REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Notes for Cross-border Data Transfers

2026

TABLE OF CONTENTS

DEFINATION OF TERMS

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

"Audit" means the Data Protection Compliance Audit as provided for in Section 23 of the Act;

"Consent" means any manifestation of express, unequivocal, free, specific, and informed indication of the data subject's wishes by a statement or by clear affirmative action, signifying agreement to the processing of personal data relating to a data subject

"Cookies" are small text files that websites store on your device when you visit them. They help remember things like your login details, preferences, and browsing history to make your experience smoother and more personalized.

"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 that, 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 Processor" means a natural or legal person, public authority, agency, or other body that 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.

"Institution/Entity/ Organisation" means a legal person, public authority, agency, or other body that processes personal data.

"Information Communication & Technology Policy (ICT Policy)" means a set of guidelines, strategies, and procedures managing an organisation's technology infrastructure, including hardware, software, and networks

"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.

"Privacy Notice (or Privacy Statement)" is an *outward-facing* document intended for data subjects/users generally. It explains how an organisation processes personal data (e.g. collects, uses, stores etc), in compliance the duty to notify under Section 29 of the Data Protection Act, 2019.

"Data Protection Policy", is an internal document designed for use within the organisation. It guides employees, management and internal stakeholders on how to handle personal data and ensure compliance with the Data Protection Act, 2019 and the relevant Regulations.

"Regulations" means all the regulations enacted in accordance with section 71 of the Act.

"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.

"The Office" means the Office of the Data Protection Commissioner.

"Review" means evaluating documentation to ensure compliance with relevant standards or requirements.

FORWARD

The rapid digitalisation of economies and the growing flow of personal data across national borders present both opportunities and challenges for data protection. As Kenya continues to integrate into the global digital economy, ensuring that cross-border transfers of personal data uphold the data privacy and protection standards remains a core interest and mandate of the Office of the Data Protection Commissioner.

The Data Protection Act, 2019, and the Data Protection (General) Regulations, 2021 establish the legal framework governing the transfer of personal data outside Kenya. These provisions seek to strike a balance between enabling the free flow of data necessary for trade, innovation, and service delivery, and safeguarding the privacy and security of personal data.

This Guidance Note has been developed to assist data controllers and data processors in understanding their obligations when transferring personal data. It provides practical guidance on the conditions for lawful cross-border transfers, the safeguards that must be in place, and the mechanisms available to ensure adequate protection of personal data in the recipient country or organisation.

The guidance is not intended to replace or override the provisions of the Act or the General Regulations. Rather, it serves as a complementary resource to promote compliance and as an added resource to foster public trust in the handling of personal data across jurisdictions.

I would like to thank all the stakeholders who have contributed to its development and the furtherance of discussions on cross-border data flows.

Immaculate Kassait, SC, MBS
Data Commissioner

DEFINITION OF TERMS

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

"**Adequacy Decision**" is a formal determination by the Data Commissioner that a foreign country, region, or international organization ensures a level of personal data protection essentially equivalent to Kenya's Data Protection Act and Regulations.

"**Binding Corporate Rule**s" Binding Corporate Rules" means personal data protection policies adhered to by a data controller or data processor that is subject to the Act, 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 to remotely store, process, or distribute 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 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, the sexual orientation of the Data Subject. This includes personal data prescribed as sensitive personal data by the Data Commissioner pursuant to Section 47 of the Data Protection Act.

"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.

INTRODUCTION

Cross-border transfer of personal data involves the transmission, access, or making available of personal data from Kenya to a recipient located outside Kenya. Cross-border transfers are an integral part of today's digital economy and occur in many situations, including when businesses operate in multiple jurisdictions, in outsourcing arrangements, in the delivery of digital services across jurisdictions, in the use of cloud computing, 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. Cross-border transfer of personal data 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 organisations in cloud environments. This risk is often compounded by the lack of adequate data security measures and the involvement of parties in cross-border transfers 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.

PRIVACY CONCERNS

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

1. **Lack of transparency and purpose deviation** – Personal data transferred for a specified and legitimate purpose may be further processed for incompatible purposes without the knowledge or consent of the data subject, resulting in misuse, unlawful processing, and potential breaches of the purpose limitation, lawfulness, fairness and transparency principles.

2. **Limited data subject control and visibility** – Data subjects may lack adequate information regarding the location, recipients, and legal basis of cross-border data transfers, limiting their ability to exercise rights such as access, objection, withdrawal of consent, and redress.

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-** Where the destination country does not provide an adequate level of data protection, or where legal safeguards, independent oversight, effective remedies for data subjects, or limitations on access by public authorities are insufficient, transferred personal data may face a higher risk of misuse, unauthorised access or unlawful processing.

5. **Onward transfers to third parties** – Once personal data has been transferred to a recipient outside Kenya, there is a risk that it may be further transferred to other controllers or processors in additional jurisdictions without adequate safeguards or authorisation.

6. **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.

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 and foreign data received in Kenya.

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.

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 in relation to information concerning their family or private affairs, and protect them from unnecessary disclosure of such information or unlawful interference with the privacy of their communications.

b) **Article 35** It provides that every citizen has the right to access information held by the State, as well as information held by another person where such information is required for the exercise or protection of any right or fundamental freedom.

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

The Data Protection (General) Regulations, 2021. This operationalizes the Data Protection Act by prescribing 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 conditions for lawful cross-border transfers and mandatory registration with the Office.

The Data Protection (Complaints Handling and Enforcement Procedures) Regulations 2021. Provide Complaints Handling and Enforcement Procedures

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 misuse and cybercrimes; and facilitate international cooperation in dealing with computer misuse and cybercrime.

e) **Kenya Cloud Policy 2025 -** 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, foster interoperability and strengthen collaboration across nations, and complement other relevant existing cloud computing regulations.

APPLICATION OF DATA PROTECTION PRINCIPLES

1.1. **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.

1.2. **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. Where the transfer purpose is incompatible with the original purpose, ensure the data subject is informed and a risk assessment is conducted where necessary.

1.3. **Data Minimisation**

This principle dictates that organisations should only collect and transfer personal data that is strictly necessary for a clear and lawful purpose across borders. Transferring entities must ensure that only the minimum, strictly necessary personal data is collected and transmitted across borders, with clear justification documented for each category of data.

1.4. **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.

1.5. **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.

1.6. **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.

1.7. **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.

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 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.

Appropriate Data Protection Safeguards

When relying on appropriate safeguards to transfer personal data in and out 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

To facilitate the implementation of Regulation 40(a), the Office has developed **Standard Clauses for Legal Instruments Containing Appropriate Safeguards for Cross-Border Transfers of Personal Data**, annexed to this Guidance. These standard clauses are intended to be incorporated into a legal instrument between the transferring entity and the recipient to establish appropriate safeguards in accordance with the Act and the Regulations. The annexes include:

- **Annex 15.4 – Standard Clauses for Legal Instruments Containing Appropriate Safeguards for Controller-to-Controller Transfers;** and
- **Annex 15.5 – Standard Clauses for Legal Instruments Containing Appropriate Safeguards for Controller-to-Processor Transfers.**

When evaluating whether adequate safeguards exist under Regulation 40(b), a transferring entity should take into account all relevant circumstances of the transfer, including the legal and regulatory framework applicable in the destination country, the nature and sensitivity of the personal data, the enforceability of the safeguards, the technical and organisational measures implemented by the recipient, the likelihood of onward transfers, and the availability of effective remedies for data subjects.

