Africa's Data Opportunity?

Cross-Border Data Flows and IoT

GSMA
January, 2021

Welcome Remarks

Akinwale Goodluck

Head of Africa

GSMA

Cross-Border Data Flows
The impact of data localisation on IoT

Caroline Mbugua

Senior Policy Manager

Sub-Saharan Africa, GSMA

Data Protection and Trade in Africa

African Continental Free Trade Area

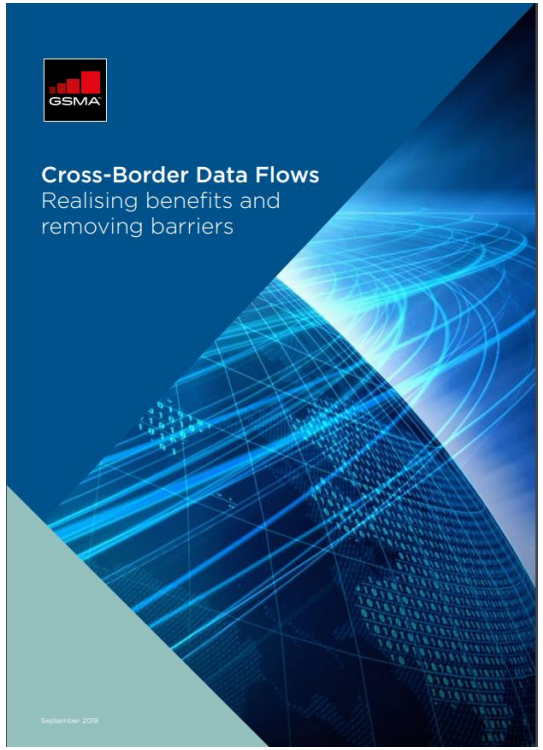
Malabo Convention
Cybersecurity & Privacy

Smart Africa
Data Protection initiative

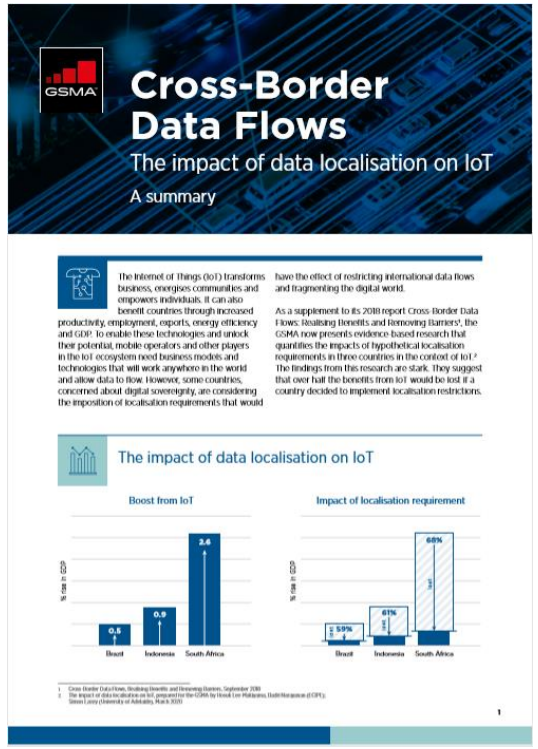
Africa Data Leadership Initiative

African Network of
Data Protection Authorities

Qualitative and Quantitive Analysis of cross-border data flows



The reasons why data needs to flow are easy to describe but hard to quantify



A new GSMA study: **Cross-Border Data Flows - The impact of data localisation on IoT** attempts to ***quantify*** the potential impacts of hypothetical data localisation restrictions (DLR) on the expected gains from IoT

To download visit: gsma.com/cross-border-data-flows-the-impact-of-data-localisation-on-iot

