AFRICERT EXPERT BRIEFING

Challenges and Opportunities for African Companies in a Unique and Evolving Data Protection Landscape: The Essential Role of the DPO

Desmond Israel, Esq. CISSP, CIPM

Desmond Israel, Esq
CISSP, CIPM, CC, CCT
Partner, AGNOS Legal Company
Lecturer, GIMPA Law School

PROFILE

- **Partner (Cyberlaw and Technology Practice), AGNOS Legal Company**
- **Lecturer, GIMPA Law School**
- **Lead Consultant, Information Security Architects Ltd**
- **Training Consultant, National Banking College**
- **Non-Executive Director, Zerone Analytiqs (Canada)**
- **Member, EC-Council BETA Testing Committee (United States of America)**
- **Volunteer, ISC2 Exam Development**
- **Research Lead, XRSI Guardian Safety Framework (California)**
- **Former Research Fellow, Center for AI and Digital Policy (Washington DC)**
- **Alumni LLM'23, The George Washington Law School (Washington DC)**

What we will look at...

- **PART I: The Evolving Data Protection Landscape in Africa**
- **PART II: The Role of the DPO in this Ecosystem**
- **PART III: What Organizations Should Do Now**

Introduction

Context:
Africa's **digital transformation** is accelerating across sectors—e-commerce, banking, e-government, fintech.

Focus:
As data becomes a strategic asset, the **Data Protection Officer (DPO)** is pivotal for trust, compliance, and innovation.

Kenya Revenue Authority (KRA) Data Breach (2019)
In March 2019, the Kenya Revenue Authority (KRA) experienced a data breach that exposed taxpayer data. The breach exposed sensitive taxpayer information, including names, IDs, email addresses, and phone numbers.

South African Information Regulator Data Leak (2021)
In May 2021, the South African Information Regulator suffered a data leak that exposed the personal information of individuals who had filed complaints against organizations for violations of the Protection of Personal Information Act (POPIA). The breach exposed sensitive data, including names, addresses, contact details, and complaints.

PART I: The Evolving Data Protection Landscape in Africa

Legal and Regulatory Evolution

Regional Highlights:

African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) – slow ratification.

National Laws: Ghana (Act 843), Nigeria (NDPR), Kenya (Data Protection Act 2019), South Africa (POPIA) etc.

Trend: Shift from aspirational to enforcement.

Data Protection Maturity Gaps

Challenges:

- Lack of harmonization across jurisdictions.
- Inadequate capacity in enforcement institutions.
- Low organizational awareness or budget prioritization.

Opportunity: Building continental consensus on principles like consent, breach notification, cross-border data flow, etc.

Regulatory Pressure vs. Business Value

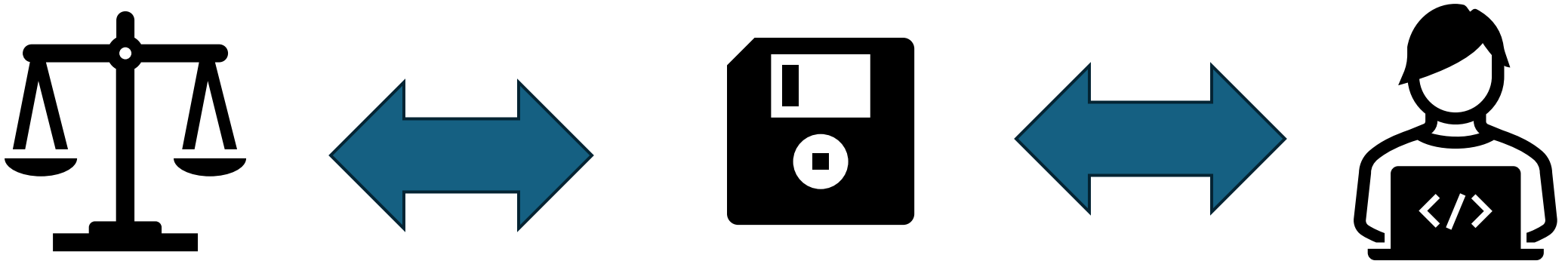
Challenge: Many African companies still treat data protection as a legal burden.
Opportunity: Reframe compliance as a **value proposition** for:

- **Investor confidence** (especially foreign investment).
- **Customer trust**.

Operational resilience (cybersecurity/data governance overlap).

PART II: The Role of the DPO in this Ecosystem

Explaining the Correlation



Data Privacy is guaranteed under law

Data Protection is a collection of administrative and technical controls to ensure data privacy

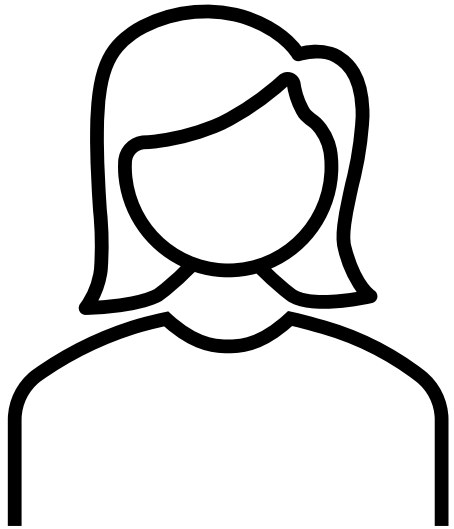
Data Protection Officer (DPO) ensures the compliance

Who is a Data Protection Officer (DPO)?

