

Security and Data Protection Overview

A plain-language view of Cogran hosting, access controls, payment security, and data handling.

01 Understand the layers of protection

Cogran’s security model combines managed cloud infrastructure with application permissions, secure connections, restricted administration, and operational procedures. This overview explains those layers and the questions your organization should resolve during a security review.

Microsoft Azure hosting

Cogran uses Microsoft Azure hosting and SQL Server database services. Each client organization has its own database. Application and API services sit between public users and the database, with database access restricted to the application/API layer and authorized administrators.

Encrypted browser connections

Cogran’s documented browser-to-server connections require HTTPS with TLS 1.2 or higher. This protects information while it travels between the browser and the service. Encryption of stored data, files, backups, and external transfers should be reviewed for the specific deployment and requirements.

Infrastructure assurance and application assurance

Cogran is hosted on SOC 2-audited Microsoft Azure infrastructure. This describes the hosting environment. It does not establish a separate Cogran SOC 2 report or an independent audit of Cogran’s application controls.

Layer	Purpose
Azure infrastructure	Managed hosting and database foundation
Cogran application	Authentication, permissions, and controlled data access
Operational practices	Administration, support access, response, and recovery
Your organization	Staff authorization, collection policies, and secure daily use

02 Give staff the access their role needs

Role based permissions

Cogran security roles can restrict menus, forms, functions, and data. Client administrators can create groups that match staff responsibilities. Unique user identities support accountability, and access can be changed when responsibilities change or revoked when a person leaves.

Example role	Access to evaluate during setup
Counselor or instructor	Assigned participant and attendance information needed for the role
Front desk staff	Customer assistance and approved check-in/payment functions
Finance staff	Payment, refund, balance, and reconciliation information
System administrator	Configuration and permission management
Temporary staff	Limited functions for a defined period, followed by removal

These are planning examples. Verify the actual permissions and data visibility of each configured account.

Multi factor authentication

Optional code-based dual authentication adds a verification step to password sign-in. Production administrative access also has documented two-factor protections. If your organization requires MFA for every administrative or privileged account, review enforcement, recovery, and any exception paths during setup.

Single sign on

Enterprise SAML single sign-on is an available option. Confirm identity-provider compatibility, account provisioning, role assignment, sign-out and offboarding behavior, implementation work, and pricing. Test the proposed configuration before relying on it for a required access policy.

Production and support access

Cogran’s security documentation describes restricted production access, strong administrative credentials, IP restrictions, and authorized-device controls. Support access is limited to authorized needs such as resolving a customer issue. Review available access logging and evidence if your procurement requirements call for it.

03 Protect participant and payment information

Client information remains yours

Client organizations retain ownership of their information. Cogran's materials state that client data is not sold or rented. Access for support is limited to appropriate purposes such as issue resolution, client instructions, or legal requirements. Review the current privacy terms and service-provider arrangements for the complete processing scope.

Payment card data is handled by Stripe

Your organization authorizes its Stripe account. Stripe handles payment-card details, while Cogran keeps the transaction results and references needed for payment status and supported refunds. Cogran does not store credit card numbers in its database.

Payments use Stripe's PCI DSS Level 1-certified infrastructure. Stripe's certification applies to Stripe; it does not certify every customer workflow or provide an independent Level 1 certification of Cogran. Cogran has PCI-related materials available for review.

Make collection and daily use intentional

- ☐ Collect only participant and household information needed for the service.
- ☐ Decide which roles may see medical, emergency, and pickup information.
- ☐ Review consent, required forms, and retention with your organization's policy owner.
- ☐ Limit fields in downloaded rosters and store printed copies securely.
- ☐ Use an approved channel for sensitive files; avoid sending passwords or card details in support requests.
- ☐ Remove unneeded access when seasonal staff leave or roles change.

Plan for data export and retention

Agree what can be exported, in which formats, who can authorize an export, and how records will be handled when service ends. Confirm retention and deletion expectations for live records, documents, backups, and working copies. Export access and backup retention are separate questions.

04 Review response and recovery arrangements

Incident response and service recovery

Cogran maintains documented incident-response and disaster-recovery procedures. These address investigation, containment, restoration, communication, and follow-up. Recovery documentation describes layered backups and restoration of application and database services, with testing before service resumes.

Request the current plans and service terms to review notification triggers and timing, escalation contacts, availability commitments, and recovery expectations. A recovery plan describes intended actions; a recovery test provides evidence of how those actions performed.

Ask for or confirm	Why it matters
Current architecture and data locations	Understand storage, processing, backup, and support access locations
Subprocessors and data-processing terms	Identify which providers handle which information
MFA and SSO configuration evidence	Verify that required access policies can be applied
Encryption and access-log coverage	Understand which records and transfer paths are protected and auditable
Backup and recovery details	Confirm retention, recovery objectives, and recent testing evidence
Incident plan and service terms	Establish notification responsibilities and escalation
Relevant audit and testing evidence	Check scope, date, and applicability to the proposed service

Request a security review

Send your organization name, questionnaire or required documents, and procurement timeline to hello@cogransystems.com. If you are an existing customer reporting a suspected issue, contact support or your account representative promptly with a description and safe contact details.

Related materials: Cogran Security and Data Protection Brief; privacy and access-control policies; incident-response and disaster-recovery plans; service-level and retention documentation. See [security and compliance](#) for the current public overview.