Does Cyber Crucible comply with Egypt's data protection law?

Short answer: Yes. Egypt requires prior approval for cross-border transfers of personal data — a materially higher bar than contractual safeguards. Cyber Crucible can be deployed so that no transfer occurs, removing the approval requirement rather than navigating it.

What the law requires

Egypt's data protection framework requires **prior approval** for transfers of personal data outside the country. That is a permission-based model rather than a safeguards-based one: you cannot simply put contractual protections in place and proceed.

Why the approval model changes vendor selection

Under a safeguards model, a vendor with strong contractual terms is workable. Under an approval model, every cross-border flow is an administrative process with timing, discretion, and renewal risk attached.

A security tool that continuously exports telemetry creates an ongoing flow requiring that approval to remain valid. If approval lapses or conditions change, the tool's normal operation becomes a compliance problem.

The straightforward answer

The air-gapped on-premises deployment produces zero outbound telemetry — nothing is transferred, so no approval is required. Regional staging keeps processing local where a hybrid model is preferred.

The categories most likely to attract regulatory attention — keys, credentials, tokens, file contents — are never collected regardless of deployment.

> Status at time of writing — confirm current requirements and approval procedure with local counsel.

Revision #2
Created 2026-07-21 19:00:10 UTC by Dennis Underwood
Updated 2026-07-21 19:33:16 UTC by Dennis Underwood