In addition, a country or territory may be considered to have appropriate data protection safeguards where it has:

i. ratified and fully implemented the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention);

ii. entered into a reciprocal data protection agreement with Kenya; or

iii. implemented binding corporate rules within a concerned group of undertakings or enterprises.

a) 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, protects personal data, and promotes secure digital transformation across Africa.

While the convention is one of the mechanisms that are deemed appropriate for data transfer, the Data Commissioner retains discretionary authority on such transfer. Pursuant to Section 49(2) of the Act, the Data Commissioner can assess and determine the adequacy on a case-by-case basis. The Data Commissioner maintains oversight and ensures that even where a lawful basis for transfer, like compelling legitimate interests under Section 48 is claimed, the security safeguards are genuinely effective and the legal basis is correctly applied.

Section 49(3) of the Act, provides that the Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined. This provision is critical because it gives the Data Commissioner the ultimate supervisory authority over international data transfers, even when a data controller or processor presupposes that they have complied with the requirements of Sections 48 and 49.

Moreover, Part 5 of the Data Sharing Code, 2025, developed pursuant to Section 55 of the Act, prescribes conditions for cross-border sharing of personal data, which include that where a recipient country or organisation does not have an adequate level of protection, the data controller or processor must implement appropriate safeguards to protect the personal data during the transfer and processing.

In addition, data controllers and data processors that transfer personal data outside Kenya are required to notify the Office of the Data Protection Commissioner of the transfer to ensure that the Office is aware of cross-border data flows and can monitor compliance with the Act. Enforcement of non-compliance with the Data Sharing Code is anchored in Section 58 of the Act, as highlighted in Part 6 of the Data Sharing Code, 2025.

Under the Convention, protection of privacy rights in cross-border transfers falls within the ambit of national data protection legislation. This includes:

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

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.

b) 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 42(b), which empowers the Office to assess and approve mechanisms that ensure adequate protection of personal data transferred outside Kenya.

c) 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 of undertakings or enterprises engaged in a joint economic activity. BCRs are legally binding and enforceable internal rules and policies adopted by multinational corporations/groups to regulate intra-group transfer of personal data across different jurisdictions while ensuring a consistent level of data protection.

Elements of Valid BCRs

For BCR to be valid, the following elements 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 for 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 legal requirements in a third country that are likely to adversely affect the level of protection

guaranteed by the BCRs will be reported to the ODPC and, where applicable, any other 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.

- **Cooperation with supervisory authorities:** The BCRs should include a commitment by all members of the group to cooperate with the ODPC and any other competent supervisory authorities in relation to the implementation and enforcement of the BCRs.

- **Liability:** The BCRs should clearly identify the entity responsible for accepting liability for breaches of the BCRs and for providing effective remedies and compensation to affected data subjects where required.

BCRs are particularly suitable for multinational groups that regularly transfer personal data between affiliated entities across multiple jurisdictions. They provide a single, organisation-wide framework for ensuring compliance with applicable data protection requirements and reducing the need to negotiate separate contractual safeguards for each intra-group transfer.

Where transfers take place outside a corporate group, or where BCRs have not been adopted, organisations may instead rely on other appropriate safeguards, including the Standard Clauses for Legal Instruments Containing Appropriate Safeguards for Cross-Border Transfers of Personal Data annexed to this Guidance.

i. Approval of the BCRs

After developing BCRs, organisations are required to obtain the approval of the ODPC. Where the proposed cross-border transfers involve jurisdictions whose legal frameworks require approval or recognition by another competent supervisory authority, organisations should also comply with those applicable requirements.

Given that different jurisdictions may apply varying legal standards and procedural requirements for the approval or recognition of BCRs, organisations are encouraged to:

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

- Align their BCRs with international best practices to enhance consistency and acceptance across jurisdictions.

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

ii. Update to the BCRs.

BCRs should include a mechanism for ensuring that any significant changes to the BCRs or to the list of entities bound by the BCRs are notified without undue delay to all relevant group members and to the ODPC, and where applicable, other relevant supervisory authorities. Any

material changes affecting data subject rights, categories of transferred data, the purposes of processing, transfer destinations or the safeguards provided under the BCRs shall be communicated to data subjects. Certain modifications will also require a new approval from the ODPC and relevant supervisory authorities. Such changes that necessitate the need for new approval may include the addition of new recipient countries or territories, changes that affect the rights of data subject, significant changes to the safeguards to protect personal data or substantial changes to the scope or operation of the BCRs

iii. Compliance Monitoring and Audit

BCRs should provide for regular monitoring of compliance and periodic audits to verify their effective implementation across all entities bound by the BCRs. 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.

Transfer on the basis of an Adequacy Decision

Personal data may be transferred to another country or an international organisation 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.

The Data Commissioner may publish a list of countries, territories, sectors, or international organisations that have been assessed and found to provide an adequate level of data protection for cross-border data transfers.

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. This public interest must be proportionate, necessary, documented, and authorised under a clear legal mandate. 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.

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, ensure it is in line with Section 49 of the Act.

Onward Transfers

Onward transfer is the subsequent transfer of personal data by the data recipient to an external third party or destination jurisdiction after the initial cross-border transfer has occurred. 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:

a) **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.

b) **Equivalent Protection in the Recipient Jurisdiction -** The Data Recipient must conduct a risk assessment, 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.

c) **Binding Accession to the Contract -** Before the onward transfer occurs, the onward recipient must formally accede to the same obligations as the Data Recipient, and 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.

d) **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.

e) **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.

f) **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.

g) **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.

h) **Suspension or Termination of Onward Transfers –** Where the Data Recipient becomes aware that an onward recipient can no longer comply with the applicable safeguards, it shall suspend the onward transfer or terminate the arrangement without undue delay and take appropriate measures to protect the transferred personal data.

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 a 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.

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

Rights of Data Subjects

Section 26 of the Act grants data subjects 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 exercise of data subjects' rights by establishing procedures to handle these requests efficiently and within the statutory timeframes.

Sensitive Personal Data

Sensitive personal data as defined under Section 2 of the Act, is information revealing the natural person's race, health status, ethnic or 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.

Further categories of sensitive personal data

Section 47 of the Data Protection Act, 2019 allows the Data Commissioner to specify additional categories of sensitive personal data, which may require additional safeguards or restrictions.

In prescribing additional categories of sensitive personal data, the Data Commissioner may specify any further grounds on which such specified categories may be processed, having regard to:

a) to the risk of significant harm that may be caused to a data subject by the processing of such category of personal data;
b) to the expectation of confidentiality attached to such a category of personal data;
c) to whether a significantly discernible class of data subjects may suffer significant harm from the processing of such category of personal data;
d) to the adequacy of protection afforded by ordinary provisions applicable to personal data.

Transfer of sensitive personal data

Under Section 49(1) of the Act, 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.

Compliance Obligations when transferring personal data

The following are key compliance obligations when transferring personal data

1.14 Legal Instruments Containing Appropriate Safeguards

Where a transferring entity relies on appropriate safeguards under Regulation 40 of the General regulations, the cross-border transfer should be governed by a **legal instrument containing appropriate safeguards** between the transferring entity and the recipient.

Such legal instruments should clearly define the rights and obligations of the parties and ensure that the transferred personal data continues to receive a level of protection essentially equivalent to that provided under the Act and the Regulations. They should also satisfy the minimum contractual requirements set out in Regulation 48, including provisions relating to the transferring entity's right to verify the recipient's data protection measures and the identification of the recipient country or countries.

