

BEYOND THE LAWS IN DATA PROTECTION & PRIVACY

**From Legal Frameworks to Effective
Enforcement**

**Data Protection Commissioner, Mauritius
President, AFAPDP
Co-Chair, Common Thread Network
Chair, AU Data Governance Committee**



Framing the Challenge

- Rapid growth of data protection laws across Africa
- Persistent gap between legislation and enforcement
- Expanding digital identity and data ecosystems
- Next decade focus: operationalising data protection





The Reality Gap

- **Laws \neq compliance**
- **Compliance \neq accountability**
- **Accountability \neq enforcement**
- **Drivers: limited capacity, technical gaps, fragmented governance**



Enforcement Challenges

- Under-resourced Data Protection Authorities (DPAs)
- Limited specialised technical units
- Weak coordination with regulators, CERTs and law enforcement
- Constraints in applying sanctions and follow-through

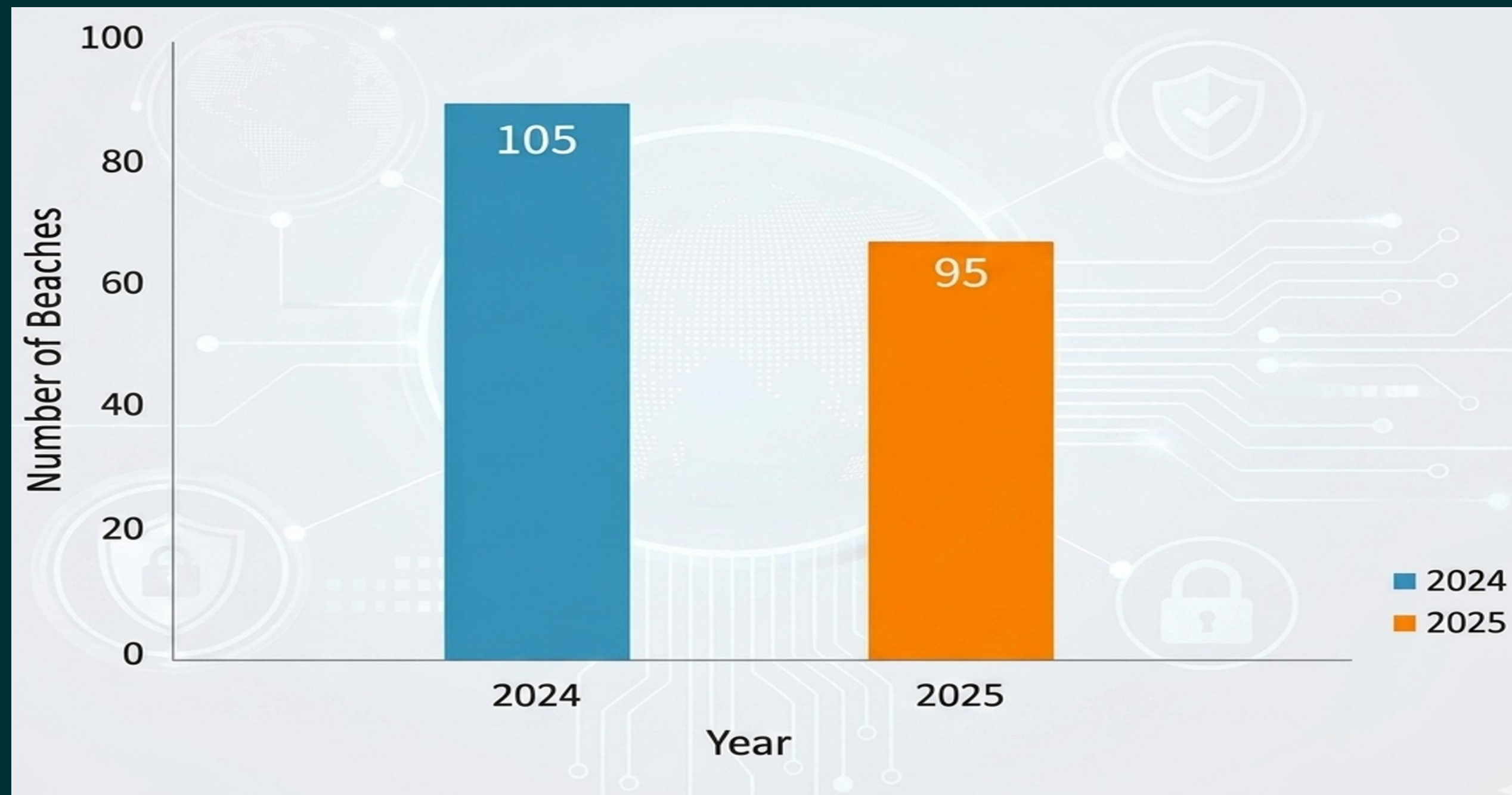



Rising Data Breaches

- Increase in reported personal data breaches
- Common incidents: email errors, unauthorised disclosures, system vulnerabilities
- Investigations becoming more technical and complex

