MetricLabs.

ENTERPRISE TECHNICAL BRIEF

GOVERNANCE & COMPLIANCE FRAMEWORK

Data Residency & Compliance Summary

A technical reference for Internal Audit, Information Officers, and IT governance review.

PREPARED BY

MetricLabs (Pty) Ltd

TARGET AUDIENCE

Audit, Risk & IT Leadership

PRIMARY REGULATION

POPIA (Act 4 of 2013)

INFRASTRUCTURE

Microsoft Azure / Fabric (ZA)

Data Residency & Compliance Summary

A technical reference for Internal Audit, Information Officers, and IT governance review.

> This document is written to be forwarded directly — to your Internal Audit function, your Information Officer, or your IT governance committee — without needing a meeting first. It sets out, plainly, where data lives, how access is controlled, and how MetricLabs' platform aligns with South Africa's Protection of Personal Information Act (POPIA).

1 Where Your Data Is Hosted

MetricLabs' platform runs on Microsoft Azure and Microsoft Fabric. Azure operates dedicated, physical data center regions inside South Africa — specifically South Africa North (Johannesburg) and South Africa West — live since 2019, with data genuinely stored at rest within the country, not merely routed through it.

For any specific engagement, MetricLabs confirms the exact Fabric capacity region and residency configuration as part of onboarding, and documents this in writing before any data is connected — so your team has a specific, confirmed answer for your specific environment, not a general industry claim.

Data is encrypted in transit and at rest as standard Azure infrastructure practice, and access to the underlying storage layer is restricted to the specific service identities the platform requires — not broad administrative access.

2 How Access Is Controlled

Every user's access to the underlying data platform is individually granted and independently auditable — not a shared login, and not an all-or-nothing permission model. Specifically:

- ✓ **Schema-Level Scoping:** Access is scoped at the schema level: reporting-layer access is separated from raw internal system data by design.
- ✓ **Auditable Permissions:** Each user's permissions are logged and reviewable — who can see what is a documented fact, not a guess.

- ✓ **Granular Revocation:** Access can be granted, restricted, or revoked per user, without affecting anyone else's access.
- ✓ **Backup & Recovery:** Backup and recovery follows standard Azure infrastructure practice, with recovery point and recovery time objectives confirmed and documented per engagement.

3 POPIA Alignment

MetricLabs' obligations here are specific, not general — mapped directly to the relevant sections of the Act:

POPIA Section	Requirement	How This Is Addressed
`Section 19`	Security measures on integrity and confidentiality of personal information	Individually controlled, auditable access; encryption in transit and at rest; hosted on Azure infrastructure with independent ISO 27001 and SOC 2 Type II certification.
`Sections 20-21`	Operator obligations — requires a written contract establishing security measures, with immediate notification of any suspected unauthorized access	MetricLabs acts as an Operator, governed by a written agreement per Section 21, processing data strictly on your instruction — never as an independent controller of it.
`Section 22`	Notification of security compromises, as soon as reasonably possible	A documented incident response process, with client notification committed to within 24 hours of any confirmed compromise.

4 What This Means For Your Governance Process

This summary is designed to answer the questions that typically stall a first conversation — not to replace a proper due-diligence process. For a full technical walkthrough, an actual review of the architecture, or a signed Data Processing Agreement specific to your engagement, MetricLabs will provide full documentation as part of a formal Enterprise engagement.

This includes, on request:

- ✓ A named sub-processor list specific to your engagement
- ✓ A completed security questionnaire in your organization's own format

- ✓ A walkthrough of the incident response process with your own IT or security team present

MetricLabs.

Ready to Review Your Architecture?

We welcome technical due-diligence. Book an architecture review or security walkthrough directly with our engineering team.

Request Technical Walkthrough

See the actual architecture and governance model directly, with your own technical team present.

Book Architecture Review

Need Specific Documentation?

Request our signed Data Processing Agreement (DPA), sub-processor list, or complete your internal vendor questionnaire.

Request Vendor Pack

WEBSITE

metriclabs.co.za

DIRECT EMAIL

info@metriclabs.co.za

HEADQUARTERS

2 Ncondo Pl, Umhlanga Ridge
Durban, 4319, South Africa