Security brief

VERSION 2.1 · 27 OCTOBER 2026 · 6 MINUTE READ

> Your software checks licences itself, so it never depends on our uptime. Each customer's signing key stays in AWS KMS hardware. Card numbers never reach us. Your data is encrypted, logged, and yours to export or delete.

01 Hosting

AWS EU (Frankfurt), with US (N. Virginia) on request. Enterprise can choose dedicated infrastructure in its own region. Every customer isolated with row level security, and signing keys locked to each customer.

02 Licences

Signed with Ed25519 over every field. Your software holds only the public key, so it can verify a licence but never create one. Every licence is matched to its payment every night, and every SDK gives the same answer, proven by public test vectors.

03 Signing keys

One key per customer, created and kept in AWS KMS hardware and never exportable, including by Veryion staff. Every signature logged. Keys rotate without breaking issued licences, and deleting a key requires a waiting period of at least 7 days.

04 Availability

Verification runs on the device. If Veryion is unreachable, licences keep working and check in later. Every service runs in two Availability Zones. Offline leases and air gapped licences supported.

05 Data

TLS 1.2 or higher in transit. AES 256 at rest with keys in AWS KMS, plus field encryption of licence keys and phone numbers with a key for each account. Enterprise can bring its own encryption key. Deletion on request or 30 days after the contract ends.

06 Access

Passkeys and two factor sign in for everyone. Single sign on (SAML and OIDC) from Business, SCIM on Enterprise. Role based permissions, and approval for any action that moves money.

07 Audit log

Who, what and when for every change, approval and export, in write once storage. Kept 1, 2, 3 or 7 years by plan. Exportable, and streamed to your SIEM on Enterprise.

08 Card data

Entered in the payment provider's hosted fields, never reaches Veryion. PCI DSS scope SAQ A.

09 AI assistant

Sara runs on Amazon Bedrock in our AWS region and sees only what the signed in user can see. Customer data never trains AI models. Money actions need a person's approval.

10 Compliance

UK and EU GDPR, PCI DSS SAQ A and Cyber Essentials in place at launch. Independent penetration test before launch. SOC 2 Type I audit in progress, SOC 2 Type II observation period started, ISO 27001 planned. Independent review of the licence cryptography, December 2026 to January 2027. Dates on the Trust Center.

11 Recovery and incidents

At most 5 minutes of data lost and back within 1 hour inside the region. Point in time recovery for 35 days, a daily backup copy in a second region, restores tested every quarter. On call engineer around the clock, and affected customers told within 72 hours.

12 Vulnerabilities

security@veryion.com. Reply within 2 business days. No legal action against good faith research. Every SDK version supported for at least 5 years, and customers warned within 24 hours of an actively exploited flaw.

Statuses shown as planned for launch day. Every figure in this brief is checked against the engineering plan and by our lawyer before it is published.