CROSS-BORDER DATA FLOWS

DPGSK WEBINAR

5TH AUGUST 2025

CROSS-BORDER DATA TRANSFERS

Presented by:

Katumbi Mailu,
Principal Data Protection Officer,
Compliance,
The Office of the Data Protection Commissioner.

LEGAL & REGULATORY FRAMEWORK

CONSTITUTIONAL AND LEGAL FRAMEWORK FOR DATA PROTECTION IN KENYA

The Constitution of Kenya, 2010 guarantees the right to privacy as a fundamental right.

Article 31 of the Constitution states, "every person has the right to privacy, which includes the right not to have:

(c) information relating to their family or private affairs unnecessarily required or revealed; or

(d) the privacy of their communications infringed."

Article 35 (2) ensures the right of every person to the correction or deletion of untrue or misleading information that affects the person.

DATA PROTECTION ACT 2019

- The Data Protection Act, 2019 came into law on 25 November 2019 to:
- Give effect to Article 31 (c) and (d) of the Constitution, as the overarching legislative framework for data protection; and
- To establish the Office of the Data Protection Commissioner, regulate the processing of personal data and provide for the rights of data subjects and obligations of data controllers and data processors.

SUBSIDIARY REGULATION

- Data Protection (General) Regulations, 2021
- Data Protection (Complaints Handling and Enforcement Procedure) Regulations, 2021
- Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021

MANDATE OF ODPC

- Regulate the processing of personal data to ensure it aligns with legal standards.
- Protect the privacy of individuals by enforcing data protection principles.
- Establish legal and institutional frameworks for personal data protection.
- Ensure compliance with the principles outlined in Section 25 of the Act.
- Provide rights and remedies to data subjects whose personal data is mishandled.
- Oversee registration of data controllers and processors operating in Kenya.
- Investigate complaints and enforce penalties for violations of the Act.

LEGAL & REGULATORY FRAMEWORK – CBDT

- The Data Protection Act, 2019 – Part VI sections 48, 49 & 50.
- The Data Protection(General) Regulations 2021 – Part VII regulations 39 – 48 and reg 26 on strategic purpose interest

DEFINITIONS

KEY DEFINITIONS

Data Subject

A natural person who is the subject of personal data.

Data Controller

A natural or legal person who determines the means and purpose for processing personal data

Data Processor

A natural or legal person who processes data on the instructions of the data controller

