THE QUANTUM CLUB

TRUST & COMPLIANCE

Security & Trust Overview

EU-resident - GDPR-compliant - EU-AI-Act-aligned - your data is never used to train models.

This overview summarises how The Quantum Club protects customer and candidate data across Club OS: our compliance posture, security architecture, sub-processors, and AI governance. Every claim is sourced from controls that are in effect today, or is labelled with its honest, current state.

Last updated 2026-06-22

Generated 2026-06-26 - trust.thequantumclub.com

Data residency: European Union (AWS eu-west-1). Breach notification: within 72 hours (GDPR). Identity: passkeys, SSO (SAML 2.0 / OIDC), SCIM 2.0, MFA with step-up.

Compliance posture

We never claim an attestation we do not hold. Each framework below is shown at the state we can evidence today.

GDPR - in effect today

Compliant in-product: data-subject access, export, erasure and rectification; granular, affirmative consent; defined retention windows; 72-hour breach notification. A DPA is available now.

EU data residency - in effect today

Customer data is stored and processed in the European Union (AWS eu-west-1, via Supabase). No multi-region toggle - EU by default and by design.

EU AI Act - controls implemented; independent attestation on roadmap

Club AI is assistive; a human always makes the hiring decision. Assessments are screening-support only - never standalone selection. Designed to meet the transparency and human-oversight duties for hiring AI.

SOC 2 (Type II) - controls implemented; independent attestation on roadmap

Controls are implemented to the SOC 2 Trust Services Criteria (security, availability, confidentiality). An independent Type II attestation is on our roadmap; this page will publish the report and auditor when it completes.

ISO/IEC 27001 - controls implemented; independent attestation on roadmap

Our information-security management maps to ISO/IEC 27001:2022 controls. Formal certification is planned; we will publish the certificate and scope statement once issued.

ISO/IEC 42001 (AI) - committed; not yet started

The AI-management-system standard is the highest-leverage assurance for a hiring-AI platform. Pursuing certification is on our roadmap and will be evidenced here.

Security architecture

Defence in depth across identity, data protection, application and operational controls.

Identity & access

- Passkey-first authentication - WebAuthn with user verification; phishing-resistant by design.
- Enterprise SSO - SAML 2.0 and OIDC federation for partner organisations.
- SCIM 2.0 provisioning - RFC 7644 directory-driven joiner/mover/leaver with full audit trail.
- MFA + step-up (AAL2) - Multi-factor with enforced re-authentication for sensitive operations.

Data protection

- Encryption in transit - TLS 1.2+ everywhere; HSTS with preload.
- Encryption at rest - Database, storage and backups encrypted at rest (AES-256).
- Row-Level Security - Postgres RLS enforced across 100+ tables - tenant isolation at the database layer.
- Secrets management - No secrets in client code; service-role material is server-side only.

Detection & resilience

- Atomic rate limiting - Auth-aware, fail-closed limiter (per-account + per-IP) on every authentication endpoint.
- Anomaly detection - Continuous scan (every 5 min) for credential-stuffing, spraying, velocity and takeover patterns - alerting today.
- Account recovery - PBKDF2-hashed recovery codes; five recovery paths with anti-enumeration guarantees.
- Audit logging - Security-relevant events recorded to an append-only audit stream.

Sub-processors

Third parties that may process customer data, with purpose, region and Data Processing Agreement (DPA) status (GDPR Art. 28).

Supabase

Purpose: Database, authentication, file storage
Region: EU (AWS eu-west-1) - DPA in place

Cloudflare

Purpose: CDN, edge compute, DNS, WAF
Region: Global edge (EU-served) - DPA in place

Stripe

Purpose: Payment processing
Region: EU / US (DPF, SCCs) - DPA in place

Resend

Purpose: Transactional & lifecycle email
Region: EU / US (SCCs) - DPA in place

AI model providers (Anthropic, Google)

Purpose: Club AI features (matching, assistant)
Region: EU / US (SCCs) - DPA in place

PostHog

Purpose: Product analytics - consent-gated, off by default
Region: EU - DPA in place

AI governance

Club AI is assistive and accountable. Hiring AI is high-risk under the EU AI Act, and we design for it accordingly.

Your data is never used to train models

Candidate CVs, notes and meeting transcripts are never used to train or fine-tune public LLMs. Only internal, anonymised telemetry calibrates our own prompts.

A human always decides

Club AI is assistive. Match scores, summaries and recommendations inform people; they never make an automated hiring decision.

Hiring AI is high-risk - we treat it that way

The EU AI Act classifies recruitment AI as high-risk. We design for transparency (users know when AI is involved), human oversight, and against adverse impact.

Assessments are screening-support, not verdicts

Our assessments are positioned as observed work-sample evidence, never standalone selection or clinical/personality diagnosis.

AI sub-processors are named

The model providers behind Club AI are listed in our sub-processor table, with region and data-handling terms.

About this document

This overview is generated on request from the live Trust Center and reflects content last updated 2026-06-22. For the full security model, sub-processor list, DPA, and machine-readable trust summary, visit the Trust Center.
https://trust.thequantumclub.com