

Does Cyber Crucible comply with GDPR?

Short answer: Yes, by design rather than by policy. Content, credentials, encryption keys, and session tokens are never collected; analysis happens on the endpoint; Cyber Crucible acts as processor under a written DPA; and deployment options keep personal data inside the EU — or inside your own building.

Mapping to GDPR principles

- **Data minimization (Art. 5)** — the excluded-data list is enumerated, not described in generalities. Telemetry is limited to what threat detection requires and is configurable.
- **Integrity and confidentiality (Art. 5, 32)** — TLS 1.3 in transit, per-agent JWE payload encryption, encryption at rest, role-based access control, key rotation, audit logging.
- **Processor obligations (Art. 28)** — written DPA specifying scope; processing only on documented instructions; sub-processors bound to equivalent terms.
- **Transfers (Chapter V)** — EU regional staging, or air-gapped deployment that eliminates transfer entirely.
- **Data protection by design (Art. 25)** — the strongest claim available: the highest-risk categories are not protected by policy, they are never collected.

Pseudonymization

Where behavioural telemetry could indirectly identify an individual, identifiers are pseudonymized or masked — a safeguard GDPR explicitly recognizes.

What this does not do

It does not make your organization GDPR compliant. Your obligations depend on your own processing purposes, lawful bases, notices, and records. What it removes is a common difficulty: a security vendor continuously exporting personal data to a third country.