Clover ERA: Security & Compliance

Enterprise-Grade Security for Employee Data

Our Commitment to Data Protection

Employee engagement data is sensitive. People share honest feedback about managers, workload, and team dynamics. Clover ERA is built on a foundation of security and privacy that protects both employees and organizations.

We understand that your security team needs specific assurances before approving any new platform. This document addresses the most common security and compliance questions we receive.

Security Architecture

Data Encryption

- All data encrypted in transit (TLS 1.3)
- All data encrypted at rest (AES-256)
- Encryption keys managed through AWS Key Management Service

Infrastructure Security

- Hosted on Azure infrastructure with SOC 2 Type II certification
- Multi-region redundancy for high availability
- Automated daily backups with 30-day retention
- Network isolation and firewall protection

Access Controls

- Role-based access control (RBAC) for all users
- Multi-factor authentication (MFA) available for all accounts
- Single Sign-On (SSO) integration via SAML 2.0
- Session management with automatic timeout
- Comprehensive audit logging of all system access

Application Security

- Regular penetration testing by third-party security firms
- Automated vulnerability scanning and patching
- Secure software development lifecycle (SDLC)
- Code review requirements for all production deployments

Employee Privacy & Anonymity

How Anonymity Works

Employee responses are anonymous by design, not by policy. Managers never see individual responses—only aggregated team data. This technical anonymity cannot be overridden by anyone, including administrators or Clover ERA staff. Cover ERA stores no personal information this includes device IDs.

Data Minimization

- We collect only the data necessary for engagement measurement
- No personal identifiable information (PII) linked to responses
- Responses aggregated at team level (minimum 5 employees)
- Small teams see aggregate data only when anonymity threshold met

Data Retention & Deletion

- Customer data retained only while account is active
- 30-day grace period after cancellation for data export
- Complete data deletion within 90 days of cancellation
- Right to deletion requests processed within 30 days

Compliance & Certifications

Standard	Compliance Details
GDPR *(EU Data Protection)*	Fully compliant with EU General Data Protection Regulation. Data processing agreements available. Data residency options for EU customers.
SOC 2 Type II *(In Progress)*	SOC 2 Type II compliant and ready. Currently operating under SOC 2 Type I controls. Audit reports available upon request under NDA.
CCPA *(California Privacy)*	Compliant with California Consumer Privacy Act. Employee data deletion rights honored. Opt-out mechanisms in place for data sharing.
HIPAA *(Healthcare)*	Not required for engagement data, but we maintain HIPAA-level security standards. Business Associate Agreements (BAA) available for healthcare customers.

Data Processing & Subprocessors

Clover ERA uses carefully vetted subprocessors for specific functions:

- Azure (infrastructure hosting, US-based)
- SendGrid (transactional email delivery)
- Stripe (payment processing, PCI DSS compliant)

Complete subprocessor list and data processing agreements available upon request.

Operational Security Practices

Employee Security Training

- All employees complete security awareness training
- Background checks required for all team members
- Strict confidentiality agreements and NDAs

Incident Response

- 24/7 security monitoring and alerting
- Documented incident response procedures
- Customer notification within 72 hours of any data breach
- Annual security audits and penetration testing

Business Continuity

- 99.9% uptime SLA guarantee
- Disaster recovery plan with documented procedures
- Regular backup testing and recovery drills
- Multi-region failover capability

Resources for Your Security Review

We understand your security team needs detailed documentation. Available upon request:

- Security questionnaire responses (CAIQ, SIG, custom)
- Data Processing Agreement (DPA) for GDPR compliance
- Business Associate Agreement (BAA) for healthcare customers
- SOC 2 audit reports (under NDA)
- Network architecture diagrams
- Penetration test results (under NDA)
- Incident response procedures documentation

Security Is a Foundation, Not an Add-On

We built Clover ERA with enterprise security from day one. Your employees trust us with honest feedback. We take that responsibility seriously.

Security questions? Contact: security@cloverera.com

General inquiries: contact@cloverera.com • Phone: (212) 918-4448