As mentioned, to facilitate compliance with these requirements, the Office has developed **Standard Clauses for Legal Instruments Containing Appropriate Safeguards for Cross-Border Transfers of Personal Data**, annexed to this Guidance. Organisations relying on appropriate safeguards are encouraged to incorporate these clauses into their legal instruments, adapting them where necessary to reflect the specific circumstances of the transfer.

A legal instrument governing a cross-border transfer should, as appropriate, address matters including:

- the legal basis and conditions for the transfer;
- the roles and responsibilities of the parties;
- the categories of personal data and purposes of processing;
- technical and organisational security measures;
- restrictions on onward transfers;
- data subject rights;
- audit and verification mechanisms;
- personal data breach notification;
- liability and indemnification;
- return or deletion of personal data upon termination; and
- dispute resolution and governing law.

1.15 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 General 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 where such transfer may result in high risk to the right and freedom of the data subject. 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.

1.16 Transfer Documentation

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

a) formally document the transfer
b) the documentation shall be provided to the Data 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.

1.17 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.

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 the provider compliance throughout the contract period.

Cloud Service Models

Cloud service models include the following:

i. Infrastructure as a Service (IaaS)
ii. Platform as a Service (PaaS)
iii. 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.

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. Due to sharing of the resources 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.

Key Security Measures

a) **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.

b) **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.

c) **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.

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

e) **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.

f) **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.

Compliance Requirements on cloud storage

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 organisational 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 where the storage entails high risk processing.
- 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.

ANNEXES

Compliance Checklist

The following compliance checklist is a useful tool which organisations may use to check their compliance with cross-border data transfer requirements under the Act and Regulations, as well as the best-practice recommendations under this Guidance Note.

Gazette Notice No. 1043, of 31st January, 2022 Vol. CXXIV—No 21:-
Designation of Critical Infrastructure

Kenya_Gazette_Vol_C
XXVIINo_83_250614_

BCRs Application Forms

OFFICE OF THE DATA PROTECTION COMMISSIONER

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 to the Application Form

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: _____

Standard Clauses for Legal Instruments Containing Appropriate Safeguards for Data Controller to Data Controller Cross-Border Transfers of Personal Data

PART I – GENERAL PROVISIONS

Clause 1. Purpose and Scope

1.1 These Standard Clauses establish appropriate safeguards for the cross-border transfer of personal data between data controllers in accordance with Part VI of the Data Protection Act, 2019 (the Act) and the Data Protection (General) Regulations, 2021 (the General Regulations).

1.2 These Standard Clauses are intended to be incorporated into a legally binding instrument between a Transferring Entity and a Data Recipient where appropriate safeguards are relied upon as the legal basis for a cross-border transfer of personal data under Regulation 40(a) of the General regulations.

1.3 These Standard Clauses apply solely to the cross-border transfer of personal data described in **Annex I** and form an integral part of the legal instrument between the Parties.

1.4 These Standard Clauses shall not be interpreted as limiting or excluding any obligation imposed on either Party under the Act, and it's attendant Regulations, or any other applicable law providing a higher level of protection for personal data.

Clause 2. Definitions and Interpretation

2.1 Unless otherwise defined in these Standard Clauses, the terms used herein shall have the meanings assigned to them in the Act, the Regulations and the Guidance on Cross-Border Transfers of Personal Data issued by the Office of the Data Protection Commissioner.

2.2 For the purposes of these Standard Clauses:

a) **"Legal Instrument"** means the legally binding agreement between the Transferring Entity and the Data Recipient into which these Standard Clauses are incorporated.

b) **"Party"** means either the Transferring Entity or the Data Recipient, and **"Parties"** means both collectively.

c) **"Standard Clauses"** means these Standard Clauses for Legal Instruments Containing Appropriate Safeguards for Controller-to-Controller Cross-Border Transfers of Personal Data.

2.3 These Standard Clauses shall be interpreted in a manner that gives effect to the objectives and principles of the Act and the Regulations. In the event of any inconsistency between these Standard Clauses and the Act or the Regulations, the provisions of the Act and the Regulations shall prevail.

Clause 3. Hierarchy

3.1 These Standard Clauses form part of the Legal Instrument between the Parties and shall prevail over any contractual provision that is inconsistent with them, unless such provision affords a higher level of protection for personal data.

3.2 Nothing in the Legal Instrument shall reduce or limit the level of protection afforded to personal data under these Standard Clauses, the Act or the Regulations.

Clause 4. Description of the Transfer

4.1 The Parties shall complete **Annex I** with accurate and up-to-date information describing the cross-border transfer of personal data and the safeguards applicable to the transfer.

4.2 **Annex I** shall form an integral part of these Standard Clauses.

Clause 5. Duration

5.1 These Standard Clauses shall remain in force for as long as the Data Recipient processes personal data transferred under the Legal Instrument, unless terminated in accordance with its terms.

5.2 The termination of the Legal Instrument shall not relieve either Party of any obligation under these Standard Clauses that is intended to survive termination, including obligations relating to confidentiality, security, liability, data subject rights, the return or deletion of personal data, and cooperation with the Office of the Data Protection Commissioner.

PART II – APPROPRIATE SAFEGUARDS

Clause 6. Lawfulness, Fairness and Transparency

6.1 Each Party shall ensure that personal data transferred under the Legal Instrument is processed lawfully, fairly and in a transparent manner, in accordance with the Act, the Regulations and these Standard Clauses.

6.2 The Data Recipient shall process the transferred personal data only where there is a lawful basis for such processing under the Act.

6.3 The Parties shall ensure that data subjects are provided with the information required under the Act concerning the cross-border transfer and subsequent processing of their personal data, unless an exemption under the Act applies.

6.4 The Data Recipient shall cooperate with the Transferring Entity in providing any information reasonably required to demonstrate compliance with this Clause.

Clause 7. Purpose Limitation

7.1 The Data Recipient shall process the transferred personal data solely for the purposes specified in Annex I or for any other purpose authorised under the Act, the Regulations and the Legal Instrument.

7.2 The Data Recipient shall not process the transferred personal data for purposes that are incompatible with those for which the personal data was transferred unless otherwise authorised under the Act or with the prior written authorisation of the Transferring Entity.

7.3 Where the Data Recipient intends to process the transferred personal data for a new purpose, it shall notify the Transferring Entity in advance and ensure that such processing is lawful under the Act.

Clause 8. Data Minimisation

8.1 The Parties shall ensure that only personal data that is adequate, relevant and limited to what is necessary for the purposes specified in **Annex I** is transferred and processed.

8.2 The Parties shall implement appropriate measures to avoid the collection, transfer or retention of personal data that is excessive in relation to the purposes of processing.

Clause 9. Accuracy

9.1 Each Party shall take reasonable steps to ensure that personal data transferred under the Legal Instrument is accurate and, where necessary, kept up to date.

9.2 Where either Party becomes aware that transferred personal data is inaccurate or incomplete, it shall take appropriate measures to rectify, erase or restrict the processing of such personal data, as appropriate, and notify the other Party without undue delay where this may affect the rights or interests of the data subject.

Clause 10. Storage Limitation

10.1 The Data Recipient shall retain the transferred personal data only for as long as is necessary to fulfil the purposes specified in **Annex I** or as otherwise required or authorised by the Act or other applicable law.