Findings

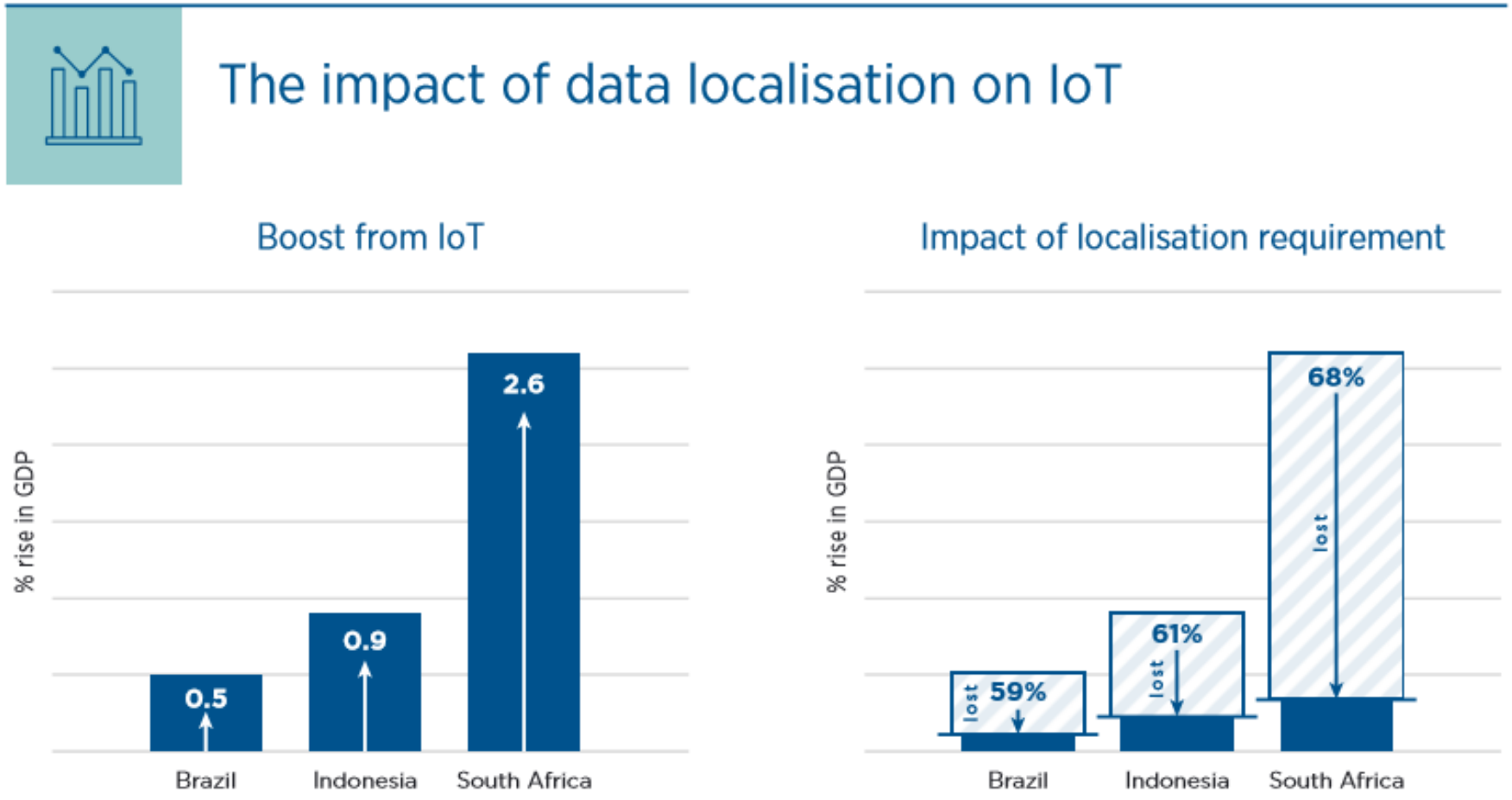
The number of IoT connections is growing by almost **15%** per year

and is set to reach approximately **25 billion** connections by 2025

The sectors that are impacted by IoT play a crucial role in emerging economies such as agriculture, basic manufacturing, transport, logistics, healthcare and education.

IoT has become a ‘horizontal technology’. The uptake of IoT and related technologies has a transformative impact on the way people live and how firms do business, meaning that IoT gains start to produce first and second order economic effects across the whole economy.

