TRUST PACK

How we hold your data.

How CLVR Benefits hosts, encrypts, governs, and shares the data you put in our hands: with the receipts that prove it.

LAST UPDATED	VERSION	CONTACT
May 21, 2026	**v1.27.2**	**trust@clvrbenefits.com**

QUICK FACTS

DATA RESIDENCY	**EU / EEA only**	Azure & AWS EU regions. No customer data leaves the bloc.
ENCRYPTION AT REST	**AES-256**	Azure storage encryption with platform-managed keys.
ENCRYPTION IN TRANSIT	**TLS 1.2+**	sslmode=verify-full for the app-to-db link; HTTPS enforced at the edge.
STAFF AUTHENTICATION	**MFA enforced**	No staff access to production without a second factor.
INCIDENT NOTIFICATION	**72 hours**	Documented breach process; reviewed after significant changes.
COMPLIANCE POSTURE	**GDPR aligned**	Vendors hold ISO 27001 & SOC 2 Type II. Records on request.

01

Authentication and Security

How we make sure the right people, and only the right people, get in.

Multi-Factor Authentication (MFA)

Enabled for all admin and staff accounts.

LIVE

Password policies

Aligned with the standards of the relevant provider (e.g., Microsoft for Azure accounts).

LIVE

Certificate and key rotation

All certificates and keys are rotated regularly, with many handled automatically by cloud providers. Manual credentials updated every 90 days.

LIVE

BankID integration

Stronger user authentication and identity verification in user application.

PLANNED

02

Data Hosting and Location

Where your data lives, and the certifications underneath it.

Primary infrastructure

CLVR Benefits runs on Microsoft Azure for virtual machines and managed storage.

LIVE

Database backup and file storage

Database backups and file storage managed through Amazon AWS S3.

LIVE

Geographic restrictions

All servers and data hosted exclusively within Europe. No customer data ever leaves the EU/EEA.

LIVE

Compliance certifications

Both Azure and AWS hold industry-leading certifications (ISO 27001, SOC 2, GDPR compliance).

LIVE

03

Data at Rest

How customer data is protected once it has landed in our systems.

Database encryption

All customer data encrypted at rest using Azure built-in storage encryption (AES-256 with platform-managed keys).

LIVE

Database backups

Automated every 24 hours, retained for 7 days. Stored in Amazon S3 with SSE-S3 server-side encryption.

LIVE

Application-level encryption

AES-GCM encryption for highly sensitive fields using keys in Key Vault.

PLANNED

04

Data in Transit

How traffic between you, our app, and our database stays sealed.

Network isolation

All app-database traffic restricted to internal network only. Postgres not exposed to internet; port 5432 blocked at Azure NSG.

LIVE

Database TLS connections

All application-database traffic uses TLS with full certificate verification (sslmode=verify-full).

LIVE

HTTPS enforcement

All web traffic encrypted using HTTPS.

LIVE

Secure cookies

All cookies set with HttpOnly, Secure, and SameSite=strict flags to protect session integrity.

LIVE

05

Data Governance

The paper trail, the retention rules, and the contracts behind the controls.

Records of Processing Activities (RoPA)

Documented internally in codebase and reviewed during each release cycle.

LIVE

Data retention policies

Deletion and anonymization rules documented internally and reviewed on each release cycle.

LIVE

Data Processing Agreements (DPAs)

Tracked internally with all third-party vendors; documentation exists and is maintained, pending formal signatures.

IN PROGRESS

06

Data Subject Rights

Your rights under GDPR, and how to exercise them with us.

Data subject request processes

Established processes for access, correction, deletion, and portability requests with 30-day response time. Contact trust@clvrbenefits.com (mailto:trust@clvrbenefits.com) for any requests.

LIVE

Privacy Policy

Our privacy policy page is available here (/privacy-policy).

LIVE

07

Sub-processors

The vendors we share data with to operate the service, and what each one is used for.

Amazon Web Services
aws.amazon.com

Cloud storage for uploaded files and encrypted database backups, hosted in EU regions.

EU regions ISO 27001 SOC 2

Microsoft Azure
azure.microsoft.com

Hosting infrastructure and the identity provider used for organisational sign-in (OAuth via Entra ID).

EU regions ISO 27001 SOC 2

Anthropic
anthropic.com

Optional AI receipt scanning and expense auto-approval. Only receipt images and category names are sent. Data is not used to train models.

EU routing SOC 2

PostHog
posthog.com

Product analytics used to understand and improve how the platform is used.

EU regions SOC 2

HubSpot
hubspot.com

Marketing CRM only. Holds leads captured on our website (form submissions, demo requests). No customer, employee, or payroll data is ever sent to HubSpot.

US (SCC) ISO 27001 SOC 2

08

AI and Automation

Where AI touches your data, and the guardrails around each surface.

AI receipt scanning

Optional feature for expense report uploads. When enabled by the company, receipt images are sent to Claude (Anthropic) for extraction of vendor, date, amount, and VAT. Only the receipt image and benefit category names are sent. No employee names, emails, or other personal data. We do not use your data to train models. We retain only what is necessary for the feature and for audit compliance. Companies can disable this feature in AI Settings.

LIVE

AI automated expense evaluation

Optional feature that evaluates wellness expense reports for automatic approval or decline. HR retains full oversight: every AI decision is visible with confidence scores and reasoning, and any decision can be reverted at any time. Expenses where AI confidence is below 85% are deferred to human review. All decisions are logged with a full audit trail.

LIVE

09

Product Security

How the code that runs your benefits gets built and shipped.

Secure source code access

Access restricted to authorized team members only. GitHub used with enforced account security.

LIVE

Version control and release process

Structured Git workflow (git-flow). All changes tracked, reviewed, and merged into dedicated branches.

LIVE

Environment separation

Separate development and staging environments ensure thorough testing before production deployment.

LIVE

Test data management

Test data carefully selected, anonymized, and managed to avoid sensitive personal information in non-production.

LIVE

Modern secure technology stack

Built with industry-standard web technologies, containerized infrastructure, and managed cloud services. Regularly updated with security patches.

LIVE

Dependency and package vetting

All external packages reviewed before adoption. Monitor for vulnerabilities and update promptly.

LIVE

10

Security Operations

Day-to-day operations: who can do what, what we log, and what happens when something breaks.

Access control
Internal access limited to authorized staff using principle of least privilege. Administrative access restricted.

LIVE

Secrets management
Credentials injected as environment variables, never committed to code or stored in plaintext.

LIVE

System patching
Regular patching of OS, Docker images, and PostgreSQL.

LIVE

Application-level monitoring
Real-time error detection and anomaly monitoring via PostHog.

LIVE

System-level monitoring
Postgres authentication logs, firewall events (UFW), and system security logs with alerts for suspicious activity.

PLANNED

Incident response plan
72-hour breach notification process documented internally, available on request, reviewed after significant changes.

LIVE

QUESTIONS?

Talk to a real engineer about your security review.

Send the questionnaire, DPA redlines, or whatever's holding up your review. You'll get answers and the relevant documents within a few business days.

trust@clvrbenefits.com

This pack is generated from the live Trust Center at https://clvrbenefits.com/en/trust. The web page is authoritative : if anything in this PDF differs from the live page, the live page wins.

Generated 2026-05-21 12:49 UTC · CLVR Benefits AB · Stockholm, Sweden