OFFICE OF THE DATA PROTECTION COMMISSIONER

GUIDANCE NOTE ON CROSS BORDER DATA TRANSFER

Table of Contents

1. "Definition of Terms

"Act" means the Data Protection Act, No 24. of 2019.

"**Adequacy Decision**" in the context of data protection, is a determination by a data protection authority, that a third country or international organisation offers an equivalent level of protection for personal data

"**Binding Corporate Rule**s" means personal data protection policies adhered to by a data controller or data processor established in Kenya for transfers or a set of transfers of personal data to a data controller or data processor in one or more countries within a group of entities, or a group of entities engaged in a joint economic activity;

"Cloud Service" means a service delivered over the internet that allows users to access computing resources—such as storage, software, or processing power—without owning or managing physical servers or infrastructure.

"**Cloud Storage**" means a service model in which data is transmitted and stored on remote storage systems, where it is maintained, managed, backed up and made available to users over a network, typically, the internet

"**Critical information infrastructure system or data**" means an information system, program or data that supports or performs a function with respect to a national critical information infrastructure;

"**Cross-Border Data Transfer**" means the transfer of personal data across international borders.

"**Data Centre**" means a large group of networked computer servers typically used by organisations for the remote storage, processing, or distribution of large amounts of data.

"Data Commissioner" means the person appointed pursuant to section 6 of the Act.

"Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing personal data.

"Data Handlers" means a data controller and/or data processor.

"**Data Localisation**" refers to the regulatory requirement that data about a nation's citizens or residents is initially collected, processed or stored within the boundaries of a

particular "jurisdiction", such as a country or a geographic region like a regional economic community or bloc.

"Data Processor" means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Data Controller.

"Data Subject" means an identified or identifiable natural person who is the subject of personal data.

"Data in transit" means personal data transferred through Kenya in the course of onwards transportation to a country or territory outside Kenya, without the personal data being accessed or used by, or disclosed to, any entity while in Kenya, except for the purpose of such transportation.

"Entity" or **"Entities"** means a natural (individual) or legal person, public authority, agency or other body that processes (handles) personal data.

"**Group of Undertakings**" means two or more companies that are legally separate but are connected through ownership or control, typically under a parent company.

"Office" means the Office of the Data Protection Commissioner as established in Section 5 of the Act.

"Personal Data" means any information relating to an identified or identifiable natural person.

"**Processing**" means any operation or sets of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, or use, disclosure by transmission, dissemination, or otherwise making available; or alignment or combination, restriction, erasure or destruction.

"Public Interest" means a collective well-being and the common good of all citizens.

"Recipient" means an entity that receives in a territory outside Kenya the personal data transferred to the recipient by or on behalf of the transferring entity, but does not include an entity that receives the personal data solely as a network service provider or carrier;

"Regulations" means a law, rule, or other order prescribed by authority, especially to regulate conduct;

"**Relevant international organisation**" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

"Sensitive Personal Data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex, or the sexual orientation of the Data Subject.

"Serving Copy" refers to a replica or duplicate of personal data that is transferred out of the country.

"**Strategic Interest of the State**" processing activities which form part of state's interest that are important for the security, economic prosperity, or influence of a nation and that requires data localisation.

"**Cross-border Transfer Agreements**" means legally binding contracts that outline the roles and obligations of the transferring entity and the recipient of personal data.

"Transferring entity" means an entity that transfers personal data from Kenya to a country or a territory outside Kenya but does not include an entity dealing with data in transit.

2. Introduction

Cross-border transfer of personal data involves sending personal information to a foreign country. This occurs when businesses operate in multiple jurisdictions, or when individuals share their data with entities located outside their country. The Act, like many data protection laws worldwide, has specific provisions governing cross-border transfers of personal data. These provisions aim to ensure that personal data is adequately protected, even when it is in transit to countries with different data protection laws.

Due to emerging technological trends, the country has experienced a rise in the cross-border transfer of personal data. Personal data in transit is a frequent target of cyberattacks, data breaches, phishing, ransomware attacks, and account takeovers. These pose significant risks to the personal data collected, processed, and stored by various organizations in cloud environments. This risk is often compounded by the lack of adequate data security measures and the involvement of parties in the cross-border transfer that may not adhere to the highest data protection standards.

Additionally, the widespread adoption of cloud computing and the interconnection of numerous organisational systems and devices have further complicated data security challenges. Therefore, as data increasingly flows across borders, the establishment of a robust data protection framework has become essential to safeguard personal information. The right to privacy is enshrined in the Kenyan Constitution, as expounded

under the Act, which provides the required legal framework to all individuals and organisations engaging in cross-border transfer of personal data.

3. Privacy concerns

Some of the significant privacy concerns in cross-border transfer of personal data include:

1. **Lack of transparency and misuse of personal data -** Personal data being transferred for a specific purpose may potentially be used for different purposes, thereby amounting to misuse and a potential breach.
2. **Lack of user control -** Users often lack clear information about where their data is stored, processed, or transferred. Without transparency, users cannot effectively manage their privacy rights across borders.
3. **Data breaches and cybersecurity risks-** Attackers may gain unauthorized access to personal data in transit, compromising its confidentiality. If personal data is not adequately encrypted during transfer, it may be intercepted and compromised by malicious actors.
4. **Varying levels of data protection laws-** Personal data transferred to a country with weaker privacy laws may be more vulnerable to misuse or unauthorised access.
5. **Enforcement challenges -** The global nature of data flows makes enforcement difficult, especially where personal data is transferred to or processed by entities located in foreign jurisdictions. Cooperation between national regulators is often slow or limited by differences in legal frameworks and regulatory powers and enforcement mechanisms.