Impact of Data Localisation Restrictions on IoT gains

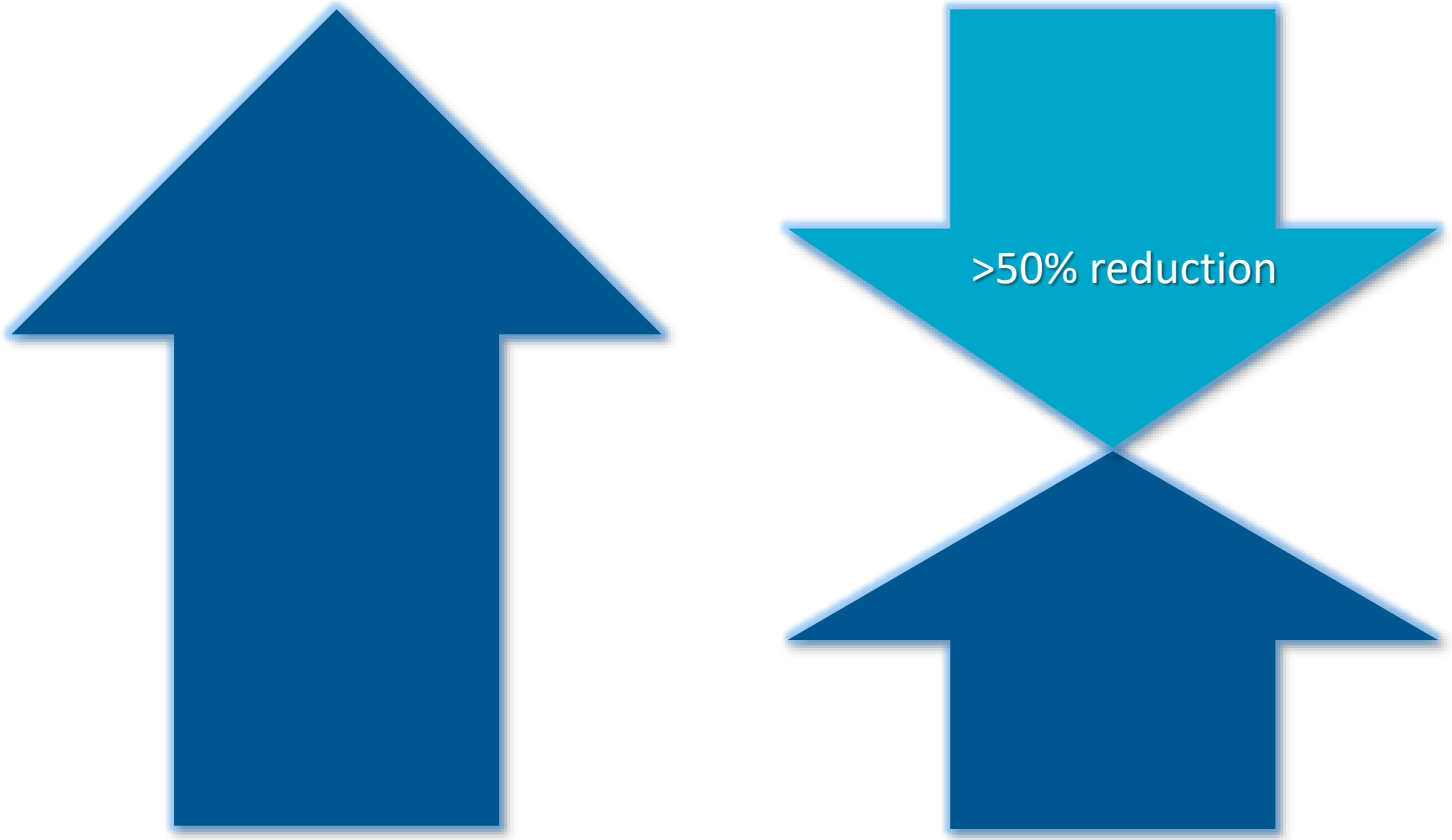


Benefits of IoT in Emerging markets.

The impact of IoT on emerging economies is undervalued.

- Increased productivity.
- Enhanced energy of cost efficiencies.
- Lower environmental impact.

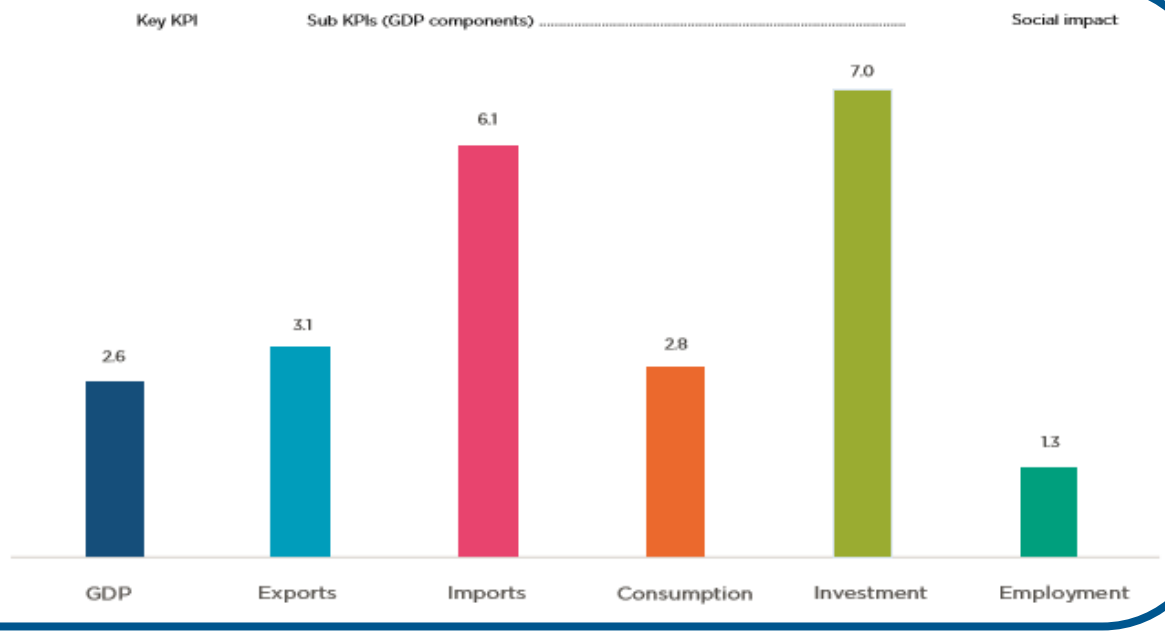
Impact of Data Localisation Restrictions on IoT gains