Mauritius Case Insights – Reported Data Breaches

Mauritius reported Data Breaches: 2024 vs 2025





Evidence & Investigation Challenges

- Difficulties in digital evidence collection and attribution
- Cross-border data flows complicate investigations
- Limited forensic tools and skilled investigators
- Enforcement without evidence is ineffective

Digital Forensic Laboratory: From Incident to Enforcement



Establishment of a Digital Forensic Laboratory to support evidence preservation, investigation and prosecution.



Key Aspects Beyond Legal Compliance:

- Ethical Data Stewardship
- Privacy by Design/Default
- Privacy Enhancing Technologies (PETs)
- Data Ethics and Transparency
- Collective Data Governance
- Data Minimization
- Trust as a Brand Value



Data Protection & Trust Economy

- Trust enables data sharing
- Supports digital identity
- Drives economic value
- Adoption of a National Data Strategy

Proactive Data Stewardship

Organizations are increasingly adopting "Stewardship" models where data is treated as an asset held in trust:

Data Trusts: Legal structures where a third party (the trustee) manages data on behalf of a group of people, ensuring it is only used for agreed-upon purposes, such as medical research.

Incentive Alignment: Leading brands like LEGO have built their business models around ethical data use as a **competitive advantage**, specifically by refusing to use third-party cookies on sites aimed at children.

Ethical Frameworks: The "Should" vs. the "Can"

Algorithmic Fairness: Actively testing AI for biases that could lead to discriminatory outcomes in hiring, lending or policing.

Data Minimization & Deletion: Moving away from "data hoarding" by strictly defining how long data is useful and ensuring it is permanently erased afterward.

Transparent Explainability: Moving beyond 50-page legal terms of service to layered notices or visual icons that clearly explain how data flows through a system.

Data Ethics Board/ Data Governance Committee

A Data Ethics Board or Data Governance Committee is a cross-functional group that reviews data use cases through an ethical lens rather than a purely legal one

- **Define the Mandate**

Select Diverse Members with diverse perspectives beyond IT and legal.

Internal: Include representatives from product, engineering, customer success and legal.

External: Consider independent ethicists, industry experts, or representatives from affected communities to avoid "groupthink".

- **Establish a Review Framework**

- **Formalize the Process**

- **Authority and Transparency:**

Define whether the board's decisions are binding or advisory. Publicly sharing their guiding principles builds external trust.

Data Ethics Board & Data Governance Committee

National Data Governance & Ethics Council (*Central Coordinating Structure*)

Core Members

Data Protection Authority

National AI Authority

CERT & Cybersecurity Authorities

Sector Ministries & Public Agencies

Private Sector & Academia

Legal, Ethics & Civil Society Representatives

Key Functions

- Ethical AI oversight and responsible data governance
- Data classification, interoperability and harmonisation
- Oversight of secure data sharing and privacy compliance
- Governance of AI, analytics and emerging technologies
- Strengthening transparency, accountability and public trust
- Alignment with the National Data Strategy

