

Where is my data processed, and can it stay inside my country?

Short answer: Yes. Cyber Crucible infrastructure can be staged so processing occurs geographically close to or within your legal jurisdiction, and a fully on-premises air-gapped deployment keeps everything inside your own network boundary with zero outbound telemetry.

Sovereign staging

Infrastructure can be positioned to keep processing within — or geographically near — the customer's legal jurisdiction. This is designed to support compliance with data residency mandates including the EU General Data Protection Regulation (GDPR), Saudi Arabia's Personal Data Protection Law (PDPL), UAE Federal Decree-Law No. 45/2021, and the Kenya Data Protection Act.

The strongest option

For organizations requiring total isolation, the on-premises model runs all backend management software inside your own physically secured server racks. Zero telemetry and zero data leave your sovereign network boundary.

Because threat evaluation and process interdiction happen locally on the endpoint in typically under 200 milliseconds, protection does not depend on any external connection. Sovereignty costs nothing in defensive capability.

“ See also: *"What deployment models are available for data sovereignty?"*

Revision #2

Created 2026-07-21 18:59:38 UTC by Dennis Underwood

Updated 2026-07-21 19:32:49 UTC by Dennis Underwood