10.2 Upon expiry of the applicable retention period, the Data Recipient shall securely return, delete or anonymise the transferred personal data in accordance with Clause 23.

Clause 11. Integrity and Confidentiality

11.1 Each Party shall implement appropriate technical and organisational measures to ensure the integrity, confidentiality and security of personal data transferred under the Legal Instrument, in accordance with the Act, the Regulations and these Standard Clauses.

11.2 The technical and organisational measures applicable to the transfer shall be described in **Annex II** and implemented and maintained in accordance with Clause 16.

11.3 Each Party shall ensure that persons authorised to process the transferred personal data are subject to appropriate confidentiality obligations.

Clause 12. Accountability

12.1 Each Party shall be responsible for, and able to demonstrate, compliance with these Standard Clauses, the Act and the Regulations.

12.2 Each Party shall establish and maintain appropriate governance measures, policies and records necessary to support compliance with these Standard Clauses.

12.3 Each Party shall cooperate with the other Party in demonstrating compliance with these Standard Clauses.

PART III – RIGHTS OF DATA SUBJECTS

Clause 13. Exercise and Protection of Data Subject Rights

13.1 The Parties shall ensure that the cross-border transfer and subsequent processing of personal data do not adversely affect the rights and freedoms of data subjects guaranteed under the Act.

13.2 Each Party shall implement appropriate measures to enable data subjects to effectively exercise their rights under the Act in relation to personal data transferred under these Standard Clauses.

13.3 A data subject may exercise their rights by submitting a request to either the Transferring Entity or the Data Recipient, unless otherwise specified in the Legal Instrument.

13.4 Where a Party receives a request or complaint relating to processing carried out by the other Party, it shall promptly notify that Party and cooperate in responding to the request or resolving the complaint within the timeframes prescribed under the Act.

13.5 Nothing in these Standard Clauses shall prejudice the right of a data subject to lodge a complaint with the Office of the Data Protection Commissioner or to seek any other remedy available under the Act or any other applicable law.

Clause 14. Enforcement of Data Subject Rights

14.1 Data subjects whose personal data is transferred under these Standard Clauses shall be entitled to invoke and enforce those provisions of these Standard Clauses that are intended to protect their rights and interests, in accordance with the Act and any other applicable law.

14.2 The Parties shall not amend or terminate these Standard Clauses in a manner that adversely affects the rights of data subjects in relation to personal data already transferred, unless the amendment provides an equivalent or higher level of protection.

14.3 Nothing in these Standard Clauses shall limit or prejudice any right or remedy available to a data subject under the Act, the Regulations or any other applicable law.

PART IV – IMPLEMENTATION AND ONGOING COMPLIANCE

Clause 15. Assessment and Demonstration of Appropriate Safeguards

15.1 Before relying on these Standard Clauses as the basis for a cross-border transfer of personal data, the Parties shall assess whether the transfer can be carried out in compliance with the Act, the Regulations and these Standard Clauses.

15.2 The assessment shall take into account, where appropriate:

a) the nature, scope, context and purposes of the transfer;
b) the categories of personal data and data subjects concerned;
c) the legal and regulatory framework applicable to the Data Recipient;
d) any laws or practices that may affect the Data Recipient's ability to comply with these Standard Clauses, including legally binding requests from public authorities for access to personal data;
e) any reliable and objectively verifiable information concerning the legal, regulatory and operational environment applicable to the transferred personal data; and
f) any supplementary technical, organisational or contractual measures necessary to ensure an appropriate level of protection.

15.3 The Parties confirm that, at the time of entering into these Standard Clauses, they have no reason to believe that the laws and practices applicable to the Data Recipient prevent compliance with these Standard Clauses.

15.4 Where a Data Protection Impact Assessment is required under the Act or the Regulations in relation to the transfer or subsequent processing of personal data, the Parties shall ensure that it is completed before the transfer takes place and reviewed where there is a material change affecting the risks associated with the transfer.

15.5 The Parties shall document the assessment and maintain records necessary to demonstrate compliance with these Standard Clauses, including, where applicable, Data Protection Impact Assessments, records of personal data breaches, onward transfers, audits and any supplementary safeguards implemented.

15.6 The Parties shall be able to demonstrate that appropriate safeguards are maintained before, during and after the cross-border transfer of personal data.

15.7 Where the Parties become aware of any material change affecting the transfer or the assessment, they shall review the assessment without undue delay and implement any additional safeguards necessary to ensure continued compliance.

Clause 16. Security Measures

16.1 The Parties shall implement and maintain appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data transferred under these Standard Clauses, taking into account the nature, scope, context and purposes of the processing, the risks to the rights and freedoms of data subjects and the state of available technology.

16.2 The technical and organisational measures implemented by the Parties shall be described in **Annex II** and shall be reviewed periodically to ensure their continued effectiveness.

16.3 Each Party shall ensure that access to the transferred personal data is restricted to authorised persons who require such access for the performance of their duties and who are subject to appropriate confidentiality obligations.

16.4 Each Party shall maintain appropriate procedures for detecting, investigating, managing and responding to personal data breaches affecting the transferred personal data.

16.5 Where either Party becomes aware of a personal data breach affecting the transferred personal data, it shall notify the other Party without undue delay and cooperate in investigating the breach, assessing its impact, implementing mitigation measures and complying with any notification obligations under the Act and the Regulations.

Clause 17. Transfers of Sensitive Personal Data

17.1 Where the cross-border transfer involves Sensitive Personal Data, the Parties shall ensure compliance with the additional requirements applicable under the Act and the Regulations.

17.2 The Parties shall implement enhanced technical and organisational measures proportionate to the nature of the data, the risks associated with the transfer and the potential impact on the rights and freedoms of data subjects.

17.3 Access to Sensitive Personal Data shall be limited to authorised persons who require such access for the purposes specified in **Annex I** and who are subject to appropriate confidentiality obligations.

17.4 Sensitive Personal Data shall not be processed or disclosed except for the purposes specified in **Annex I** or as otherwise permitted under the Act and the Regulations.

17.5 Where required under the Act or the Regulations, the Parties shall implement any additional safeguards applicable to the processing of Sensitive Personal Data, taking into account the nature of the data and the risks associated with the transfer.

Clause 18. Onward Transfers

18.1 The Data Recipient shall not make an onward transfer of personal data received under these Standard Clauses unless:

a) the onward transfer is permitted under the Act and the Regulations;

b) the onward transfer is necessary for the purposes specified in **Annex I** or is otherwise authorised under the Act;

c) the onward recipient is bound by legally enforceable obligations that provide a level of protection that is not lower than that afforded by these Standard Clauses; and

d) the Transferring Entity has provided its prior written authorisation following assessment of the proposed onward transfer, unless the Legal Instrument expressly permits such onward transfers under specified conditions.

18.2 Before making an onward transfer, the Data Recipient shall assess whether the onward recipient is able to comply with the obligations referred to in paragraph 18.1(c), taking into account the legal and regulatory framework applicable to the onward recipient, the nature of the personal data, the risks associated with the onward transfer and any supplementary safeguards that may be required. The Data Recipient shall provide the Transferring Entity with sufficient information to enable it to assess the proposed onward transfer before granting authorisation under paragraph 18.1(d).