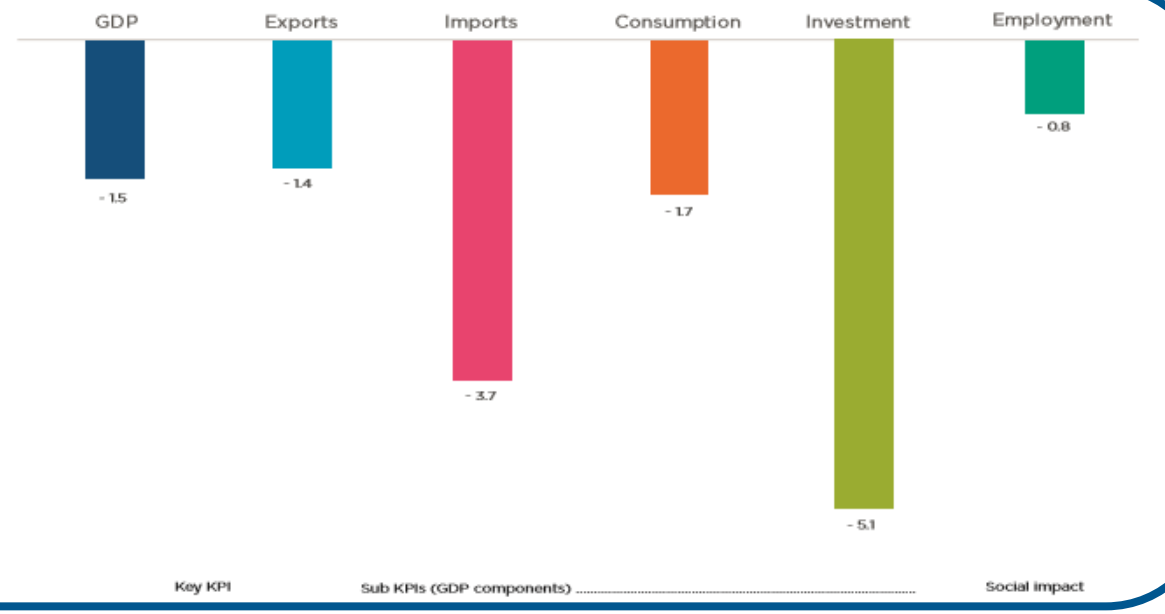
Gains from IoT

Are undermined by DLR

Contribution of IoT deployment in South Africa



Losses of DLRs on IoT in South Africa



Conclusion

From the report it is clear that IoT enables different opportunities for growth for emerging economies. This is found to be consistent in all the countries surveyed, despite different regions, industrial structures and industrial policies.

The cost of imposing data localisation measures and other similar restrictions on cross-border data flows (that have similar cost-raising effects to DLRs), will only continue to rise further as data becomes increasingly important across all areas of economic activity.

These increased costs result in suppressed economic activity across the entire economy — with negative impacts not just in GDP growth, but also trade flows, employment and investment.

Policymakers will need to consider the negative consequences of imposing DLRs and similar restrictions on cross-border data flows when developing data privacy policy in the different countries in Africa.

To mitigate the impact of these measures, action should be limited to the most essential policy objectives and be imposed in a way that is minimally trade restrictive

Africa's Data Opportunity? Cross-Border Data Flows and IoT

By Drudeisha Madhub
Data Protection Commissioner (Mauritius)

A Roadmap for cross-border data flows

① **Allow data to flow by default**

Prohibit data localization requirements except in very specific circumstances in order to create regulatory certainty for businesses

② **Establish a level of data protection**

Establish national legal frameworks that protect the data of private individuals. Complement this with laws that protect proprietary rights.

③ **Prioritize cybersecurity**

Enact transparent cybersecurity legislation in line with international norms and maintain robust data security infrastructure.

④ **Hardwire accountability between nations**

Establish cooperation mechanisms between national authorities to hold governments accountable for the security and confidentiality of the data they share, while making allowances for compliance.

⑤ **Prioritize connectivity, technical interoperability, data portability and data provenance**

Prioritize the development of connectivity infrastructure as a prerequisite to building a local data economy, encourage technical standards to increase interoperability, facilitate data portability at the B2B level to support SMEs, and encourage data publishers to ensure data integrity.

⑥ **Future-proof the policy environment**

Allow for the possibility of future alternative models (such as federated learning models and data trusts) that can also fulfil the spirit of cross-border data flows.

Government concerns that prompt data localization requirements

Political security

Protecting the sovereignty of the government and the democratic system

Economic security

Protecting the nation's economic wealth and freedom

Cybersecurity

Protecting digital assets from theft or damage

Domestic security

Upholding national laws and protecting the nation against internal security threats

Essential infrastructure

Protecting access to critical infrastructure such as transport hubs, network communications, banking infrastructure, etc.

Environmental security

Preventing environmental problems such as water scarcity, food shortages or climate change

Energy and natural resources security

Protecting access to energy resources for energy consumption

Establish a level of data protection

Policy recommendations

- Participating governments should be required to have national legal frameworks in place that protect the data of individuals, e.g. a data protection law.
- Cross-border transfers of personal data should generally be permitted under national laws.
- A clear cooperation mechanism between national authorities needs to be established to enhance trust and allow for regulatory compliance across borders.
- Compatibility or policy interoperability between data protection and privacy laws is encouraged to ensure certainty and security.
- Governments should investigate the possibility of reaching explicit agreement on the adequacy of other countries' data protection and privacy regimes where the respective legal systems offer substantially similar privacy protections so as to create a common space for the movement of personal data.
- Lawmakers should encourage and enable secure data sharing and focus legislation and law enforcement on abuses such as cybercrime, fraud and harmful discrimination.
- If lawmakers enact broadly applicable privacy laws to define baselines, they should be technologically neutral so as to remain future-proof.

Core principles of data protection and privacy

Reference:

World Economic Forum, A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy, White Paper, June 2020

