Upon contract termination, data can be exported in structured format (e.g., CSV, PDF) prior to secure deletion.

8. Third-Party Integrations

- - Alignify supports optional integrations with LMS and SIS platforms using secure APIs.
- - All third-party tools are vetted to meet equivalent data privacy and security standards.

9. Security Certifications and Practices

- - Regular vulnerability scans and security patching
- - Least-privilege principle applied to infrastructure access
- - Scheduled disaster recovery testing and data backups

10. Contact and Reporting

Questions about this compliance overview or requests for additional documentation (e.g., SOC 2 report, penetration test summary) may be directed to:

Email: compliance@alignifyplatform.com

This document is intended to support institutional due diligence and should be reviewed alongside your institution’s internal policies and risk frameworks.