18.3 The Data Recipient shall remain fully responsible for ensuring that any onward transfer complies with these Standard Clauses and shall remain liable for any breach by the onward

recipient that results in a failure to provide the level of protection required under these Standard Clauses, without prejudice to any rights available to data subjects under the Act.

18.4 The Data Recipient shall maintain a record of all onward transfers, including the identity of the onward recipient, the purpose of the transfer, the categories of personal data transferred, the legal basis relied upon and the safeguards implemented.

18.5 Where the Data Recipient becomes aware that an onward recipient is unable or unwilling to comply with the applicable safeguards, it shall immediately suspend any further onward transfers to that recipient and take appropriate measures to protect the transferred personal data, including, requiring the onward recipient to return or securely delete the personal data.

18.6 An onward recipient shall not make a further cross-border transfer of the personal data unless such transfer complies with the requirements of this Clause and provides a level of protection that is not lower than that afforded by these Standard Clauses.

Clause 19. Cooperation, Audit and Oversight

19.1 The Parties shall cooperate with one another and with the Office of the Data Protection Commissioner in matters relating to the implementation of these Standard Clauses.

19.2 Upon reasonable request, each Party shall provide the other Party with information necessary to demonstrate compliance with these Standard Clauses, subject to legal professional privilege, commercial confidentiality and information security considerations.

19.3 Where reasonably necessary to verify compliance with these Standard Clauses, the Parties shall facilitate audits or other appropriate verification measures.

19.4 The Parties shall provide information requested by the Office of the Data Protection Commissioner and comply with any lawful direction, order or determination relating to the transferred personal data.

Clause 20. Changes Affecting Compliance

20.1 Where either Party becomes aware of any circumstance that is likely to affect its ability to comply with these Standard Clauses, including changes in applicable law or legally binding requests from public authorities for access to transferred personal data, it shall promptly notify the other Party.

20.2 The Parties shall assess the impact of such circumstances on the protection afforded to the transferred personal data and determine whether additional safeguards are required to maintain compliance with these Standard Clauses.

20.3 Where legally permissible, the Data Recipient shall notify the Transferring Entity of any legally binding request from a public authority for access to transferred personal data and shall:

a) review the legality of the request under the applicable law;
b) disclose only the minimum amount of personal data legally required;
c) where reasonable grounds exist, take reasonable steps to challenge or seek clarification of any request that appears unlawful or disproportionate; and
d) document the request and any disclosure made.

20.4 Where the Data Recipient determines that it is no longer able to comply with these Standard Clauses, it shall promptly notify the Transferring Entity, providing all relevant information necessary to assess the impact on the transferred personal data and, where appropriate, identify measures to restore compliance.

20.5 Following a notification under paragraph 20.4, the Parties shall promptly assess whether appropriate safeguards can be restored. Where compliance cannot be restored within a reasonable period, they shall suspend the transfer or terminate the Legal Instrument in accordance with Part V.

20.6 Where the transfer is suspended or the Legal Instrument is terminated pursuant to this Clause, the Data Recipient shall, at the choice of the Transferring Entity and unless otherwise required by law, return or securely delete all personal data transferred under these Standard Clauses and certify that it has done so.

20.7 The Data Recipient shall inform the Transferring Entity without undue delay of any change in the laws or practices applicable to it, or of any other circumstance, that is likely to adversely affect its ability to comply with these Standard Clauses.

PART V – FINAL PROVISIONS

Clause 21. Liability

21.1 Each Party shall be responsible for complying with its obligations under these Standard Clauses and shall remain accountable for any processing of personal data carried out under the Legal Instrument.

21.2 Where both Parties are responsible for the same damage suffered by a data subject as a result of a breach of these Standard Clauses, each Party shall be liable in accordance with the applicable law.

21.3 Nothing in these Standard Clauses shall exclude or limit any rights or remedies available to data subjects under the Act or any other applicable law.

Clause 22. Suspension and Termination

22.1 Either Party may suspend the cross-border transfer of personal data where it reasonably believes that the other Party is no longer able to comply with these Standard Clauses.

22.2 Where the circumstances giving rise to the suspension are not remedied within a reasonable period, either Party may terminate the Legal Instrument, in whole or in part, to the extent necessary to protect the transferred personal data.

22.3 Suspension or termination under this Clause shall be without prejudice to any obligations accrued before the date of suspension or termination.

Clause 23. Return, Deletion and Continuing Obligations

23.1 Upon termination of the Legal Instrument or cessation of the processing activities giving rise to the transfer, the Data Recipient shall, at the choice of the Transferring Entity and unless otherwise required by law:

a) return all transferred personal data and any copies thereof to the Transferring Entity; or

b) securely delete or destroy the transferred personal data and certify that it has done so.

23.2 Where the Data Recipient is required by law to retain the transferred personal data, it shall continue to protect the personal data in accordance with these Standard Clauses for as long as the personal data is retained.

23.3 Any obligations under these Standard Clauses which, by their nature, are intended to continue after suspension or termination of the Legal Instrument, including obligations relating to confidentiality, security, cooperation with the Office of the Data Protection Commissioner, liability and the protection of retained personal data, shall remain in effect until they have been fully discharged.

Clause 24. Amendments

24.1 These Standard Clauses shall not be modified in a manner that reduces the level of protection afforded to data subjects under the Act, the Regulations or these Standard Clauses.

24.2 The Parties may incorporate additional contractual safeguards into the Legal Instrument, provided that such safeguards are not inconsistent with these Standard Clauses and do not directly or indirectly reduce the level of protection afforded to data subjects.

24.3 Any amendment to the Legal Instrument affecting the cross-border transfer of personal data shall be documented in writing.

Clause 25. Governing Law and Jurisdiction

25.1 These Standard Clauses shall be governed by the laws of Kenya.

25.2 Any dispute arising from or relating to these Standard Clauses shall be resolved in accordance with the dispute resolution mechanism contained in the Legal Instrument, provided that such mechanism does not prejudice the powers of the Office of the Data Protection Commissioner or the rights of data subjects under the Act.

25.3 Nothing in these Standard Clauses shall prevent the Office of the Data Protection Commissioner from exercising its statutory powers under the Act or affect the right of a data subject to lodge a complaint with the Office or seek any remedy available under the Act or any other applicable law.

ANNEXES

General Provisions

A.1 These Annexes form an integral part of the Standard Clauses and shall be completed by the Parties before the commencement of the cross-border transfer of personal data.

A.2 The information contained in the Annexes shall be accurate, complete and kept up to date throughout the duration of the Legal Instrument.

A.3 Where a material change affects the cross-border transfer, the processing activities or the safeguards relied upon, the relevant Annex shall be updated without undue delay.

A.4 The Parties acknowledge that these Annexes constitute the primary record of the cross-border transfer governed by these Standard Clauses. Failure to complete or maintain the Annexes shall affect the Parties' ability to demonstrate compliance with Part VI of the Data Protection Act, 2019, Regulation 40(a) of the Data Protection (General) Regulations, 2021, and these Standard Clauses.