Ammar Sabbagh

Head of Technology & IoT,
Ericsson

Oyeronke Oyetunde

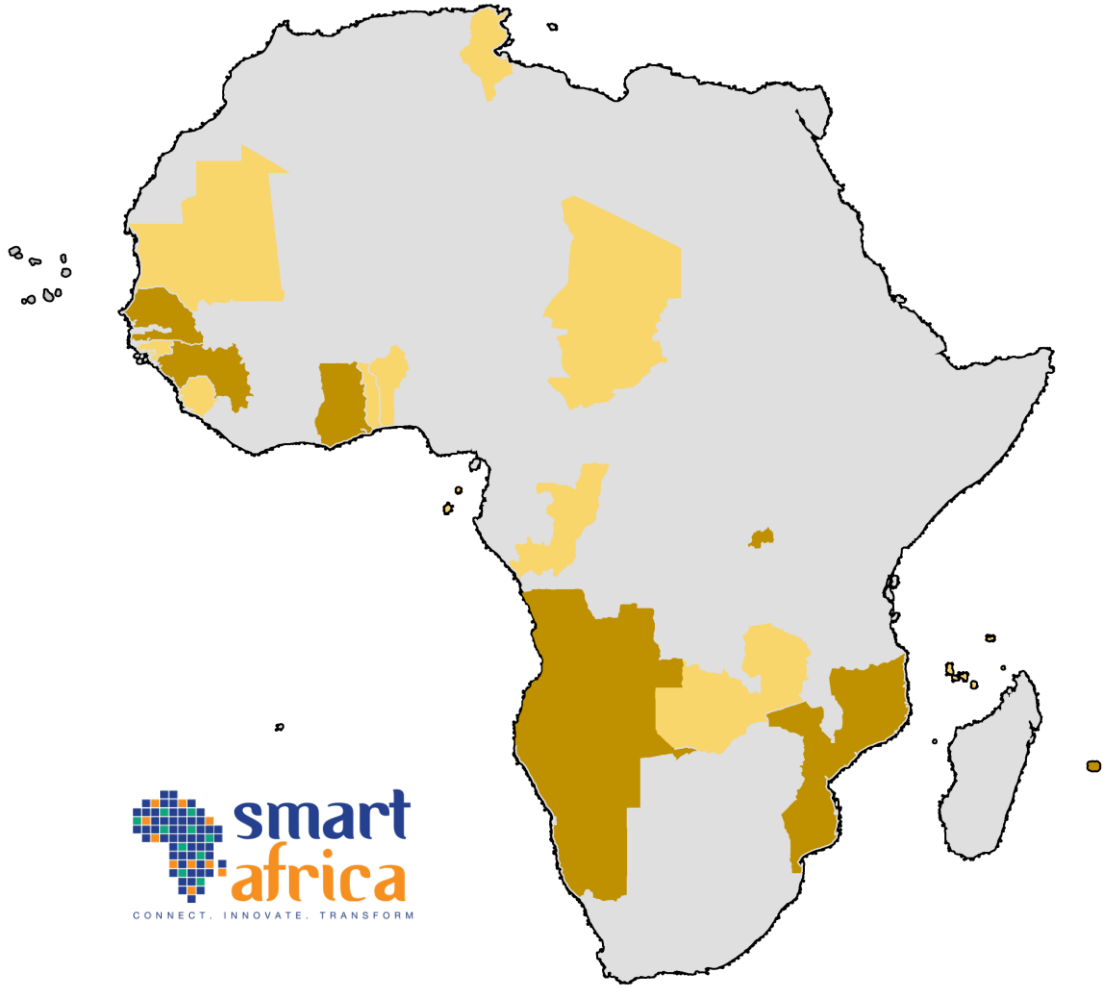
General Manager: Regulatory Affairs,
MTN Group

Africa's Data Opportunity

Cross Border Data Flows and IoT by Thelma Quaye

smart africa
CONNECT. INNOVATE. TRANSFORM

THE AFRICAN UNION CONVENTION ON CYBER SECURITY AND DATA PROTECTION



African Union Convention on Cyber Security and Personal Data Protection - Malabo Convention (2014)

Signed: 14 countries

Ratified: 8 countries

Treaty : legally binding after signature and ratification.

Main principles:

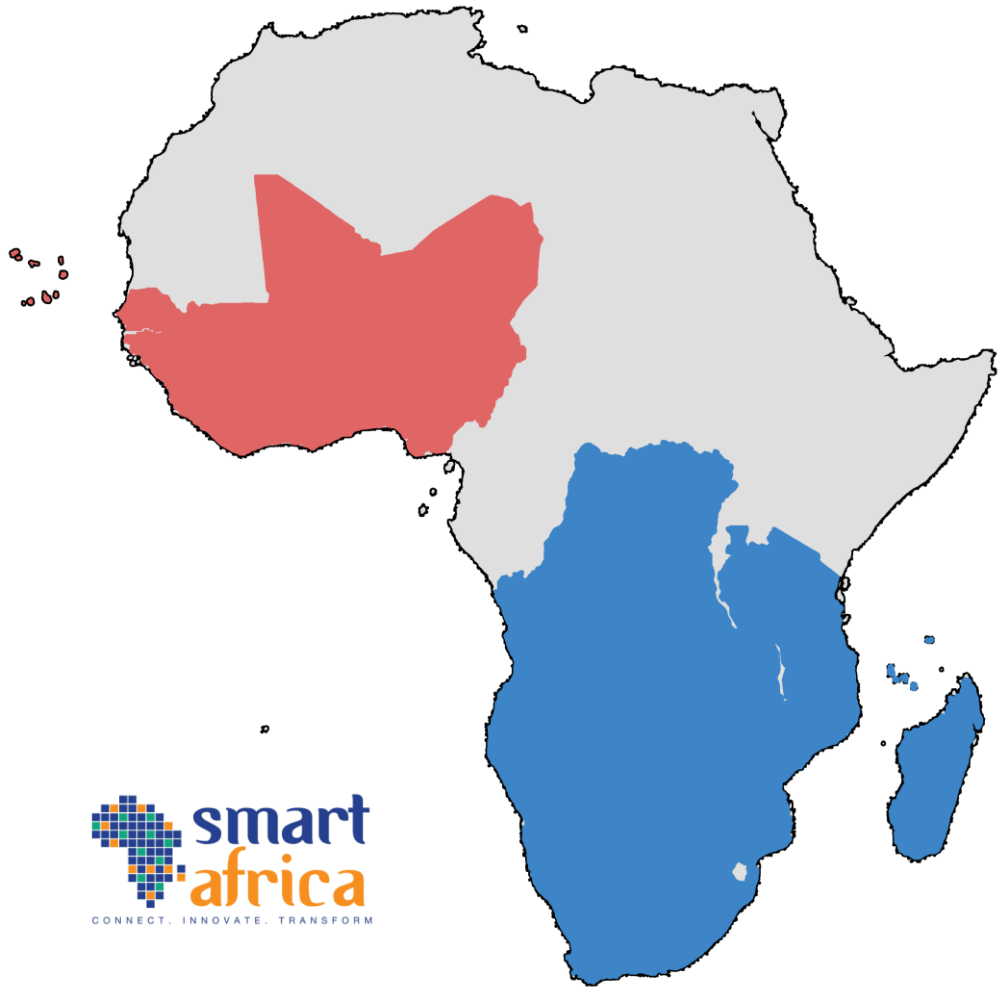
- Consent and legitimacy
- Lawful and fair processing
- Purpose, relevance and retention of data
- Accuracy of data over its lifespan
- Transparency of processing
- Confidentiality and security of personal data