4. Scope and Purpose

This guidance note applies to all entities that handle personal data within Kenya and transfer or intend to transfer such data outside Kenya. It outlines the legal, regulatory, and operational obligations that data handlers must observe to ensure that personal data remains protected when transmitted to foreign jurisdictions.

The purpose of this guideline is to provide a clear framework for cross-border data transfers, safeguarding the privacy and rights of data subjects, promoting transparency and accountability, and mitigating risks associated with cyber threats, unauthorized access, and data misuse.

Additionally, it aims to harmonize Kenya's data protection practices with international standards, ensuring that organisations can engage in global operations while remaining compliant with the Act and Regulations. Therefore, it expounds on the obligations that data handlers should consider while transferring personal data outside Kenya and should be regarded as a minimum standard which can be supplemented by additional measures for the protection of privacy and individual rights, which may impact or be impacted by the processing of cross-border transfers of personal data.

5. Legislative Framework

The cross-border transfer of personal data in Kenya is governed by several legislative frameworks, including but not limited to:

a) **The Constitution of Kenya, 2010.**

Article 31 (c) and (d) guarantee individuals the right to privacy regarding to information relating to their family or private affairs unnecessarily required or revealed, or that of their communication infringed.

Article 35 states that every citizen has the right to access information the State holds and information another person holds necessary to exercise or protect any right or fundamental freedom.

b) The Data Protection Act, 2019, Establishes the Office of the Data Protection Commissioner and provides for the various conditions for transfer of personal data.

c) The Data Protection General Regulations, 2021, outline how personal data should be handled in Kenya, emphasizing consent, data subject rights, and cross-border transfers. They also set duties for data controllers and processors, including mandatory registration with the ODPC.

d) The Computer Misuse and Cybercrime (Amendment) Act, 2024; This Act provides for offences relating to computer systems; it enables timely and effective detection, prohibition, prevention, response, investigation, and prosecution of computer and cybercrimes; and facilitate international cooperation in dealing with computer and cybercrime.

e) **Kenya Cloud Policy 2024 -** The purpose of this policy is to ensure the seamless transition from traditional on-premises data center practices to Cloud Computing technology, facilitate cross-border transmission, fostering interoperability and strengthening collaboration across nations and complementing other relevant existing cloud computing regulations.

6. Application of Data Protection Principles

6.1. Lawfulness, fairness and transparency

The transferring entity must ensure that personal data transfer is lawful, and the data subject is informed in a transparent manner about the transfer, its purposes, and their rights both at the time of data collection and when the personal data transfer occurs.

6.2. Purpose limitation

Personal data can only be transferred and used for a specific and legitimate purpose. Any further use, including transfers, must be compatible with the original purpose.

6.3. Data Minimisation

This principle dictates that organizations should only collect and transfer personal data that is strictly necessary for a clear and lawful purpose across borders. Organizations must ensure the data shared is relevant, limited, and not excessive.

Data controllers and processors should carefully determine the minimum amount of information needed and avoid transferring unnecessary data.

6.4. Accuracy

Data handlers are required to take all reasonably practicable steps to ensure that personal data held is accurate and up to date. The transferring entity must ensure that the data transferred is accurate and up to date.

6.5. Storage Limitation

Personal data should not be kept in a format that identifies the data subjects longer than necessary for the purposes for which it was transferred.

6.6. Integrity & Confidentiality

The transferring entity should ensure that adequate security measures are put in place to protect personal data from unauthorised access, loss, destruction, or damage during and after the cross-border transfer.

6.7. Accountability

Data controllers and processors are required to demonstrate compliance when transferring personal data across borders. This includes ensuring the existence of adequate safeguards, executing data processing agreements, conducting due diligence on third parties, and maintaining oversight mechanisms to guarantee that all parties involved adhere to the Act

7. Key Considerations for Cross-Border Transfer of Personal Data

Part VI of the Act provides for the conditions which a transferring entity should comply with when they are transferring personal data out of the country. In addition, regulation 40 outlines the various bases a transferring entity can rely on while transferring. The bases include:

a) appropriate data protection safeguards;
b) an adequacy decision made by the Data Commissioner;
c) transfer as a necessity; or
d) consent of the data subject.

7.1. Appropriate Data Protection Safeguards

When relying on appropriate safeguards to transfer personal data to another country or relevant international organisation, a transferring entity should either:

a) have a legal instrument containing appropriate safeguards for the protection of personal data binding the intended recipient that is essentially equivalent to the protection under the Act and the Regulations; or
b) after evaluating the transfer circumstances, the entity concludes that adequate safeguards are in place to protect the personal data

A country or territory is deemed to have appropriate data protection safeguards if they have:

a) ratified the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention)
b) a reciprocal data protection agreement with Kenya; or
c) a contractual binding corporate rule among a concerned group of undertakings or enterprises.

7.2. The African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention)

The Malabo Convention is a treaty of the African Union adopted in 2014 that establishes a continental framework for cybersecurity, harmonizes national laws to combat cybercrime, protect personal data, and promote secure digital transformation across Africa.

