De[*Jure*; **Facto**]: Data Governance in the Age of Cloud Computing

Nairobi, KE ForumX 2026

netcb ForumX

Keynote Speaker: Background

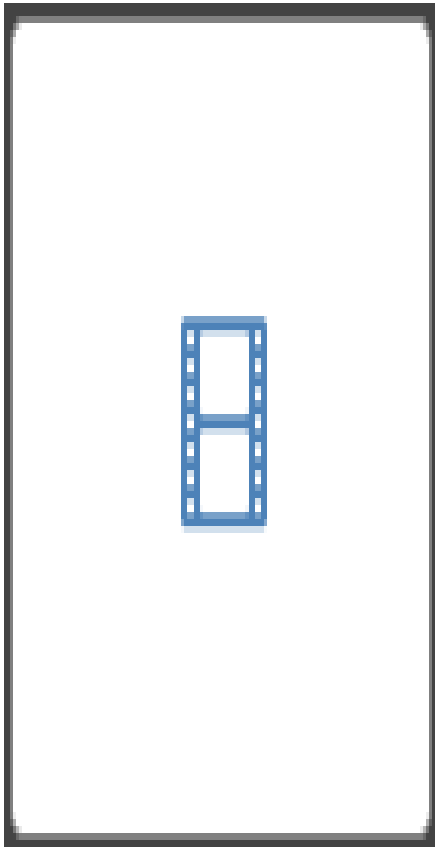
- Mr. Keith Takunda Chatsauka – Fellow and Director of Innovation, Cyberlaw, Cybersecurity and Compliance at NETCB ZA (Pty) Ltd:
  - Expert in data governance, information security, and compliance, with extensive experience delivering government and private-focused training and symposia across Southern Africa.
  - Qualifications: B.Sc Mathematics and Information Systems (RSA – in progress); Bachelor of Laws [L.LB](Cum Laude) from the University of South Africa, and a plethora of industry certifications from ISC2 (CC[SM]), OpenText [Zenworks, Identity and Access Management], Wazuh [Systems Administrator], AWS[Certified Cloud Practitioner] in addition to certificates from the Queen Mary University of London (Cloud Computing Law specialisation) Duke University [FinTech Law and Policy], the University of London[Applied Cryptography] and the University of Colorado [Network Design and Implementation].
  - Academic honours/recognition: **Postgraduate Merit Award recipient (2024)** at the University of the Witwatersrand, where he became the **first in South Africa to undertake intersectional studies which merge Cyberlaw and Cybersecurity** as a subset of National Security Studies during his Master of Laws studies, which focused on Cloud Computing regulation in the Public Sector.
  - **Fellow and Advisor at WeThinkCode_**, a South African company which focuses on upskilling the youth through teaching them how to code and become budding entrepreneurs through apprenticeships and a robust incubator program, which is this month's spotlighted Tech Innovator in Africa by **CNN International (U.S.A) – February 2026**.
- Finally, Mr Chatsauka is the only academic in the Southern Hemisphere who works with OpenSSL on cryptographic standards, serving as an academic voting delegate for the University of Cape Town, in addition to his work focused on protecting Quantum Technology Intellectual Property Rights in conjunction with the South African Quantum Technology Initiative (SA QuTI). Mr Chatsauka is also a member of the International Association of Cryptologic Researchers, focusing on Post Quantum Resilient Cryptography.

Goal of the Keynote

- To move the audience from seeing compliance as a checklist to understanding it as a dynamic, strategic framework that is essential for both security and business resilience in the cloud computing era.

Subtitle: From Policy to Practice – Aligning De Jure Obligations with De Facto Realities in a Hyper-Connected World

Primer: United States V.P Kamala Harris on SaaS usage and Security



Picture this scenario: "Imagine your company's customer data, stored in a cloud server in Nairobi, or Mombasa — or is it Frankfurt?— is breached. The Board asks two questions: 1) Are we secure? 2) Are we compliant? Your answer determines your company's future."

- The Duality of the Problem:

  The Promise: Agility, scalability, and innovation driven by cloud adoption.

  The Peril: Expanding attack surface, complex data flows, and a tangled web of legal obligations.

  Core Frameworks: the two lenses for the talk:

  De Jure: The "Law of the Land" – what the statutes and regulations demand.

  De Facto: The "Law of the System" – what your contracts, shared responsibility model, and technical configurations actually enforce.