Rights of data subjects:

- Right to information
- Right of access
- Right to object
- Right of rectification or erasure

Ratified Countries : Angola,Ghana,Guinea,Mozambique,Mauritius,Namibia,Rwanda, Senegal

REGIONAL LAWS



ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010)

Supplementary act : binding on Member States and the institutions of the Community.

Main principles:

- Consent and legitimacy
- Legality and fairness
- Purpose, relevance and preservation
- Accuracy
- Transparency
- Confidentiality and security
- Choice of data processor

Rights of data subjects:

- Right to information
- Right of access
- Right to object
- Right to rectification and destruction

SADC Model Law on Data Protection (2012)

Model law : non-binding.

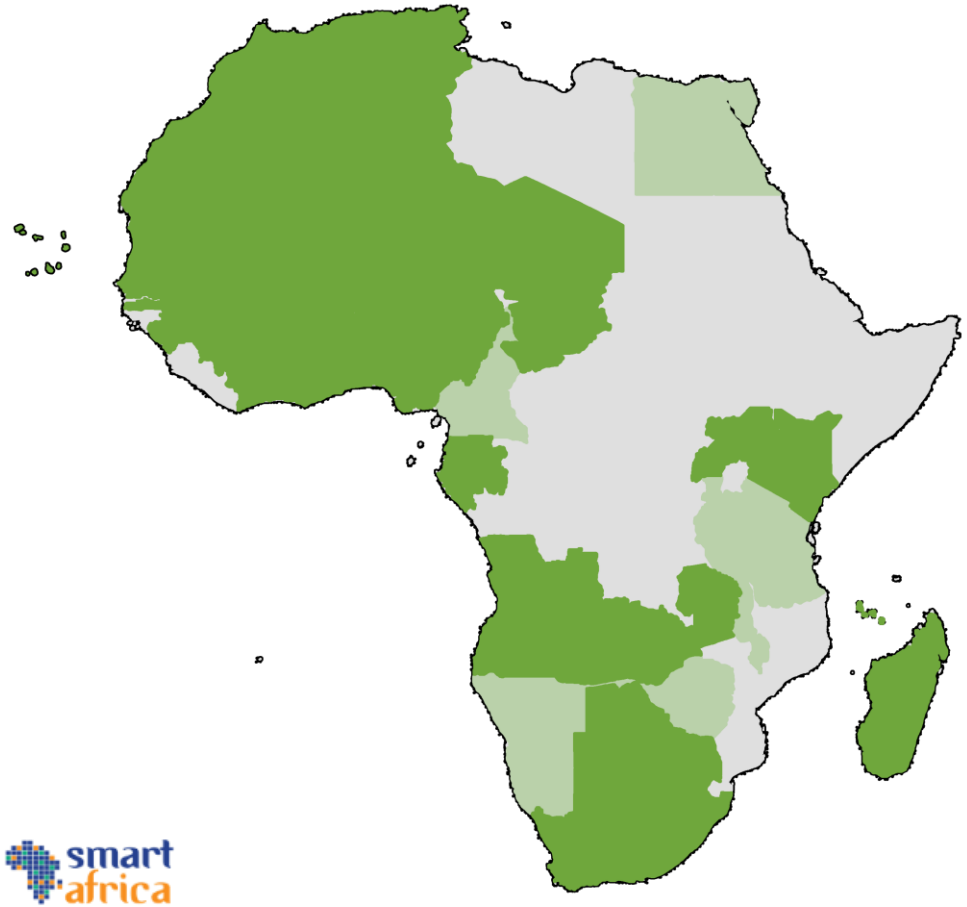
Main duties for data controllers and processors :

- Information to the data subject
- Authority to process data belongs to data controller
- Security
- Obligation of notification to the authority
- Accountability

Rights of data subjects:

- Right of access
- Right of rectification, deletion and temporary limitation of access
- Right of objection

STATE OF PLAY FOR THE LEGAL AND REGULATORY ENVIRONMENT



State of data protection regulation in Africa

30 countries do have specific data protection laws

(54 % of African countries)

