

Does Cyber Crucible meet Zambia's data localization requirement?

Short answer: Yes. Zambia's Data Protection Act requires controllers to process and store personal and sensitive personal data on a data centre or server **within Zambia**. Cyber Crucible's on-premises deployment satisfies this directly — the backend runs inside your own infrastructure, in-country.

What the law requires

Part X of Zambia's Data Protection Act regulates cross-border transfer, and Section 70 obliges a data controller to process and store personal and sensitive personal data on a data centre or server located within Zambia.

This is a **storage location mandate**, not a safeguards test. Contractual protections do not satisfy it.

Why this eliminates most cloud-based security tools

A vendor whose product requires shipping endpoint telemetry to a cloud region outside Zambia cannot meet Section 70 by improving its contracts or encryption. The requirement is about *where the data physically sits*.

Why this architecture satisfies it

- **On-premises backend** — all management software runs on servers you control, inside Zambia.
- **Local analysis** — threat evaluation and interdiction occur on the endpoint itself, so protection never depends on an out-of-country service.
- **Zero outbound telemetry** in the air-gapped configuration.

- **Minimal scope** — keys, credentials, tokens, and content are never collected, so the volume of personal data subject to Section 70 is small to begin with.

“ Status at time of writing — confirm with local counsel, including any sector-specific rules.

Revision #2

Created 2026-07-21 19:00:12 UTC by Dennis Underwood

Updated 2026-07-21 19:33:18 UTC by Dennis Underwood