COUNTERING THE DATA PROTECTION CHALLENGES IN THE AFRICAN REGION

INTRODUCTION

Sophisticated cybercrimes and digital espionage are rising in Africa due to various countries' financial and economic growth. Every modern business across the African continent uses digital collaboration to fuel business growth. Through this collaboration, they unknowingly place their valuable digital assets, such as intellectual property, customer data, financial information, etc., at greater risk due to the mishandling of sensitive information, data theft, and cyber-attacks. While data breaches can occur anywhere in the world, they are particularly prevalent in Africa due to the continent's lack of established cybersecurity infrastructure and regulations. Such incidents have compelled various government bodies to design stringent regulations to protect the privacy of both individuals and organizations. As a result, African businesses and consumers need to be aware of the risks of data breaches, adhere to data regulations, and take steps to protect their personal information.

Since 2021, the pandemic has caused 43% increase in the African population of 1.37 billion connecting to the Internet to work remotely.

According to the Kenyan cybersecurity company Serianu, the cost implications of weak networks and lack of robust cybersecurity policies for Africa are estimated at USD 4.1 Billion

According to AFRIPOL, Business Email Compromise (BEC) is one of the most significant concerns for cybercrime on the African continent.

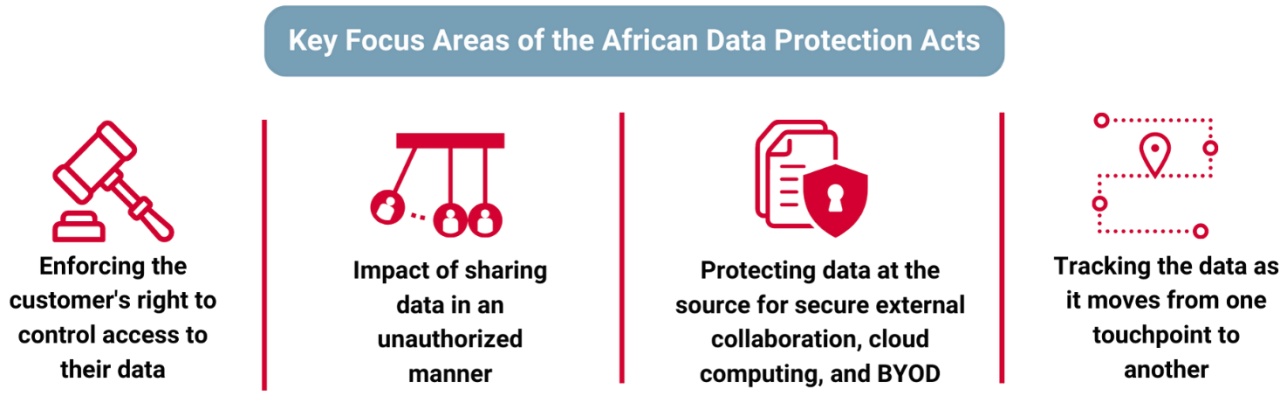
Need for Data Protection Acts in Africa

Over 50 percent of African countries have adopted data protection, privacy, and security laws. With the rapid rise in digitization due to the pandemic, the broad implementation of such laws across the continent has never been more urgent. The increasing financial investment opportunities in the African region have expedited the need for organizations to understand and adopt data protection regulations.

The African continent's data protection acts aim to help African countries broaden their scope of economic development, which today is highly dependent on Internet connectivity and digital trade.

The data protection acts that are currently active in the African region are:

- Kenya Data Protection Act (2018)
- Ghana Data Protection Act (2012)
- Nigeria Data Protection Act (2019)
- Uganda's Data Protection and Privacy Act (2019)
- Egypt Data Protection Law (2020)
- Botswana Data Protection Act (2021)
- The Protection of Personal Information Act 4 of 2013 (POPIA), South Africa



DATA-CENTRIC SECURITY HELPS ORGANIZATIONS MEET COMPLIANCE & PRIVACY GOALS

Granular data-centric security to persistently protect information wherever it resides regardless of who accesses it and how it's being shared or stored

Data-centric audit compliance logs

Complete control over files while they are in transit, at rest and/or at work

Real-time automated security and **alerts** for unauthorized activities, daily reports

How Seclore Can Help Organizations Comply with Data Protection Acts in Africa

Multi-cloud environments, data sharing, and third-party collaboration can expose personal consumer data and a company's most sensitive digital assets – intellectual property, company financials, customer data, etc. - leading to data breaches and loss. Traditional perimeter-centric security tools fail to secure data in such a scenario.

Seclore's Data-Centric Security solution aims to protect sensitive data by supplying persistent, granular data-centric controls that secure information.

Simply put, data-centric security controls always stay with the data wherever it goes, enabling organizations to:

- Protect confidential information
- Eliminate data leakage and data theft, especially while outsourcing business operations
- Comply with the relevant guidelines and regulatory compliance obligations

In today's post-Wikileaks world, organizations need a novel approach to securing and governing their data inside and outside organizational boundaries. Many prominent organizations in the African region should use Seclore's Data-centric security in various sectors such as Banking, Insurance, Government & Defense, Healthcare, and other private organizations. Seclore can help entities comply with the relevant sections of African countries' various data protection acts and achieve comprehensive data governance for consumers' personal information.

About Seclore

Seclore is the data protection platform securing the enterprise's digital assets wherever they go. The platform allows organizations to use best-of-breed solutions to discover, classify, protect, and track enterprise data within and outside the organization's boundaries. Over 2000 companies and government organizations in 29 countries use Seclore to achieve their data security, governance, and compliance objectives.

Learn how easy it is to keep your most sensitive data safe and compliant.

Contact us at: info@seclore.com or CALL 1-844-4-SECLORE.