Ratification refers to the formal process by which a State that has signed the Convention confirms its consent to be legally bound by it. The convention is one of the mechanisms that are deemed appropriate for data transfer. However, the Data Commissioner retains discretionary authority, pursuant to Section 49(2) of the Act, to assess and determine the adequacy of such safeguards on a case-by-case basis.

While the Convention does not explicitly detail adequacy frameworks, it requires that cross-border transfers protect privacy rights and comply with national data protection legislation. This includes:

- Ensuring the receiving jurisdiction has equivalent levels of protection
- Using contractual safeguards and data-sharing agreements
- Requiring explicit authorization from the DPA where risks exist

Kenya's Data Protection Act requires regulatory oversight of cross-border transfers where adequacy cannot be guaranteed.

Adequacy assessments are independent regulatory decisions based on the overall effectiveness of a country's data protection framework, and as such, a ratification of the convention does not confer an automatic approval of transfer. However, ratification may strengthen a country's adequacy prospects, but it does not override the statutory conditions for transfer, nor does it permit onward transfer of personal data received under an adequacy decision.

7.3. Reciprocal Data Protection Agreement

A Reciprocal Data Protection Agreement (RDPA) refers to a bilateral or multilateral arrangement between Kenya and another jurisdiction, whereby both parties mutually recognize and uphold comparable data protection standards. Such agreements are designed to facilitate lawful and secure cross-border transfer of personal data while ensuring that data subjects' rights remain protected.

The RDPA is one of the mechanisms that are deemed appropriate for safeguards for data transfer. The Act does not explicitly define RDPA as a standalone mechanism. However, they fall within the broader category of "appropriate safeguards" under Section 49(3), which empowers the Office to assess and approve mechanisms that ensure adequate protection of personal data transferred outside Kenya.

7.4. Binding Corporate Rules

Regulation 42 of the General Regulations deems Binding Corporate Rules ("BCRs") as an appropriate safeguard for Cross-Border Data Transfer within a corporate group. BCRs are legally binding and enforceable internal rules and policies adopted by multinational corporations/groups of undertaking to regulate the transfer of personal data within their corporate group across jurisdictions.

Elements of Valid BCRs

For BCR to be valid, the following element must be addressed in the BCRs:

- **Scope of application:** The BCRs must specify the data transfers to which they apply, the categories of personal data, the type of processing and its purpose, the types of data subjects, enforceable rights on data subjects, and identify any third countries where data is transferred.
- **Binding nature of BCRs:** The BCRs must be legally binding and apply to and are enforced by every member concerned of the group of corporate/undertakings and its employees.
- **Group structure:** The BCRs must specify the group structure, the list of entities bound by the BCRs and their contact details, and the application of the general data protection principles.
- **Accountability:** Every entity acting as a controller must be able to demonstrate compliance with the BCRs. Processors should make information available to the controller to demonstrate their compliance with the BCRs, including through audits and inspections
- **Complaint handling:** There must be an established system that allows data subjects to complain about any BCR member. Any such complaints must be dealt with by a clearly identified department without undue delay.
- **Third country legislation:** The BCRs must include a commitment that any third country legal requirements likely to have a substantial adverse effect on the guarantees of the BCRs will be reported to a competent supervisory authority.

- **Relationship with national laws:** The BCRs should state that where local laws require a higher level of protection for personal data, the local laws will take precedence over the BCRs.

a) Approval of the BCRs

After developing BCRs, organizations are required to seek approval from the Data Commissioner and any other relevant Data Protection Authorities (DPAs) in the countries to which they intend to transfer personal data. Jurisdictional conflicts may arise where these authorities apply different legal standards.

To mitigate against jurisdictional conflicts, organizations are encouraged to:

i) Engage early with the Office and other relevant Data Protection Authorities to clarify expectations and approval requirements.

ii) Align their BCRs with international best practices, to enhance consistency and acceptance across jurisdictions.

iii) Include legal harmonisation clauses in their BCRs to account for and defer to stricter local data protection requirements where applicable.

b) Update to the BCRs.

BCRs should include an obligation that significant changes to the BCRs or to the list of BCR members are notified to all group members and to the relevant supervisory authorities. Any significant changes to the BCRs must be communicated to data subjects. Certain modifications will also require a new approval from the relevant supervisory authorities. Such changes that necessitate the need for new approval may include additional recipient countries, changes that affect the right of data subject and significant changes to the safeguards to protect personal data.

c) Compliance Monitoring and Audit

There must be compliance auditing with BCRs on a regular basis. The process must be documented and reported directly to the ultimate parent's board or to the DPO. The BCRs must also state that the audit program will cover all aspects of the BCRs and ensure that any necessary corrective action will be taken.

Company A is a multinational organization with subsidiaries in multiple countries, including Kenya. To enable seamless data transfers across its subsidiaries, the company has developed Binding Corporate Rules (BCRs) that define the scope of data transfers,

establish their legally binding nature both internally and externally, and outline the application of data protection principles, data subject rights, and complaint-handling procedures.

Furthermore, the company has implemented a compliance monitoring mechanism to ensure adherence to the BCRs throughout the group. These rules serve as a framework governing all data processing and transfer activities across the organization's global operations.

When a transferring entity relies on appropriate safeguards to transfer personal data, it must document the transfer, including the exact date and time, the recipient's name, the justification for the transfer, and a description of the personal data involved. This documentation should be made available to the Data Commissioner upon request.