- Roadmap: "In the next hour, we will map the Kenyan legal landscape, dissect the operational realities of the cloud, and build a blueprint for unifying these duelling realities."

- Objective: To clearly define the sources of legal obligations for any Kenyan organisation with operations that are cloud-based; be they localised or otherwise.

  A. The Cornerstone: Data Protection Act 24 of 2019

  Conditions for Processing: Our focus is on Security Safeguards (Integrity & Confidentiality), Information Quality, Accountability, and Cross-Border Transfers of P.I.I and P.H.I .

- Cloud Implications: The Data Protection Act , 2019 mentions "cloud" explicitly, and applies universally. The responsible party (you) remains accountable, even when using an intermediary (cloud provider).

DATA SOVEREIGNTY & LEGAL RISK IN CLOUD DEPLOYMENTS

Primary Law Applied:

- Data Protection Act, No. 24 of 2019

- Why this is primary:
  - Every major advisory (PwC, Deloitte, KPMG Kenya) and the Office of the Data Protection Commissioner treat data location and cross-border transfer as the single biggest cloud compliance risk.
- Key clauses:

  Section 25 – Obligation to ensure lawful, fair, and transparent processing

  Section 26(c) – Data controllers must implement appropriate technical and organisational measures

  Section 48 – Cross-border transfers of data • Allowed only where:
- Permissible: Adequate data protection in place; Explicit consent or safeguards are in place
- Directly governs cloud region selection, backup location, Disaster Recovery sites
  - Section 48(1) – Jurisdictional exposure via foreign processors
  - Section 56 – Joint liability of controllers and processors
- Cloud vendors are not absolved of legal responsibility – and neither are you!

DATA SOVEREIGNTY & LEGAL RISK IN CLOUD DEPLOYMENTS II – *Okiya* Case Study

Primary Law Applied:

- Data Protection Act, No. 24 of 2019

- **Permissible:** Adequate data protection in place; Explicit consent or safeguards are in place
- Case Study: *Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 Others* (2020 eKLR)
- **Facts:** The petitioner challenged the rollout of the National Integrated Identity Management System (NIIMS/Huduma Namba), arguing that biometric and demographic data was being collected and centralized without adequate legal and regulatory safeguards for data protection.
- **Held:** The Court held that although NIIMS could proceed, sufficient data protection safeguards and regulatory frameworks had to be operational before full implementation, emphasising constitutional privacy rights under Article 31.
- **Relevance to IT Governance:** Large centralised or cloud-hosted systems must implement clear safeguards before deployment, especially when processing sensitive personal data, such as P.I.I or P.H.I.

B. Secondary Law :

Data Protection (General) Regulations, 2021

- Regulation 16–18: Data localisation, transfer impact assessments

- **Risk assessment = Mandatory before cross-border transfers are permissible, and do not expose an organisation within the Republic to potential fines and more serious sanctions for non-compliance**
- **Case Study:** *Coalition for Reform and Democracy (CORD) v Republic of Kenya* **(2015 eKLR)**
- **Facts:** The petition challenged amendments expanding state surveillance and interception powers, arguing infringement of privacy rights.
- **Held:** The Court upheld parts of the law but emphasised proportionality and constitutional safeguards when interfering with private communications.
- **Relevance to IT Governance:** Cross-border cloud hosting may expose data to surveillance laws; proportionality and risk assessment are critical.

Jurisdictional exposure and cross- border flows are governed through:

Computer Misuse and Cybercrimes Act, 2018

Section 66 – Extra-territorial jurisdiction

Extra-territorial effect of Kenyan law applies where:

Kenyan citizens are affected

Kenyan systems or data are involved

- NB: Even foreign cloud breaches may trigger Kenyan enforcement

<u>REGULATORY EXPECTATIONS</u>

The ODPC requires:

Data Processing Agreements (DPAs)/Addenda where the cloud contract is reduced to an SLA

Transfer Impact Assessments (TIAs)

- Audience question: What happens in cases where there is no SLA?

- NB: Audit rights over cloud providers are essential to compliance!

Foundational Law:

- Constitution of the Republic of Kenya, 2010
  - Relevant Article(s): 31(c) & (d) – Right to privacy & protection of personal information
- **Potential pitfalls:** Failure to manage cloud data sovereignty -

  Exposes organisations to administrative fines;

  Creates regulatory investigation risk; and

  Invalidates cloud contracts if transfer safeguards are absent.