ANNEX I - Description of the Cross-Border Transfer

CROSS-BORDER DATA TRANSFER INFORMATION

(Controller to Controller)

A1. REFERENCE INFORMATION

Item	Details / Response
Transfer Reference Number	
Legal Instrument	
Effective Date	

A2. PARTIES

A2.1 Transferring Entity

Item	Details / Response
Name	
Address	
Contact Person	
Position	
Email	
Telephone	

A2.2 Data Recipient

Item	Details / Response
Name	
Address	
Contact Person	
Position	
Email	
Telephone	

A3. DESCRIPTION OF THE TRANSFER

Item	Details / Response
Purpose(s) of the Transfer	
Description of the Processing Activities	
Categories of Personal Data	
Categories of Data Subjects	
Does the Transfer Involve Sensitive Personal Data?	☐ Yes ☐ No
If Yes, Describe	

A4. DESTINATION AND TRANSFER DETAILS

Item	Details / Response
Destination Country(ies)	

Frequency of Transfer	☐ One-off ☐ Occasional ☐ Continuous
Method of Transfer	☐ Electronic ☐ Physical Media ☐ Remote Access ☐ Other
If Other, Specify	
A5. LEGAL BASIS AND RETENTION	

Item	**Details / Response**
Legal Basis for Processing under the Act	
Retention Period	
Was a Data Protection Impact Assessment Conducted?	☐ Yes ☐ No
If Yes – Date Completed	
A6. APPROPRIATE SAFEGUARDS	

Safeguard Category	**Details**
Technical Safeguards	
Organisational Safeguards	
Contractual Safeguards	
Transfer Assessment Completed	☐ Yes ☐ No
Date	
Supplementary Safeguards	
A7. ONWARD TRANSFERS	

Item	**Details / Response**
Will Onward Transfers Occur?	☐ Yes ☐ No
If Yes – Countries of Destination	
Categories of Recipients	
Purpose(s)	
Applicable Safeguards	
A8. DECLARATION	

The Parties confirm that the information contained in this Annex is accurate and complete to the best of their knowledge and undertake to update this Annex without undue delay where any material change affects the cross-border transfer described herein.

SIGNATURES

TRANSFERRING ENTITY	**DATA RECIPIENT**
Name:	Name:
Position:	Position:
Signature / Date:	Signature / Date:

ANNEX II

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Parties shall describe the technical and organisational security measures implemented to protect the transferred personal data, taking into account the nature of the processing, the risks involved and the state of available technology.

A1. GOVERNANCE

Security Measure	**Description**
Information security policies	
Staff confidentiality obligations	
Staff training and awareness	
Other	
A2. ACCESS CONTROL	

Security Measure	**Description**
Authentication	
Authorisation	
Privileged access management	
Other	
A3. DATA SECURITY	

Security Measure	**Description**
Encryption	
Pseudonymisation (where applicable)	
Secure transmission	
Secure storage	
Backup and recovery	
Secure disposal	
A4. SYSTEM SECURITY	

Security Measure	**Description**
Logging and monitoring	
Network security	
Malware protection	
Vulnerability and patch management	
A5. PHYSICAL SECURITY	

Security Measure	**Description**
Physical access controls	
Environmental and infrastructure protection	
A6. INCIDENT MANAGEMENT	

Security Measure	**Description**

Incident response procedures	
Business continuity	
Disaster recovery	
A7. ADDITIONAL INFORMATION OR ANY OTHER SECURITY MEASURES	

DECLARATION

The Parties confirm that the technical and organisational security measures described in this Annex are appropriate to the risks presented by the transfer and shall be reviewed and updated where necessary to ensure continued protection of the transferred personal data.

SIGNATURES

TRANSFERRING ENTITY	**DATA RECIPIENT**
Name:	Name:
Position:	Position:
Signature / Date:	Signature / Date:

ANNEX III

RECORD OF ONWARD TRANSFERS

This Annex shall be completed where onward transfers are undertaken pursuant to Clause 18 of these Standard Clauses.

Date	Onward Recipient	Country	Purpose	Categories of Personal Data	Legal Basis	Authorisation Date	Authorised By	Safeguards Applied	Status

ADDITIONAL NOTES

DECLARATION

The Data Recipient confirms that each onward transfer recorded in this Annex has been carried out in accordance with Clause 18 of these Standard Clauses and that the applicable safeguards remain in place.

SIGNATURE

DATA RECIPIENT	DATE
Name:	
Position:	
Signature:	

Standard Clauses for Legal Instruments Containing Appropriate Safeguards for Data Controller to Data Processor Cross-Border Transfers of Personal Data

PART I – GENERAL PROVISIONS

Clause 1. Purpose and Scope

1.1 These Standard Clauses establish appropriate safeguards for the cross-border transfer of personal data from a Data Controller to a Data Processor in accordance with Part VI of the Data Protection Act, 2019 (the Act) and the Data Protection (General) Regulations, 2021 (the Regulations).

1.2 These Standard Clauses are intended to be incorporated into a legally binding instrument between a Data Controller and a Data Processor where appropriate safeguards are relied upon as the legal basis for a cross-border transfer of personal data under Regulation 40(a).

1.3 These Standard Clauses apply solely to the cross-border transfer of personal data described in **Annex I** and form an integral part of the legal instrument between the Parties.

1.4 These Standard Clauses shall not be interpreted as limiting or excluding any obligation imposed on either Party under the Act, the Regulations, or any other applicable law providing a higher level of protection for personal data.

Clause 2. Definitions and Interpretation

2.1 Unless otherwise defined in these Standard Clauses, the terms used herein shall have the meanings assigned to them in the Act, the Regulations and the Guidance on Cross-Border Transfers of Personal Data issued by the Office of the Data Protection Commissioner.

2.2 For the purposes of these Standard Clauses:

a) **"Data Controller"** means the controller transferring personal data under the Legal Instrument.
b) **"Data Processor"** means the processor receiving and processing personal data on behalf of the Data Controller under the Legal Instrument.
c) **"Legal Instrument"** means the legally binding agreement between the Data Controller and the Data Processor into which these Standard Clauses are incorporated.
d) **"Party"** means either the Data Controller or the Data Processor, and **"Parties"** means both collectively.
e) **"Standard Clauses"** means these Standard Clauses for Legal Instruments Containing Appropriate Safeguards for Controller-to-Processor Cross-Border Transfers of Personal Data.

2.3 These Standard Clauses shall be interpreted in a manner that gives effect to the objectives and principles of the Act and the Regulations. In the event of any inconsistency between these Standard Clauses and the Act or the Regulations, the provisions of the Act and the Regulations shall prevail.

Clause 3. Hierarchy

3.1 These Standard Clauses form part of the Legal Instrument between the Parties and shall prevail over any contractual provision that is inconsistent with them, unless such provision affords a higher level of protection for personal data.

3.2 Nothing in the Legal Instrument shall reduce or limit the level of protection afforded to personal data under these Standard Clauses, the Act or the Regulations.

Clause 4. Description of the Transfer

4.1 The Parties shall complete **Annex I** with accurate and up-to-date information describing the cross-border transfer of personal data and the safeguards applicable to the transfer.

4.2 **Annex I** shall form an integral part of these Standard Clauses.

Clause 5. Duration

5.1 These Standard Clauses shall remain in force for as long as the Data processor processes personal data transferred under the Legal Instrument, unless terminated in accordance with its terms.

5.2 The termination of the Legal Instrument shall not relieve either Party of any obligation under these Standard Clauses that is intended to survive termination, including obligations relating to confidentiality, security, liability, data subject rights, the return or deletion of personal data, and cooperation with the Office of the Data Protection Commissioner.

PART II – APPROPRIATE SAFEGUARDS

Clause 6. Lawfulness, Fairness and Transparency

6.1 The Data Controller shall ensure that personal data transferred under the Legal Instrument is processed lawfully, fairly and in a transparent manner, in accordance with the Act, the Regulations and these Standard Clauses.