8.2. Transfer on the basis of an Adequacy Decision

Personal data may be transferred to another country or an international organization if the Data Commissioner has determined that the destination—whether a specific country, a region within it, or an international organization—ensures an adequate level of data protection.

8.3. Transfer as a Necessity

Cross border transfer of personal data may be considered lawful and necessary under the following circumstances:

a) **Performance of a Contract:** The transfer is essential to fulfill a contract between the controller and the data subject or to carry out pre-contractual measures requested by the data subject. Further, the transfer is required for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party.
b) **Establishment, Exercise or Defence of a Legal Claim:** The transfer may be necessary for the establishment, exercise, or defense of a legal claim.
c) **Legitimate Interest Pursued by Data Controller or Processor:** The transfer is based on compelling legitimate interests of the data controller or processor that do not override a data subject's rights and freedoms. Legitimate interest may arise, for example, when a data controller or processor opts to host personal data on cloud servers located outside the country to enhance operational efficiency, improve service effectiveness, and ensure greater convenience.
d) **Protection of the Vital Interest of the Data Subject**: The transfer of personal data may be necessary to protect the vital interests of the data subject or another

individual, especially when the data subject cannot give consent due to physical or legal incapacity. For cross-border personal data transfer, a data controller or processor may use vital interest in exceptional circumstances when it is necessary to protect the life or physical integrity of a data subject. Exceptional circumstances may include emergency situations such as during natural disasters or other crises.

e) **Public Interest -** Cross-border transfer of personal data may be necessary for reasons of public interest in the performance of tasks carried out under the official authority granted to the controller or processor. Examples of public interest situations include matters of public safety, such as during a pandemic, a disease outbreak, or a terrorist threat, where it becomes necessary to transfer personal data across borders to protect public health or prevent the spread of disease.

8.4 Transfer on the basis of Consent

In accordance with section 25(h) of the Act, where there is no adequacy decision, no appropriate safeguards, and no other lawful basis for the transfer, personal data may be transferred to another country only if the data subject has explicitly consented to the proposed transfer and has been informed of the potential risks involved. Furthermore, while transferring sensitive personal data, in line with Section 49 of the Act.

9. Onward Transfers

To maintain the level of protection required under Section 48 of the Act, the binding legal instrument that enabled the transfer must prohibit any onward transfer of the transferred personal data by the data recipient unless ALL of the following conditions are met:

1. **Prior Written Authorisation from the Transferring Entity**

No onward transfer may occur unless the Transferring Entity has provided specific, prior, and written authorisation for the exact third party, location, data categories, and purpose involved.

2. **Equivalent Protection in the Recipient Jurisdiction**

The Data Recipient must conduct a Transfer Impact Assessment (TIA), demonstrating that the onward recipient and the destination jurisdiction ensure a level of protection essentially equivalent to that provided under Section 48 of the Act and the safeguards contained in the contract.

3. **Binding Accession to the Contract**

Before the onward transfer occurs, the onward recipient must:

- formally accede to the same obligations as the Data Recipient,

- be bound by a contract or legal act ensuring at least the same level of protection, including audit rights, liability, sensitive-data protections, and breach-notification obligations.

4. Documentation of Each Onward Transfer

Each authorised onward transfer must be documented as required under Regulation 41(2), including:

- date and time;
- identity and location of the onward recipient;
- justification for the onward transfer;
- data categories and purposes;
- safeguards relied upon.

5. Full Liability of the Data Recipient

The Data Recipient shall remain fully and unconditionally liable for the acts and omissions of all onward recipients, including sub-processors, as if they were its own.

6. Audit Rights Extended to All Onward Recipients

The Transferring Entity's audit and inspection rights under Regulation 48 must extend to every onward recipient, with the Data Recipient ensuring access, cooperation and availability of documentation.

7. Onward Transfers for the Recipient's Own Purposes Are Strictly Prohibited

Onward transfers for the Data Recipient's own purposes—including analytics, commercial exploitation, profiling, product improvement, or marketing—are strictly prohibited.

10.0 Data Localisation

Data localisation is a legislative or regulatory requirement to domicile data within the jurisdiction in which the legal requirement is enacted. Section 50 of the Act requires that personal data for the strategic interests of the state must be domiciled in Kenya. A data controller or data processor who processes personal data for the purpose of strategic interest of the state **must**:

a) Process such personal data through a server and data centre located in Kenya or;
b) Store at least one serving copy of the concerned personal data in a data centre located in Kenya.

Pursuant to regulation 26 of the General regulations, data controllers and processors engaged in processing for the purposes listed below are be deemed to be processing for strategic interest purposes:

a) administering of the civil registration and legal identity management systems;

b) facilitating the conduct of elections for the representation of the people under the Constitution;
c) overseeing any system for administering public finances by any state organ; or
d) running any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act;
e) offering any form of early childhood education and basic education under the Basic Education Act; or
f) provision of primary or secondary health care for a data subject in the country.

Prior to the transfer of personal data across the borders, data controllers and/or data processors must comply with localisation requirements where applicable. To ensure compliance with localisation requirements, the data controllers and/or data processor should conduct assessment based on several important factors. This may include:

- **The purposes of processing:** whether the processing is conducted for the purposes listed under regulation 26.
- **The systems used:** assess the technological infrastructure employed against the systems designated as Critical Information Infrastructure pursuant to the Gazette Notice NO. 1043[1], of the Computer Misuse and Cybercrimes Act, 2018.