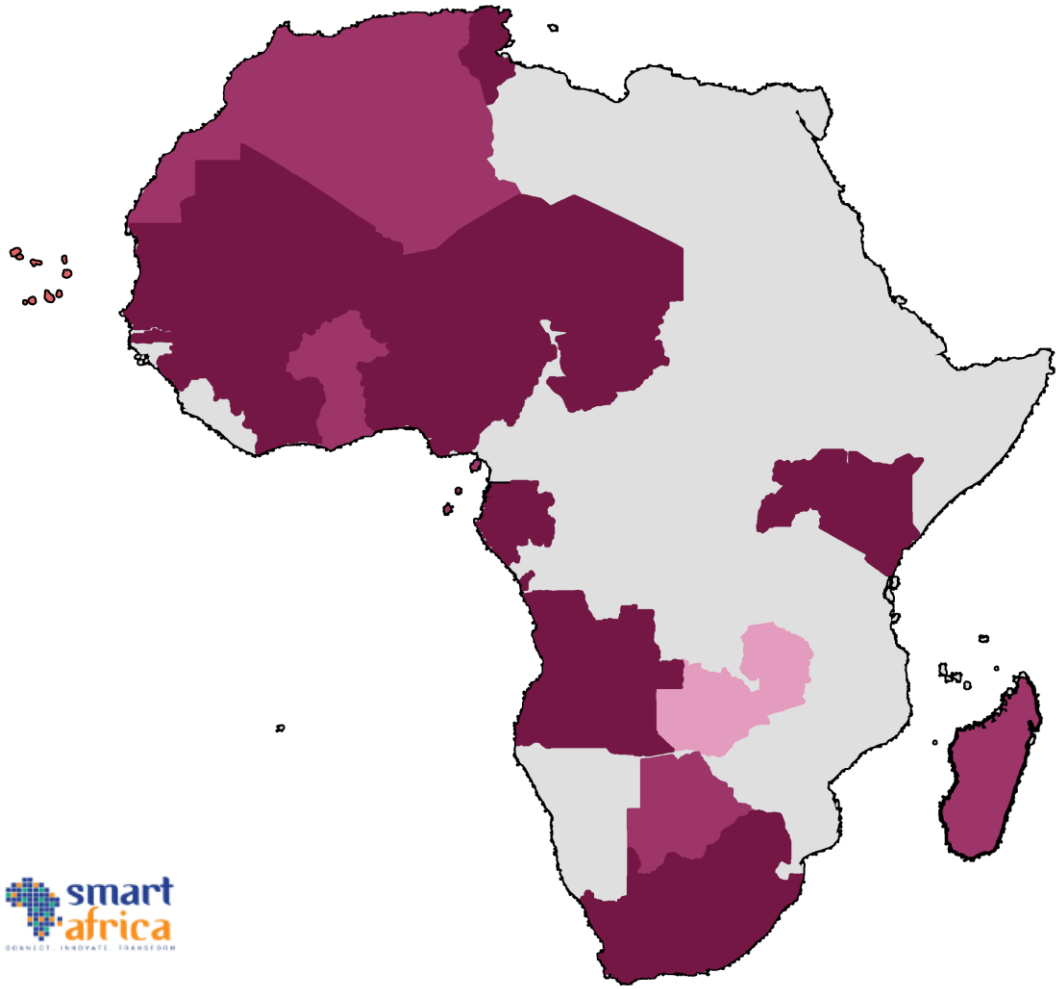
8 countries are currently drafting legislation

(17% of African countries)

16 countries do not have any specific data protection law

(30 % of African countries)

RIGHTS OF SUBJECTS



State of data subject rights in data regulations in Africa

Right to access personal data

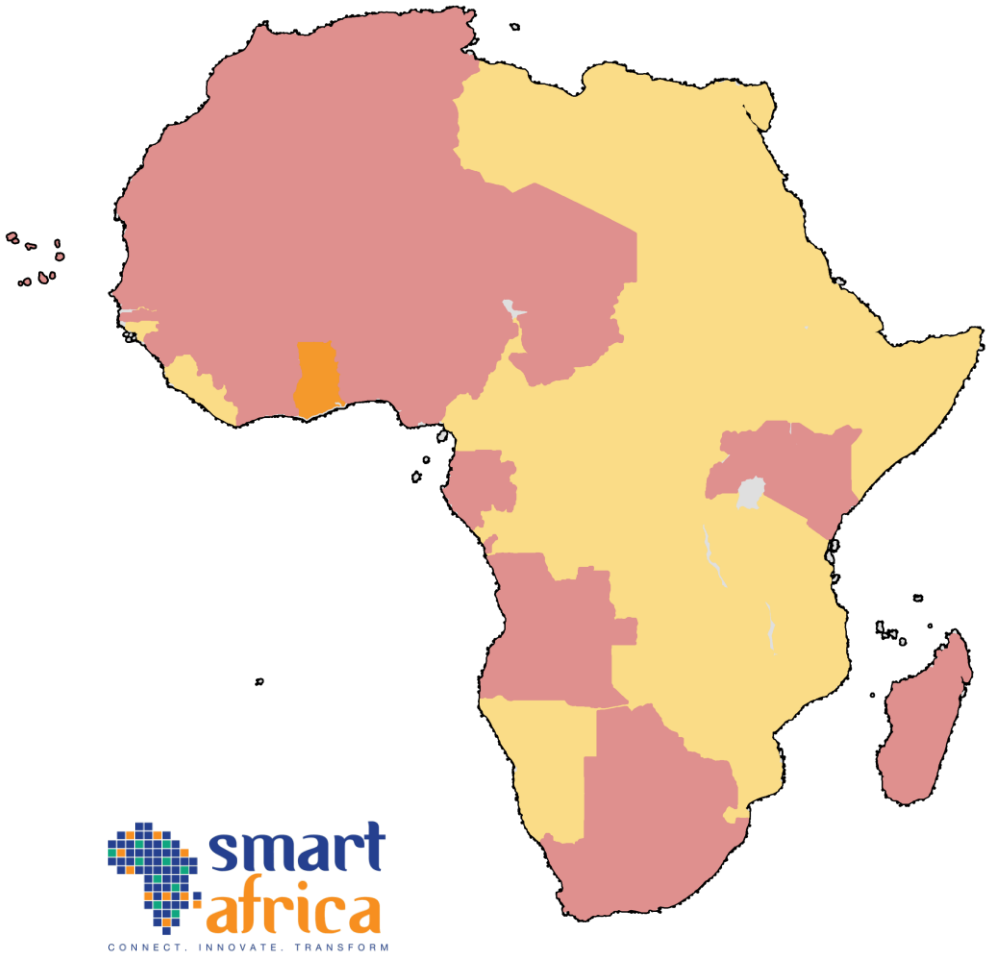
(28 countries - 52% of African countries
-
97% of countries with data protection laws)