PERSONAL & SENSITIVE PERSONAL DATA

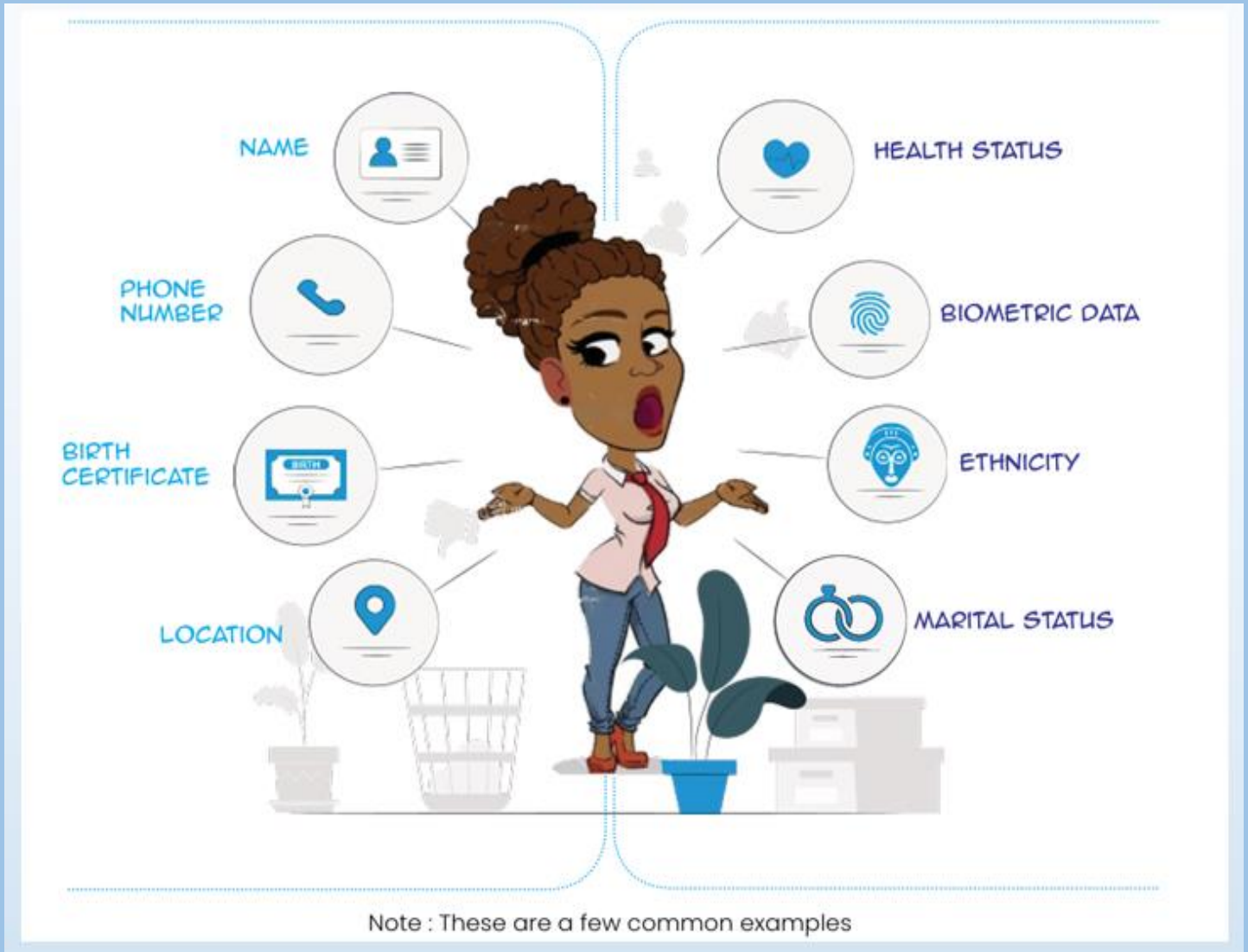
Personal Data

Any information that can be used to identify a natural person

Sensitive Personal Data

Data revealing details about a natural person that may be used to harm a data subject

PERSONAL & SENSITIVE PERSONAL DATA



CROSS-BORDER TRANSFER OF PERSONAL DATA

- *"means movements of personal data across national borders."*

- *Data Transfer vs Data Sharing*

- *Other Definitions (reg 39)*
  - *Data in transit*
  - *Recipient*
  - *Transferring Entity*
  - *Relevant International Organisation*

CONDITIONS FOR CROSS-BORDER DATA TRANSFERS

Conditions for CBDT

Condition	Explanation
Adequacy	The Data Commissioner decides that the country or international organisation to which the data is being transferred has an adequate level of protection.
Appropriate Safeguards	• Legally binding and enforceable instrument • Benchmarking of safeguards against similar transfers, eg standards within a specific sector. • Malabo Convention. • Reciprocal data protection agreement with Kenya. • Binding Corporate Rules

Conditions

TAKE NOTE

- Consent must be obtained for sensitive personal data

Condition	Explanation
Necessity	The data transfer is necessary due to the reasons listed in section 48(c)
Consent	• Data subject has been informed of risk of transfer • Explicit consent has been obtained from the data subject • This consent is a derogation to the conditions • Consent for sensitive personal data vs consent as a derogation

ADEQUACY DECISION

- Regulation 44
- Country, territory, specified sector or international Organisation.
- Publish a list on the office website of countries, territories and specified sectors that have an adequate level of protection.
- Responsibility falls on ODPC.

APPROPRIATE SAFEGUARDS

- *Ratification of the African Union Convention on Cyber Security and Personal Data Protection.*
- *Reciprocal Data Protection agreement with Kenya*
- *Binding Corporate Rules*
- *Binding legal instruments (Standard contractual clauses)*
- *Sector-specific codes of conduct*
- *Certification sec 74 of the DPA*

BINDING CORPORATE RULES

🔍 Definition: Binding Corporate Rules (BCRs) are legally binding internal rules adopted by multinational groups to ensure adequate protection of personal data transferred across borders within the group.

🛡️ Key Features: Must include enforceable data subject rights, accountability mechanisms, and compliance audits.

🌍 Purpose: Facilitate internal cross-border data flows while complying with appropriate safeguard requirements under the DPA.

📌 Comparison: BCRs go beyond standard contracts – they're a global compliance framework.