6.2 The Data Processor shall process the transferred personal data only on the documented instructions of the Data Controller, unless otherwise required by the Act or any other applicable law. Where the Data Processor is required by law to process the personal data otherwise than on the documented instructions of the Data Controller, the Data Processor shall inform the Data Controller of that legal requirement before the processing, unless prohibited by law.

6.3 The Data Controller shall ensure that data subjects are provided with the information required under the Act concerning the cross-border transfer and subsequent processing of their personal data, unless an exemption under the Act applies.

6.4 The Data Processor shall promptly inform the Data Controller if, in its opinion, any documented instruction infringes the Act, the Regulations or these Standard Clauses.

Clause 7. Purpose Limitation

7.1 The Data Processor shall process the transferred personal data solely for the purposes specified in **Annex I** and only on the documented instructions of the Data Controller.

7.2 The Data Processor shall not process the transferred personal data for its own purposes or for any purpose that is incompatible with those specified in **Annex I**, unless otherwise authorised by the Act or required by applicable law.

7.3 Where the Data Processor considers that a documented instruction would require processing for a purpose not specified in **Annex I**, it shall notify and obtain authorisation from the Data Controller before carrying out such processing.

Clause 8. Data Minimisation

8.1 The Data Controller shall ensure that only personal data that is adequate, relevant and limited to what is necessary for the purposes specified in **Annex I** is transferred to the Data Processor.

8.2 The Data Processor shall process only the personal data necessary to perform the processing activities specified in Annex I and shall not collect, use or retain personal data beyond what is required to perform those activities.

Clause 9. Accuracy

9.1 The Data Controller shall take reasonable steps to ensure that personal data transferred under the Legal Instrument is accurate and, where necessary, kept up to date.

9.2 Where the Data Processor becomes aware that transferred personal data is inaccurate or incomplete, it shall promptly notify the Data Controller and, where instructed, assist the Data Controller in rectifying, erasing or restricting the processing of the personal data, as appropriate.

Clause 10. Storage Limitation

10.1 The Data Processor shall retain the transferred personal data only for as long as necessary to perform the processing activities specified in **Annex I** or as instructed by the Data Controller, unless retention is required by the Act or any other applicable law.

10.2 Upon expiry of the applicable retention period or upon the instructions of the Data Controller, the Data Processor shall securely return, delete or anonymise the transferred personal data in accordance with Clause 23.

Clause 11. Integrity and Confidentiality

11.1 The Parties shall ensure the integrity, confidentiality and security of personal data transferred under the Legal Instrument in accordance with the Act, the Regulations and these Standard Clauses.

11.2 The technical and organisational measures applicable to the transfer shall be described in **Annex II** and implemented and maintained in accordance with Clause 16.

11.3 The Data Processor shall ensure that persons authorised to process the transferred personal data are subject to appropriate confidentiality obligations.

Clause 12. Accountability

12.1 The Data Controller shall remain responsible for ensuring that the cross-border transfer and the processing carried out on its behalf comply with the Act, the Regulations and these Standard Clauses.

12.2 The Data Processor shall be responsible for complying with the obligations specifically applicable to it under these Standard Clauses, the Act and the Regulations, and shall be able to demonstrate such compliance.

12.3 The Parties shall establish and maintain appropriate governance measures, policies and records necessary to support compliance with these Standard Clauses.

PART III – RIGHTS OF DATA SUBJECTS

Clause 13. Exercise and Protection of Data Subject Rights

13.1 The Data Controller shall ensure that the cross-border transfer and subsequent processing of personal data do not adversely affect the rights and freedoms of data subjects guaranteed under the Act.

13.2 The Data Controller and Data Processor shall implement appropriate measures to enable data subjects to effectively exercise their rights under the Act in relation to personal data transferred under these Standard Clauses.

13.3 Where either Party receives a request, complaint or other communication from a data subject relating to the transferred personal data, it shall comply with its obligations under the Act and the Regulations and, where necessary, promptly inform and cooperate with the other Party to facilitate the effective exercise of the data subject's rights.

13.4 The Data Processor shall provide the Data Controller with appropriate and timely assistance, taking into account the nature of the processing and the information available to it, to enable the Data Controller to comply with its obligations under the Act, including in relation to the exercise of data subject rights, personal data breaches, Data Protection Impact Assessments, consultations with the Office of the Data Protection Commissioner and demonstrating compliance with these Standard Clauses.

13.5 Nothing in these Standard Clauses shall prejudice the right of a data subject to lodge a complaint with the Office of the Data Protection Commissioner or to seek any other remedy available under the Act or any other applicable law.

Clause 14. Enforcement of Data Subject Rights

14.1 Data subjects whose personal data is transferred under these Standard Clauses shall be entitled to invoke and enforce those provisions of these Standard Clauses that are intended to protect their rights and interests, in accordance with the Act and any other applicable law.

14.2 The Parties shall not amend or terminate these Standard Clauses in a manner that adversely affects the rights of data subjects in relation to personal data already transferred, unless the amendment provides an equivalent or higher level of protection.

14.3 Nothing in these Standard Clauses shall limit or prejudice any right or remedy available to a data subject under the Act, the Regulations or any other applicable law.

PART IV – IMPLEMENTATION AND ONGOING COMPLIANCE

Clause 15. Assessment and Demonstration of Appropriate Safeguards

15.1 Before relying on these Standard Clauses as the basis for a cross-border transfer of personal data, the Data Controller and the Data Processor shall assess whether the transfer can be carried out in compliance with the Act, the Regulations and these Standard Clauses.

15.2 The assessment shall take into account, where appropriate:

a) the nature, scope, context and purposes of the transfer;
b) the categories of personal data and data subjects concerned;
c) the legal and regulatory framework applicable to the Data Processor;
d) any laws or practices that may affect the Data Processor's ability to comply with these Standard Clauses, including legally binding requests from public authorities for access to personal data;
e) any reliable and objectively verifiable information concerning the legal, regulatory and operational environment applicable to the transferred personal data; and
f) any supplementary technical, organisational or contractual measures necessary to ensure an appropriate level of protection.

15.3 The Parties confirm that, at the time of entering into these Standard Clauses, they have no reason to believe that the laws and practices applicable to the Data Processor prevent compliance with these Standard Clauses.

15.4 Where a Data Protection Impact Assessment is required under the Act or the Regulations in relation to the transfer or subsequent processing of personal data, the Parties shall ensure that it is completed before the transfer takes place and reviewed where there is a material change affecting the risks associated with the transfer.

15.5 The Parties shall document the assessment and maintain records necessary to demonstrate compliance with these Standard Clauses, including, Data Protection Impact Assessments, records of personal data breaches, sub-processing arrangements, audits and any supplementary safeguards implemented.

15.6 The Parties shall be able to demonstrate that appropriate safeguards are maintained before, during and after the cross-border transfer of personal data.

15.7 Where the Parties become aware of any material change affecting the transfer or the assessment, they shall review the assessment without undue delay and implement any additional safeguards necessary to ensure continued compliance.

Clause 16. Security Measures

16.1 The Data Controller and the Data Processor shall implement and maintain appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data transferred under these Standard Clauses, taking into account the nature, scope, context and purposes of the processing, the risks to the rights and freedoms of data subjects and the state of available technology.

16.2 The technical and organisational measures implemented by the Parties shall be described in **Annex II** and shall be reviewed periodically to ensure their continued effectiveness.