Right to access and rectify personal data

(27 countries - 50% of African countries
-
93% of countries with data protection laws)

Right to access, rectify and erase personal data

(20 countries - 37% of African countries
-
69% of countries with data protection laws)



CROSS BORDER DATA FLOWS

State of cross-border data flows regulation in Africa

Absence of cross-border data flow restrictions

(26 countries - 48% of African countries)

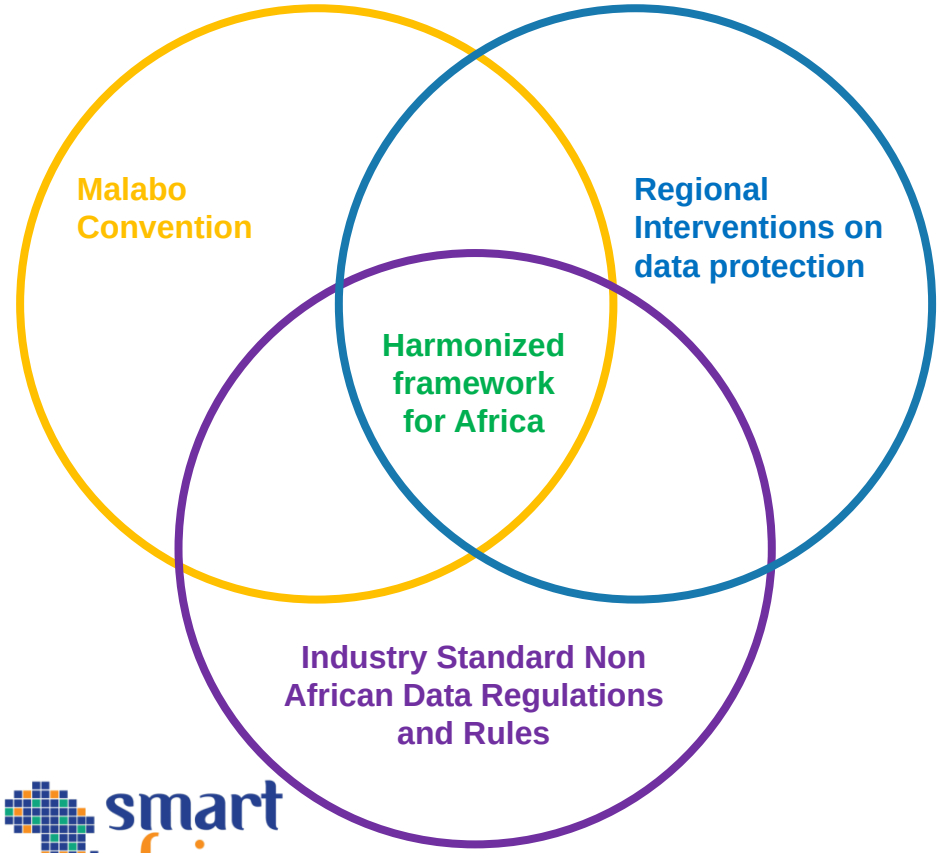
No prior restriction for data transfers: ex-post accountability for data exporters

(2 countries - 4% of African countries)

Cross-border data flows require contractual safeguards, prior authorization or adequacy decisions by authorities

(26 countries - 48% of African countries)

WHAT DOES SMART AFRICA WANT TO DO?



Mission:

To create a harmonized framework for data protection and data regulation, in light of existing international, continental and regional frameworks.

Objectives:

1. To develop a mapping of existing frameworks to identify commonalities / similarities and points of divergence

2. To create a framework document that serves as a guideline for Smart Africa Member States who want to develop specific country data protection and policy

WHAT ARE THE EXPECTED BENEFITS?...

smart africa
CONNECT. INNOVATE. TRANSFORM

Expected Benefits

- A harmonised framework will mean a better bargaining power for the continent as a whole
- Immediate benefit of scale by businesses across the country to move us beyond the 18% intra-Africa trade.
- Easy adaptability of new technology, especially data driven technologies like IoT, AI etc, which will allow easy data transfer across borders.

Panel Discussion Moderated by

Boris Wojtan

Director of Privacy, GSMA

Drudeisha Madhub
Data Protection Commissioner, Mauritius

Ammar Sabbagh
Head of Technology & IoT, Ericsson

Oyeronke Oyetunde
General Manager: Regulatory Affairs, MTN Group

Thelma Quaye
Head of Digital Infrastructure Program, Smart Africa

Vote of Thanks

Boris Wojtan

Director of Privacy, GSMA