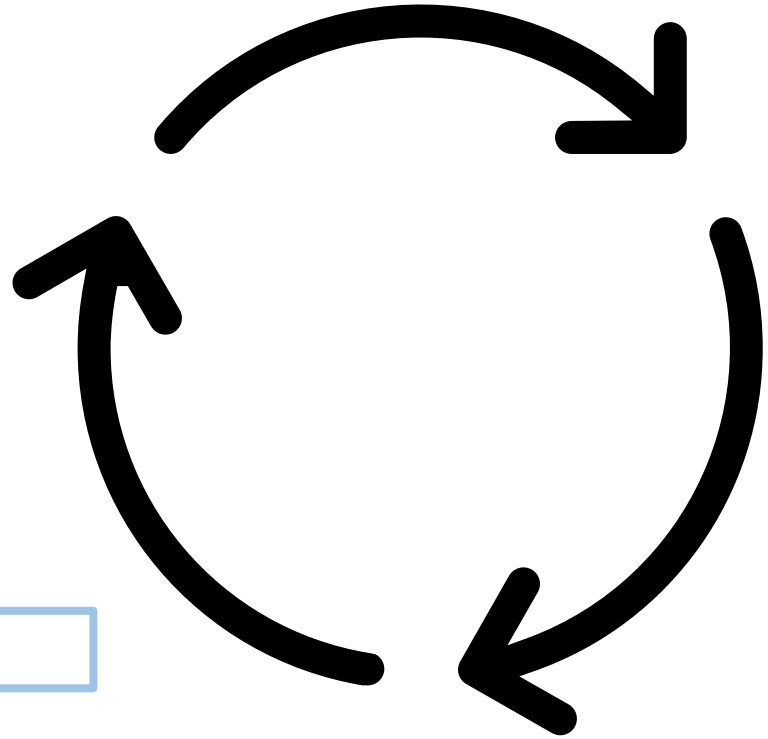
BINDING CORPORATE RULES

🌐 Kenya – Regulation 43 of the Data Protection (General) Regulations, 2021 explicitly recognises BCRs.

- Requirements:
- Must be legally binding on all entities and employees within the group.
- Grant enforceable rights to data subjects.
- Detail governance structures, processing purposes, complaint handling procedures.
- Must outline group structure, transfer scope, rights enforcement, security, and audit.
- Kenya's ODPC may require notification and reserve the right to reject non-compliant BCRs.

🔍 Oversight: The Office of the Data Protection Commissioner (ODPC) may require documentation and updates.

REVIEW PROCESS BY ODPC



Transfer based on Necessity

(sec 48 & reg 45)

(c) the transfer is necessary—

(i) for the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for any matter of public interest;

(iv) for the establishment, exercise or defence of a legal claim;

(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vi) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

Transfer based on Consent

(reg 46)

46. (1) In accordance with section 25 (g) of the Act, in the absence of an adequacy decision, appropriate safeguards or prerequisites for transfer as a necessity, a transfer or a set of transfers of personal data to another country shall take place only on the condition that the data subject—

(a) has explicitly consented to the proposed transfer; and

(b) has been informed of the possible risks of such transfers.

(2) Without limiting the generality of sub-regulation (1), a data controller or processor must seek consent from a data subject for the transfer of sensitive personal data, in accordance with section 49 of the Act.

Cross-border transfer (Regulation 47 & 48

Subsequent Transfer:

- Obligations of DC/DP
- Obligation of transferring entity on setting conditions for subsequent transfers

Cross-border transfer agreements:

- Countries where the data may be transferred
- Grants unlimited access to the transferring entity to ascertain the recipient's ability to store the data.

DATA LOCALIZATION

Data Localization (Sec 50, Reg 26)

Definition

Data localisation is a requirement/obligation to domicile specific data in a particular jurisdiction.

Regulation 26

The limitation is on entities processing personal data for the purpose of strategic interest or special interest purposes of the state. They must:

- Process data through a server/data centre located in Kenya; or
- Store one serving copy of the data in a data centre located in Kenya

Strategic Interest Purpose

- Civil Registration and legal identity management systems
- Elections
- Administration of public finances
- Protected computer systems under the CM&C Act
- Early childhood & basic education under the Basic Education Act
- Primary or secondary healthcare

CONSEQUENCES OF NON-COMPLIANCE

CONSEQUENCES

ODPC

- Enforcement Notice – areas of non-compliance
- Penalty notice – fine not exceeding 5 million
- Complaints by data subjects - compensation

Industry

- Reputational risk and loss of trust
- Loss of business and opportunities in foreign markets
- Competitive advantage

THANK YOU