Example
A hospital, based in Kenya, has deployed a cloud-based Electronic Medical Records (EMR) system to digitize patient records. The EMR servers are in country X. This approach enhances data accessibility and continuity of patient care. To comply with data localisation requirements, the hospital ensures that it maintains an accurate and up-to-date serving copy of the patient's data.

11.0 Rights of Data Subjects

Section 26 of the Act grants data subject various rights to protect their personal data. In the context of cross-border data transfers, these rights are designed to give data subjects control over their personal information and to ensure transparency and accountability when their data is transferred to other countries. Data handlers must facilitate the

[1] Microsoft Word - Gazette Vol. 21 Special Issue (Admin. Units).doc (nc4.go.ke)

exercise of data subjects' rights by establishing procedures to handle these requests efficiently and within the statutory timeframes.

12.0 Sensitive Personal Data

Sensitive personal data—defined under Section 2 of the Act, is information revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation. These categories of personal data requires heightened protection due to the increased risk of harm in the event of misuse, disclosure, or unauthorised access.

Under Section 49(1) DPA, the cross-border transfer of sensitive personal data requires the explicit consent of the data subject and the obtaining of confirmation of appropriate safeguards. This requirement must be expressly reflected in the Contract and the transfer documentation.

In addition, consistent with the enhanced protections mandated by Sections 25 and Part V of the Act, the Contract must ensure that the processing of sensitive personal data is subject to stricter organisational, technical, administrative, and contractual safeguards than those applicable to ordinary categories of personal data.

These safeguards must be proportionate to the sensitivity of the data and the risks involved in the processing activity, consistent with international high-risk transfer frameworks.

13.0 Compliance Obligations when transferring personal data

13.1. Transfer Agreements

Transfer agreements are legally binding contracts that outline the roles and obligations of the transferring entity and the recipient in the transfer of personal data. These agreements ensure compliance with Section 42 of the Act and Regulation 48 that stipulates the obligations for data controllers and processors to enter into processing agreements.

In respect to cross-border data transfers, Regulation 48 guides that a transferring entity may enter into a written agreement with the recipient of personal data, which shall contain provisions relating to;

a) Allowing the transferring entity unlimited access to verify the recipient's data protection systems, and
b) Clearly identifying recipient countries.

The Office guides that the written agreements should, in clear terms, include the following key aspects to guide cross-border data transfers. These aspects should include, but not be limited to:

a) Conditions of Data Transfers

Processor agreements must clearly define the conditions under which personal data may be transferred across borders. These conditions include:

- Appropriate data protection safeguards;
- transfer as a necessity;
- adequacy decision made by the Data Commissioner; or
- consent of a data subject.

b) Roles of the Transferring and Receiving Parties

The written agreements should outline the roles and responsibilities of both transferring and receiving entities involved in cross-border data transfers, ensuring compliance with data protection laws. These obligations may include:

- Both parties must implement adequate technical and organizational security measures to protect personal data during and after the transfer;
- The receiving party must cooperate with relevant authorities in case of audits, investigations, or legal inquiries;
- Both parties must establish procedures for reporting data breaches in accordance with the law;
- The agreement must specify the obligation to maintain records of processing activities and allow for audits to verify compliance; and
- Upon termination of the agreement, the receiving party must either delete or return the personal data, as instructed by the transferring entity.

c) Technical and Organizational Safeguards

The written agreement should provide clear technical and organizational safeguards that ensure:

- Confidentiality: Personal data is protected from unauthorized access both during and after transfer.

- Integrity: The personal data being transferred should not be altered or tampered with.
- Availability: Personal data should remain accessible and usable only for authorized purposes, ensuring data continuity even after the transfer.

Both parties must ensure that these protections are upheld not only within their own systems but also in any subsequent transfers to third parties (onward transfers).

d) Termination and Consequences

The written agreement must specify how the personal data will be handled after the contract ends. This includes:

- Data Deletion or Return: The receiving party must return or securely delete all personal data received under the agreement, as per the instructions of the transferring entity.
- Ongoing Obligations: Some obligations (such as confidentiality) may continue after the agreement is terminated.

e) Indemnity and Liability

Transfer agreements must clearly outline the liability of both parties during the data transfers in the event of non-compliance and data breaches, including obligations to compensate for the data subjects.

Each party's liability should be clearly defined to avoid disputes, including clauses on indemnification for financial and reputational damages.

13.2. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a critical process for evaluating the potential risks and protections involved when transferring personal data across international borders. Section 31 of the Act and Part VIII of the Regulations outline that for high-risk processing activities, the data handler should conduct a DPIA to assess and mitigate privacy risks associated with the transfer. This is crucial in protecting data subjects' rights and maintaining the integrity of personal data throughout the transfer process.

The Office has published a Guidance Note on DPIA available on www.odpc.go.ke.

13.3. Transfer Documentation

When an organisation transfers personal data outside the country, it must keep proper records of that transfer. Under Regulation 41 (2), the organisation shall

(a) formally document the transfer

(b) the documentation shall be provided to the Commissioner on request; and

(c) the documentation shall include

(i) the date and time of the transfer;

(ii) the name of the recipient;

(iii) the justification for the transfer; and

(iv) a description of the personal data transferred.

13.4. Demonstrations of safeguards (prior, during and after)

Before undertaking any transfer of personal data, a data controller or data processor shall demonstrate to the Data Commissioner, upon request, that appropriate safeguards are in place to ensure the security and protection of the data. Data handlers must establish and provide evidence of these safeguards prior to transferring personal data outside Kenya.

