Does Cyber Crucible comply with Kenya's Data Protection Act?

Short answer: Yes. Kenya's Data Protection Act 2019 restricts cross-border transfer to countries with appropriate safeguards, and applies a stricter rule to sensitive personal data. Cyber Crucible does not collect sensitive personal data at all, and can be deployed so that no data leaves Kenya.

What the law requires

Sections 48 and 49 of the Data Protection Act 2019 prohibit transferring personal data to a country lacking appropriate data security safeguards, with several permitted bases including adequacy.

The stricter rule that matters: transfer of *sensitive* personal data is permitted only where the data subject has consented **and** appropriate safeguards exist. Both conditions, not either.

Why the sensitive-data rule is the key point

That dual requirement is difficult to satisfy operationally — obtaining and evidencing individual consent for every affected data subject, on an ongoing basis, for a security tool.

Cyber Crucible sidesteps it: **no sensitive personal data is collected.** Not biometric, health, or genetic data; not data revealing racial or ethnic origin, religious belief, or political opinion. Telemetry describes system behaviour and security events, not personal attributes.

Where behavioural telemetry could indirectly identify an individual, identifiers are pseudonymized or masked.

Transfer

Regional staging keeps processing within Kenya. The air-gapped deployment produces zero outbound telemetry, so sections 48–49 are not engaged.

> Status at time of writing — confirm with local counsel.

Revision #2
Created 2026-07-21 19:00:07 UTC by Dennis Underwood
Updated 2026-07-21 19:33:13 UTC by Dennis Underwood