V. Part 1: The De Jure Landscape - The Kenyan Rulebook (15 mins)

Summary: The preceding discussion is the non-negotiable baseline. Ignorance is not a defence.

Objective: To expose the often-hidden or misunderstood operational obligations that exist in the cloud environment.

A. The Shared Responsibility Model: The Great Delusion?

The Provider's Wall: Security of the Cloud (Physical infrastructure, hypervisor).

Your Minefield: Security in the Cloud (Your data, configurations, access controls, network security groups, encryption keys, IAM policies).

The Critical Point: The cloud provider is responsible for the security of the cloud, not the security of your stuff in the cloud. Most breaches occur due to misconfigurations in the customer's area of responsibility.

The Contractual Web: SLAs, Terms of Service, and DPAs

These documents define your de facto rights, remedies, and limitations.

- **Where is your data stored? (Data residency vs. sovereignty)**

  What are the provider's obligations in a breach? What are your notification duties to them?

What sub-processors do they use? (A DPA requirement)

- Under the DPA, 2019:

Sub-processors are bound by Kenyan law and must comply with:

- Section 25–26: **Security**
- Section 56: **Processor obligations**

C. Technical Debt & Shadow IT

The "move fast and break things" culture can lead to ungoverned, poorly secured cloud deployments (*de facto* risk).

Business units spinning up SaaS applications without IT oversight, creating invisible data silos and compliance gaps.

Summary: Your *de facto* posture is defined by contract law, configurations, and culture, not just intentions. This is where theory meets practice—and often breaks down.

Objective: Provide a practical, actionable framework for bridging the *de jure* vs. *de facto* gap.

The Pillars of Unified Cloud Governance:

1. Data Discovery & Classification (The Foundation):

   Tool: Automated tools such as Wazuh or other SIEMS can be used to track all data across cloud environments – i.e., through the use of File Integrity Monitoring

   Action: Classify data based on sensitivity (e.g., public, internal, confidential, regulated) as required by the DPA. You can't protect what you don't know you have. This requires policy creation and enforcement within the modern Kenyan enterprise/organisation.

2. Policy as Code (Automating *De Jure*):

   Concept: Translate legal and security policies into automated, enforceable code - LegalTech.

Example(s): Enforcing a rule that automatically encrypts any data store tagged as a repository containing P.I.I/P.H.I; Making use of products such as SecureAnyBox that create an audit trail when accessing sensitive information stored inside a safety box.

3. Continuous Compliance Monitoring:

Move from: Point-in-time audits (for the regulator).

Move to: Real-time dashboards showing compliance status against DPA, 2019; Using CIS Benchmarks to ensure continual compliance..

4. Identity as the New Perimeter:

Strict enforcement of Principle of Least Privilege (PoLP) via Identity and Access Management (IAM).

Mandatory Multi-Factor Authentication (MFA) for all privileged access—a non-negotiable control;

- Making use of Identity Reporting to ensure that accounts that are no longer in use are removed according to internal audit requirements.

5. Incident Response Rehearsal in the Cloud:

Your IR plan must account for the cloud shared responsibility model. Who do you call at the provider? What logs are available to you? Practice a breach scenario with your cloud environment – thereby simulating the procedure to be followed once an incident is actually flagged.

Recap: The journey is from reactive compliance (*de jure* checklist) to proactive cyber resilience (aligning *de jure* with *de facto*).

The Stakes: In Kenya, the cost of non-compliance is no longer just a fine; it also comprises of reputational damage, loss of customer trust, and direct criminal liability under the Computer Misuse and Cybercrimes Act, 2018.

Final Call to Action:

1. **Audit**: Conduct a gap analysis between your *de jure* obligations (DPA, etc.) and your *de facto* cloud configurations, as well as reality.
2. **Empower**: Appoint a multi-disciplinary team (Legal, Compliance, IT, Audit) to own and decide how best your organisation can leverage and implement cloud governance.
3. **Automate**: Leverage cloud-native tools to enforce policy and maintain continuous compliance. As Kenya is technology-agnostic, leverage open source solutions such as Wazuh to maximise the positive outcomes that can result from automation.

Closing thought; Q&A (5 Min)

"In the cloud, your security and compliance posture is not a document. It is your configuration, and adherence to policy and procedural implementations. Make it count."

Contact NETCB to see how best we can assist you on your compliance and cybersecurity journey. Thank you for your time!