14.0 Considerations for Cloud Storage

The processing of personal data in cloud environments with servers located outside Kenya constitutes a cross-border data transfer. Data handlers share responsibility with cloud service providers for protecting personal data. This includes due diligence before engagement and continuous monitoring of provider compliance throughout the contract period.

14.1 Cloud Service Models

Cloud service models include the following:

a) Infrastructure as a Service (IaaS)
b) Platform as a Service (PaaS)
c) Software as a Service (SaaS)

Users of IaaS and PaaS typically retain greater control over their systems and data. Conversely, SaaS users rely on provider-managed software and infrastructure, which may limit direct control over personal data. Accordingly, controllers using SaaS should conduct risk assessments and implement mitigation measures to address reduced control and higher dependency on the provider.

14.2 Deployment Models

Cloud deployment models generally fall into two categories: public and private.

A **private cloud** is dedicated to a single organisation and is either managed internally or by a third party on its behalf. This model offers greater control over data handling and typically provides stronger privacy protections.

A **public cloud**, on the other hand, is operated for use by multiple organisations on a shared infrastructure. Because resources are shared among different users, this model may present increased privacy and data protection risks

Data controllers considering public clouds must perform thorough privacy risk assessments and implement appropriate safeguards before adoption.

14.3 Key Security Measures

i. **Logging** - Data controllers should ensure that audit trails provided by cloud service providers are retained, such as user login history and personal data change history. These logs should be reviewed regularly to detect abnormal activities and aid in investigations in an event of authorized access.

ii. **Appropriate user configuration** - Data controllers should thoroughly understand the functions of the configurations and ensure that their access to cloud services is correctly configured. Additionally, access should only be granted to authorised individuals, especially those who have operational needs to access the cloud services.

iii. **Encryption in transit and at rest** - Unprotected data, whether in transit or at rest, can expose an organisations to risks. As cloud computing provides services through the internet, personal data should be encrypted during transmission to avoid eavesdropping or man-in the-middle attacks. To protect data at rest, personal data should be encrypted when stored on the cloud to prevent unauthorised access from attackers, and it is also recommended that data controllers choose service providers that offer encryption at rest in their services.

iv. **Multi-factor Authentication (MFA) -** MFA should be considered and enabled for as many accounts as possible.

v. **Anonymisation** - Anonymisation provides an extra layer of security to the personal data stored on a cloud. Anonymising personal data means removing from the dataset any information from which an individual may be identified by anyone reading the record, taking re-identification risks into account.

vi. **Backup** - Effective backup and recovery policies and procedures should be developed by cloud service providers. For personal data stored on a cloud that are considered critical, the data controllers should ensure that an offline backup copy of the data can be obtained from the cloud service providers and restored when needed.

14.4 Compliance Requirements

Before transferring personal data to a cloud environment, data controllers and processors should:

- Establish a lawful basis for processing and ensure compliance with cross-border transfer conditions under the Act.
- Engage only providers who demonstrate adequate technical and organizational safeguards.
- Enter into Data Processing Agreements (DPAs) specifying roles, responsibilities, and compliance obligations.
- Regularly review terms of service and provider sub-processor arrangements to confirm continued compliance.
- Ensure data subjects can exercise their rights regardless of data storage location, supported by documented response procedures.
- Conduct Data Protection Impact Assessments (DPIAs) for all cloud deployments involving cross-border data transfers.
- Implement a data retention policy defining retention periods and secure deletion timelines, supported by lifecycle automation tools.
- Provide periodic employee training on secure cloud data handling and compliance with the Data Protection Act.
- Monitor provider changes, update system configurations, and reassess risks accordingly to maintain continuous compliance.

ANNEX 1: COMPLIANCE CHECKLIST

QUESTIONS	RESPONSES
1. Legal Basis for Transfer Have you identified a legal basis for transferring the data under Part VI of the Act and Regulation 40 of the Data Protection (General) Regulations?	❑ **Yes**: Proceed. ❑ **No**: A legal basis must be established before transferring data.

2. Data Subject Consent (if required) Have you obtained **explicit consent** from the data subject for the cross-border transfer of their personal data (if consent is required)?	❑ **Yes**: Ensure consent is informed, specific, and voluntary. ❑ **No**: Consent may not be necessary if another legal basis is established other than for sensitive personal data
3. Transfer as a Necessity Is the transfer **necessary** for the performance of a contract, public interest, or legal claims?	❑ Yes: Verify and document the necessity. ❑ No: Move to other conditions or safeguards.
4. Appropriate Safeguards Have you implemented and documented **adequate safeguards** for the data transfer? *(tick where appropriate)*	❑ Equivalent data protection laws ❑ Binding Corporate Rules (BCRs) ❑ Technical safeguards (e.g., encryption, pseudonymization)? ❑ Organizational safeguards (e.g., employee training, access controls)?
5. Deemed Appropriate Safeguards Is the receiving country or territory **deemed adequate** regarding data protection, as defined by Act?	❑ **Yes**: You may transfer the data without additional safeguards. ❑ **No**: Implement appropriate safeguards.
6. Data Processing Agreement Have you entered into a **Data Processing Agreement** with the receiving party, as required under Section 42 of the Act? •	❑ **Yes**: Ensure the agreement includes provisions related to cross-border transfers, including access to the recipient's information systems, and specifies onward transfers. ❑ **No**: Draft and implement a compliant data processing agreement.
7. Technical and Organizational Security Measures Have you implemented **technical and organizational security measures** to ensure the protection of the data being transferred? *(tick where appropriate)*	❑ **Encryption** during transfer? ❑ **Pseudonymization** where applicable? ❑ **Access controls** to limit who can view or process the data?