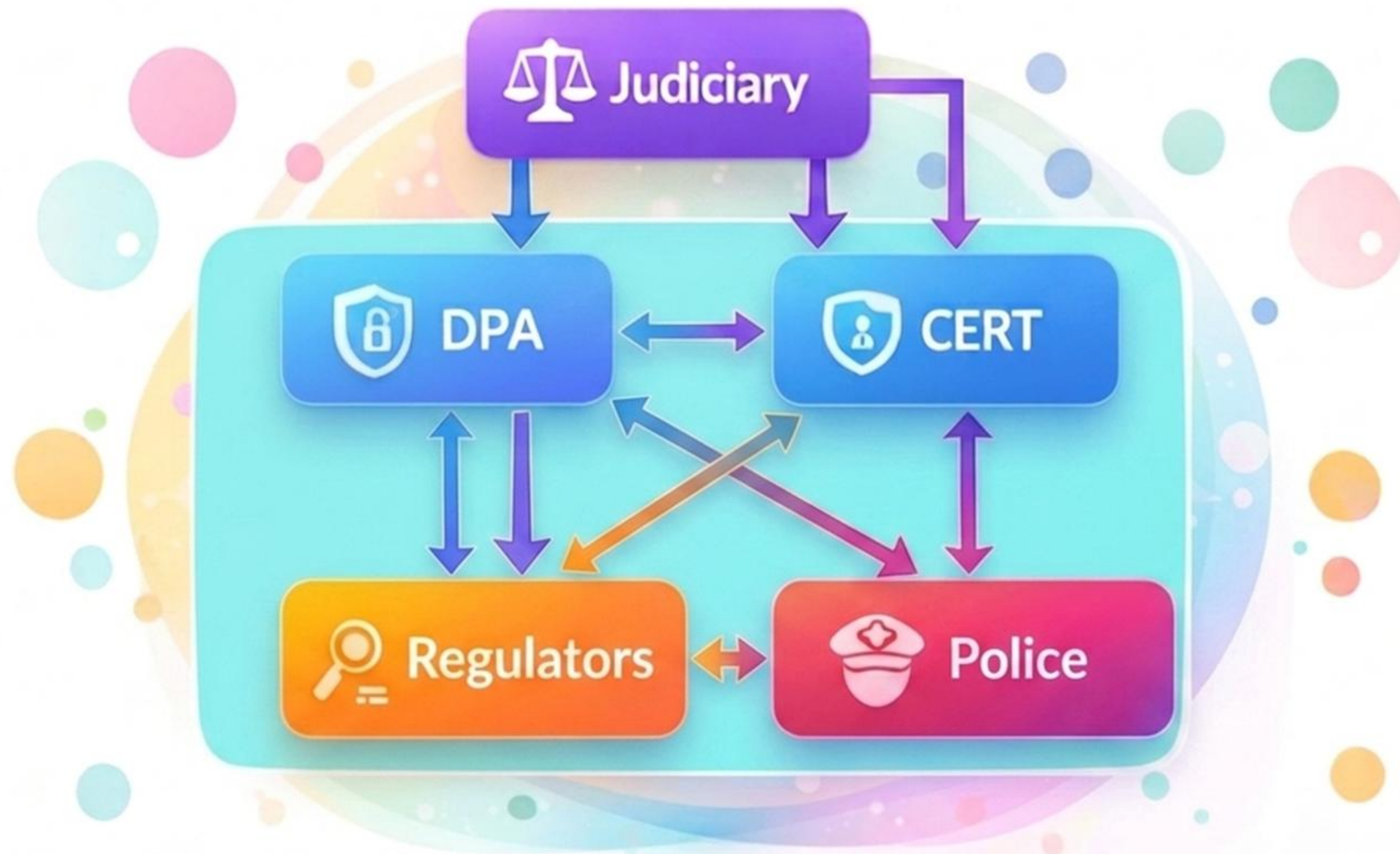
Strategic Outcomes

- Trusted digital ecosystem
- Responsible and ethical use of data
- Improved inter-agency coordination
- Secure and privacy-centric innovation
- Enhanced national data governance maturity

For example, the Mauritius National Data Strategy 2025–2029



Enforcement Ecosystem (Coordination)



No single authority can enforce alone — structured cooperation is essential.

Strengthening the Enforcement Ecosystem



- Legal and financial empowerment of DPAs
- Development of technical capabilities (audits, forensics)
- Formal cooperation frameworks (MoUs)
- Operational collaboration across institutions



Sector-Specific Regulation

- Generic laws are insufficient for high-risk sectors
- Need for tailored guidance and clear standards
- Example: Mauritian financial sector and data protection guidance

Capacity Building: The Missing Link

- Human capacity is central to compliance
- Need for structured training frameworks
- Bridging the skills gap in organisations





Top 5 Actions for Governments

- Invest in DPA capacity (financial and technical)
- Establish digital forensic capabilities
- Strengthen inter-agency coordination
- Develop sector-specific frameworks
- Institutionalise DPO training and certification

From Law to Practice: Compliance Tools

- Publication of guidelines and codes of practice
- Use of templates (DPIA, data sharing agreements)
- Improved clarity, consistency and accountability



Professionalising Data Protection Officer



**DPOs as compliance
leaders and
accountability
anchors**



**Example: Upcoming
regulations
formalising the DPO
role in Mauritius**



**Increased
organisational
responsibility and
oversight**

Digital Training Platforms

- Scalable online training for DPOs and staff
- Continuous professional development
- Standardisation and accessibility across sectors



Next Frontier of Enforcement



AI risks



**Cross-border
data**



**Cloud
sovereignty**

Interactive Question

What are the biggest barriers to effective enforcement?

- A. Capacity**
- B. Legal framework**
- C. Coordination**
- D. Political support**

Roadmap (2026-2030)

Phase 1: Institutional strengthening

Phase 2: Technical capability development

Phase 3: Sectoral regulation and enforcement
scaling

Phase 4: Regional and cross-border
cooperation



Closing Message



- Africa has built strong legal foundations
- The next step is operational enforcement
- Data protection must move from compliance to confidence

**THANK
YOU**

**Questions
&
Discussion**