A trust posture you can hand to your CISO.

Decot is a contract lifecycle management platform for regulated teams. Documents are encrypted before storage, access is customer-controlled, and key actions are anchored on a public ledger so any party can verify the record without trusting Decot.

CURRENT TRUST STATUS

Certifications
Not yet formally certified against ISO 27001 or SOC 2. We say so plainly and will walk you through our controls on request.

Electronic signatures
Qualified electronic signatures (QES) via DigiCert — eIDAS-aligned and validate as trusted in Adobe Acrobat.

Network
Audit hashes are anchored on the Sui public ledger (currently Sui testnet).

Data protection
Built to GDPR principles, including support for data-deletion requests. The on-chain hash alone is non-identifying.

Encryption & storage
SEAL threshold encryption (AES-256). Documents live on Walrus as ciphertext; the storage layer never sees plaintext.

Due diligence
We answer security questionnaires in plain English, typically within two business days.

HOW WE PROTECT YOUR CONTRACTS

Encrypted with SEAL
Documents are encrypted with SEAL threshold encryption and stored on Walrus. The storage layer and any third party see only ciphertext.

Audit is independent
A SHA-256 fingerprint of key actions is anchored on the Sui public ledger. Any party can verify the chain of events without trusting Decot.

Access is yours to control
You decide who can open each contract and with what role; access is enforced by on-chain grants. Decot does not open your contracts on its own.

Data deletion on request
We support data-deletion requests in line with GDPR principles. The on-chain hash alone is non-identifying.

SUB-PROCESSORS — WHO CAN TOUCH YOUR DATA

Sui Foundation	Public-ledger network — sees: ciphertext hash, public account ID. Never plaintext.
Walrus / Mysten	Decentralised storage — sees: encrypted blobs. Cannot decrypt.
Cloudflare	CDN + DNS for decot.io and docs.decot.io.
Google Cloud	Application hosting (API, queues, encrypted metadata).
AWS Cognito	Identity & authentication — sees: the user's SSO claim / login identity.
Email (self-hosted)	Transactional email sent from Decot's own mail server on decot.io. No third-party email processor.
DigiCert	Qualified electronic-signature (QES) certificate authority for eIDAS-aligned signing.
Google / Microsoft	Sign-in (OpenID) issuers. Sees: the user's SSO claim at login.

This summary reflects Decot's current posture and is provided for evaluation. It is not a warranty or certification. For a security questionnaire or a data-processing agreement, contact us.