	❑ **Incident response plan** in case of a data breach?
8. Risk Assessment (TIA) (if applicable) Have you conducted a **Transfer Impact Assessment (TIA)** to evaluate the potential risks and benefits of the data transfer, especially if the receiving country has weaker data protection laws?	❑ **Yes**: Ensure the assessment covers legal, organizational, and technical aspects. ❑ **No**: Conduct a TIA to identify and mitigate risks.
9. Data Subject Rights Are you ensuring that the **rights of data subjects** are respected throughout the data transfer process, including the right to access, rectification, and erasure of data?	❑ **Yes**: Ensure mechanisms are in place to address these rights in the receiving country. ❑ **No**: Implement procedures to handle data subject rights.
10. Third-Party Transfers (Onward Transfers) If the recipient of the data will further transfer it to a third party, have you included provisions in the agreement to govern **onward transfers**?	❑ **Yes**: Ensure adequate safeguards are in place for any onward transfers. ❑ **No**: Address onward transfers in the agreement.
11. Audit and Monitoring Have you established procedures for **auditing** and **monitoring** the cross-border data transfer process to ensure ongoing compliance?	❑ **Yes**: Schedule regular audits and monitoring of data transfers. ❑ **No**: Implement monitoring processes and ensure access to records of processing activities.
12. Data Breach Notification Do you have a **data breach notification** plan in place, including notifying the Data Protection Commissioner and affected data subjects in case of a breach during or after the transfer?	❑ **Yes**: Ensure all relevant parties are informed of the plan. ❑ **No**: Develop and implement a breach notification procedure.
13. Re-evaluate the Transfer	❑ **Yes**: Set a review schedule.

Have you planned for periodic **re-evaluation** of the transfer to ensure continued compliance with Kenya's data protection laws, especially if the legal environment changes in the receiving country?	❑ **No**: Establish a timeline for re-evaluating the transfer.

ANNEX 2: GAZETTE NOTICE - DESIGNATION OF CRITICAL INFRASTRUCTURE

ANNEX 3: BCR APPLICATION FORMS

Application Form for Approval of Binding Corporate Rules (BCRs) for Data Controllers

Under the Data Protection Act and Regulations, Binding Corporate Rules (BCRs) are one of the mechanisms for ensuring appropriate safeguards are in place for intra-group transfers. BCRs are suitable for use by a group of undertakings or a group of enterprises engaged in a joint economic activity.

To be valid, BCRs must comply with Section 48 of the Act, Regulations 40 to 43, and any guidance issued by the Office of the Data Protection Commissioner (ODPC). The ODPC reviews and approves BCRs for Controllers (BCR-C) and for Processors (BCR-P).

The purpose of this application form is to help applicants demonstrate how their proposed BCRs meet the legal and regulatory requirements.

Instructions

- *If you are unsure whether BCRs are suitable for your group, please contact the ODPC at compliance@odpc.go.ke for guidance before submitting this form.*
- *When completing the form, applicants shall provide references to specific sections of the BCRs and other annexes where relevant.*
- *This application form is made available on the ODPC website in editable Word format to ensure that any interested party can easily complete it. Applicants are encouraged to use as much space as necessary when providing information and justifications, taking into account the particular circumstances of their processing activities.*
- *Applicants must submit one electronic or physical copy of the completed and signed application form, BCRs, and other annexes to the ODPC. Providing a list of all entities within the group that are bound by the BCRs, together with their registration details and addresses, is also mandatory.*

- *Where applicable, applicants can indicate any parts of the submission that contain confidential information. The ODPC will handle such information in accordance with the law.*
- *If you wish to apply for BCRs for Processors (BCR-P) instead of, or in addition to, BCRs for Controllers, a separate application form and BCR documentation must be submitted. The ODPC will not accept a single set of BCRs that attempts to cover both Controllers and Processors in the same document.*

Section 1: Applicant Information

- Name of the Group: .....
- Address of Group Headquarters: .....
- Name of the Kenyan applicant entity: .....
- Physical address of the Kenyan applicant entity: .....
- Business Registration Service Number (BRS) of applicant: .....
- Is the applicant registered as a data controller with the ODPC?

  ☐ Yes ☐ No

  If the answer is yes, indicate the registration number of the applicant: .....

  If the answer is no, provide reasoning:
- Legal nature of the applicant (company, partnership, charity, etc.): .....
- Description of applicant's position within the Group (include organogram/structure as annex): .....
- Contact person for this application:
  - Name:
  - Title (CEO, DPO, lawyer):
  - Address:
  - Email:

- Phone:

Section 2: Description of Processing and Data Flows

Provide details of the nature and scope of personal data covered by the BCRs, including:

- Expected nature and categories of personal data covered by the BCRs (e.g., HR data, customer data, sensitive data):
- Expected categories of data subjects (employees, customers, suppliers, etc.) concerned:

For each data subject category, specify:

- Categories (sensitive, non-sensitive) and types of personal data (name, address, date of birth, etc):
- Any children's data processed (if applicable):
- Purposes of processing:
- Processing operations (e.g., collection, storage, transfer):
- Legal bases for processing data:
- Do you currently transfer data from Kenya? ☐ Yes ☐ No

  If yes, what data transfer legal bases or safeguards do you rely on:

- Purpose of intended transfers under BCRs and subsequent processing:
- List all group members and countries to which data may be transferred under BCRs:
- Will the BCRs apply to: ☐ Transfers from Kenya only ☐ All intra-group transfers
- Have the BCRs of the Group relating to the same categories of data subjects and personal data been submitted to any other supervisory authority for approval?