Definition (Global Norms): An **independent**, senior-level function responsible for monitoring data processing and advising on obligations. The role is usually **mandated under data protection regulations.**

Scope:

- Legal compliance
- Risk management
- Stakeholder training
- Liaising with regulators



Essential Responsibilities of the DPO

Advisory Role:
Data Protection Impact Assessments (DPIAs)
Privacy by Design & Default

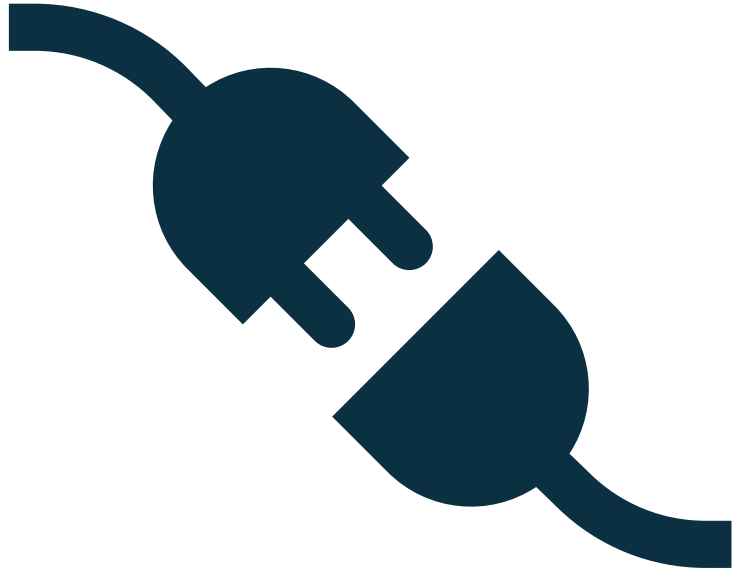
Monitoring Role:
Internal audits
Policy enforcement

Bridge Role:

Connecting IT, legal, HR, marketing, and external stakeholders.

Challenges Facing DPOs in Africa

- **Institutional Issues**:
  Under-resourced functions
  Lack of executive buy-in



- **Cultural Barriers**:
  Low privacy literacy among staff

- **Legal Complexity**:
  Navigating overlapping domestic and international data flows

The DPO as a Strategic Asset

DPO not just a **“compliance cop”:**

- Enables safe digital innovation (e.g., mobile payments, health tech)
- Positions company for cross-border business

Guides ethical AI, big data analytics, and data monetization strategies

Opportunity Spaces for African Businesses

- **Startups and SMEs**:
  Integrate privacy by design early (cheaper and reputationally valuable)

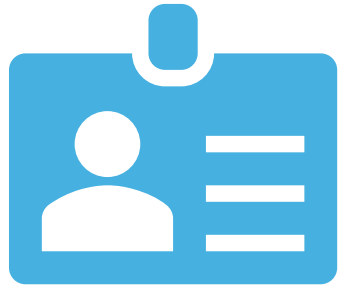
- **Banks/Telecoms/InsurTech**:
  Leverage DPO for cross-jurisdictional compliance frameworks

- **Cross-border trade (AfCFTA context)**:
  Unified privacy posture can facilitate seamless digital commerce.

PART III: What Organizations Should Do Now

Practical Steps to Empower DPOs

- **Board-Level Endorsement** – elevate the DPO to decision-making status.
- **Resourcing** – tech tools, legal budget, training.
- **Organizational Privacy Culture** – embed privacy into onboarding, product dev, procurement.
- **Cross-functional Working Group** – DPO as convener.



Capacity Building for DPOs

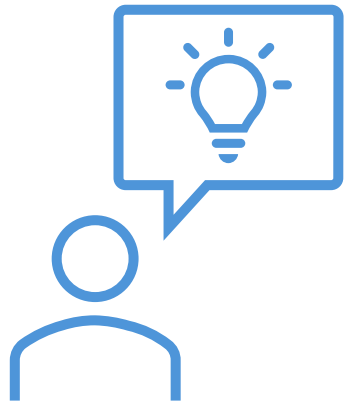
Invest in:

- Domestic training requirements. (regulations, compliance, technical implementation etc)
- International certifications (CIPP/E, CIPM, CDPO-Africa)
- Sector-specific awareness (e.g., health, fintech, telecom)
- Peer-learning forums and national associations

Final Thoughts

Africa is not playing catch-up—it's writing its own privacy narrative.

The **DPO is central** to navigating risk, seizing opportunity, and building trust in a data-driven economy.



The time to act is now.

THANK YOU

+233244284133
www.desmondisrael.legal
desmond.israel@gmail.com