  ☐ Yes ☐ No

  If the answer is yes, specify the authority and provide the status of the application or details of the outcome:

Section 3: Binding Nature of the BCRs

- Explain how the BCRs are legally binding upon the members of the Group? (intra-group agreements, contracts, unilateral declaration, etc.):
- Provide a list of group members bound, with company registration and contact details (include the list, addresses, and other details of relevant group members as an annex):
- If some Group members are exempted, specify which, how and why:
- Describe how BCRs bind employees (contracts, confidentiality undertakings, disciplinary sanctions):
- Explain binding effect on processors/sub-processors (contractual clauses, sanctions for non-compliance):
- Explain external enforceability: data subjects' rights, complaint handling mechanisms, and access to judicial/non-judicial redress and remedies in Kenya:
- Confirm that a Kenyan entity (applicant) has sufficient capabilities (including financial) to accept liability for infringements and undertakes to provide remedies/compensation

  ☐ Yes ☐ No

  If the answer is yes, demonstrate capabilities (including financial):

  If the answer is no, explain how the Group ensures that liability is actioned:

Section 4: Effectiveness

Explain how BCRs are implemented in practice including but not limited:

- Internal compliance structures and mechanisms (procedures, steering, audits):
- Training and awareness programs (frequency, scope, staff categories):
- Complaint handling mechanisms, including the process for escalating issues to the ODPC:
- Audit and verification systems (internal/external auditors, DPO network):

- Are BCRs incorporated into relevant policies? ☐ Yes ☐ No

If the answer is yes, provide the list or relevant policies (e.g. privacy policy, HR Policy, cyber security policy):

If the answer is no, please explain the reasoning and provide details:

Section 5: Reporting and Recording Changes

- Describe mechanisms to record and communicate changes to BCRs among the group members:
- Indicate reporting obligations on the changes to BCRs to the ODPC:
- Explain internal responsibilities for monitoring and reporting:

Section 6: Data Protection Safeguards

Explain how BCRs address:

- Lawfulness, fairness, transparency:
- Purpose limitation:
- Data minimisation:
- Data accuracy:
- Storage limitation:
- Integrity, confidentiality, and security safeguards:
- Processing of special categories and children's data:
- Breach notification to ODPC and affected data subjects:
- Restrictions on onward transfers:
- Other relevant safeguards:

Section 7: Accountability and Related Tools

For accountability purposes, the following tools should be deployed.

- Data Protection Impact Assessments for high-risk processing:
- Consultation with ODPC where risks remain:
- Technical and organisational measures for data security

- Data protection by design and by default principles:
- Availability of privacy policies, notices, and information about data processing to data subjects:
- Record-keeping obligations:
- Mechanisms in place to be responsible for and demonstrate compliance with BCRs:
- Explain how the BCRs provide for cooperation with the ODPC:
- Explain mechanisms for notifying the ODPC if local laws in third countries conflict with safeguards under BCRs.

Section 8: Data Protection Officer

- Confirm the Kenyan applicant entity has designated a data protection officer (DPO)

  ☐ Yes ☐ No

  If the answer is no, please explain the reasoning:

  If the answer is yes, confirm that you have already communicated the DPO's contact details to ODPC.

  ☐ Yes ☐ No

- Confirm that a DPO, network of DPOs, or a network of staff members designated for privacy issues is appointed with top management support to oversee and advice on compliance with the BCRs:

  ☐ Yes ☐ No

If the answer is yes, explain how the DPO, network of DPOs, or a network of staff members designated for privacy issues will operate.

If the answer is no, explain the reasoning and explain who would oversee and advise on compliance with the BCRs.

ANNEXES

1. Copy of the Binding Corporate Rules for the Data Controllers.
2. Binding mechanism (intra-group agreement/unilateral declaration).

3. List of entities bound by the BCRs and their addresses.
4. Organogram of group structure.
5. Extracts from separate or collective agreements or a clause in an employment contract to demonstrate that BCRs are binding on both permanent and temporary employees.
6. Ancillary documents (policies, training materials, audit frameworks) (optional)

Acknowledgement

We hereby submit this application for the ODPC approval of Binding Corporate Rules under Section 48 of the Data Protection Act, 2019, and Regulations 40–43 of the Data Protection (General) Regulations, 2021.

We acknowledge and confirm that:

- Applicant is authorised to submit the application.
- Information provided in this application is accurate and complete.
- Approval covers only transfers under these BCRs and does not replace compliance with other Kenyan Data Protection Act obligations.
- Each data transferring entity must assess third-country laws to ensure compliance.
- Transfers must stop if adequate protection cannot be ensured.
- The ODPC needs to be provided, upon request, with information and audit reports without restriction.
- The ODPC has the authority to conduct audits, inspections, and investigations to ensure compliance with BCRs.
- Group members shall comply with the ODPC directions, instructions, decisions, or enforcement and penalty notices.

Signature: _____

Name: _____

Position: _____

Date: _____