16.3 The Data Processor shall ensure that access to the transferred personal data is restricted to authorised persons who require such access for the performance of their duties and who are subject to appropriate confidentiality obligations.

16.4 The Data Controller and the Data Processor shall maintain appropriate procedures for detecting, investigating, managing and responding to personal data breaches affecting the transferred personal data.

16.5 Where either Party becomes aware of a personal data breach affecting the transferred personal data, it shall notify the other Party without undue delay and cooperate in investigating the breach, assessing its impact, implementing mitigation measures and complying with any notification obligations under the Act and the Regulations.

16.6 The Data Processor shall implement and maintain the technical and organisational security measures described in **Annex II** and shall not materially reduce the level of protection afforded to the transferred personal data without the prior written agreement of the Data Controller.

Clause 17. Transfers of Sensitive Personal Data

17.1 Where the cross-border transfer involves Sensitive Personal Data, the Parties shall ensure compliance with the additional requirements applicable under the Act and the Regulations.

17.2 The Parties shall implement enhanced technical and organisational measures proportionate to the nature of the data, the risks associated with the transfer and the potential impact on the rights and freedoms of data subjects.

17.3 Access to Sensitive Personal Data shall be limited to authorised persons who require such access for the processing activities specified in **Annex I** and who are subject to appropriate confidentiality obligations.

17.4 Sensitive Personal Data shall not be processed except in accordance with the documented instructions of the Data Controller or as otherwise permitted or required under the Act or any other applicable law.

17.5 Where required under the Act or the Regulations, the Parties shall implement any additional safeguards applicable to the processing of Sensitive Personal Data, taking into account the nature of the data and the risks associated with the transfer.

Clause 18. Sub-processing

18.1 The Data Processor shall not engage another processor to carry out processing activities involving the transferred personal data without the prior written authorisation of the Data Controller.

18.2 The authorisation referred to in paragraph 18.1 may relate to:

a) a specific sub-processor; or
b) a category of sub-processors identified in the Legal Instrument,

provided that the Data Controller is informed of any intended addition or replacement of sub-processors and is given a reasonable opportunity to object before the change takes effect.

18.3 Where the Data Processor engages a sub-processor, it shall ensure that the sub-processor is bound by a legally enforceable agreement imposing obligations that provide a level of protection that is not lower than that required under these Standard Clauses, including obligations relating to:

a) processing personal data only on the documented instructions of the Data Controller;
b) confidentiality;

c) technical and organisational security measures;
d) assistance in complying with data subject rights;
e) personal data breach management and notification;
f) audits and inspections; and
g) the return or deletion of personal data upon termination of the processing.

18.4 The Data Processor shall remain fully liable for the performance of the sub-processor's obligations and shall remain liable to the Data Controller for any act or omission of the sub-processor that results in a breach of these Standard Clauses.

18.5 The Data Processor shall maintain an up-to-date record of authorised sub-processors, including their identity, country of establishment, processing activities, date of authorisation and the safeguards implemented.

18.6 Where the Data Processor becomes aware that a sub-processor is unable or unwilling to comply with the applicable safeguards, it shall immediately suspend the processing carried out by that sub-processor, promptly inform the Data Controller and take appropriate measures to protect the transferred personal data, including, requiring the return or secure deletion of the personal data.

Clause 19. Cooperation, Audit and Oversight

19.1 The Parties shall cooperate with one another and with the Office of the Data Protection Commissioner in matters relating to the implementation of these Standard Clauses.

19.2 The Data Processor shall make available to the Data Controller all information reasonably necessary to demonstrate compliance with these Standard Clauses and shall cooperate with any lawful request from the Office of the Data Protection Commissioner relating to the transferred personal data.

19.3 Where reasonably necessary to verify compliance with these Standard Clauses, the Data Controller shall be entitled to conduct, or have conducted on its behalf, reasonable audits or other appropriate verification measures of the Data Processor, subject to reasonable notice and appropriate confidentiality and information security safeguards.

19.4 The Parties shall provide information lawfully requested by the Office of the Data Protection Commissioner and comply with any lawful direction, order or determination relating to the transferred personal data.

Clause 20. Changes Affecting Compliance

20.1 Where either Party becomes aware of any circumstance that is likely to affect its ability to comply with these Standard Clauses, including changes in applicable law or legally binding requests from public authorities for access to transferred personal data, it shall promptly notify the other Party.

20.2 The Parties shall assess the impact of such circumstances on the protection afforded to the transferred personal data and determine whether additional safeguards are required to maintain compliance with these Standard Clauses.

20.3 Where legally permissible, the Data Processor shall notify the Data Controller of any legally binding request from a public authority for access to transferred personal data and shall:

a) review the legality of the request under the applicable law;
b) disclose only the minimum amount of personal data legally required;

c) where reasonable grounds exist, take reasonable steps to challenge or seek clarification of any request that appears unlawful or disproportionate; and
d) document the request and any disclosure made.

20.4 Where the Data Processor determines that it is no longer able to comply with these Standard Clauses, it shall promptly notify the Data Controller, providing all relevant information necessary to assess the impact on the transferred personal data and, where appropriate, identify measures to restore compliance.

20.5 Following a notification under paragraph 20.4, the Parties shall promptly assess whether appropriate safeguards can be restored. Where compliance cannot be restored within a reasonable period, they shall suspend the transfer or terminate the Legal Instrument in accordance with Part V.

20.6 Where the transfer is suspended or the Legal Instrument is terminated pursuant to this Clause, the Data Processor shall, at the choice of the Data Controller and unless otherwise required by law, return or securely delete all personal data transferred under these Standard Clauses and certify that it has done so.

PART V – FINAL PROVISIONS

Clause 21. Liability

21.1 Each Party shall be responsible for complying with its obligations under these Standard Clauses and shall remain accountable for the processing activities for which it is responsible under the Act, the Regulations and the Legal Instrument.

21.2 Nothing in these Standard Clauses shall relieve the Data Controller of its obligations under the Act, nor the Data Processor of the obligations specifically applicable to it under the Act, the Regulations and these Standard Clauses.

21.3 Where both Parties are responsible for the same damage suffered by a data subject as a result of a breach of these Standard Clauses, each Party shall be liable in accordance with the applicable law.

21.4 Nothing in these Standard Clauses shall exclude or limit any rights or remedies available to data subjects under the Act or any other applicable law.

Clause 22. Suspension and Termination

22.1 Either Party may suspend the cross-border transfer of personal data where it reasonably believes that the other Party is no longer able to comply with these Standard Clauses.

22.2 Where the circumstances giving rise to the suspension are not remedied within a reasonable period, either Party may terminate the Legal Instrument, in whole or in part, to the extent necessary to protect the transferred personal data.

22.3 Suspension or termination under this Clause shall be without prejudice to any obligations accrued before the date of suspension or termination.

Clause 23. Return, Deletion and Continuing Obligations

23.1 Upon termination of the Legal Instrument or cessation of the processing activities giving rise to the transfer, the Data Processor shall, at the choice of the Data Controller and unless otherwise required by law:

a) return all transferred personal data and any copies thereof to the Data Controller; or
b) securely delete or destroy the transferred personal data and certify that it has done so.

23.2 Where the Data Processor is required by law to retain the transferred personal data, it shall continue to protect the personal data in accordance with these Standard Clauses for as long as the personal data is retained.

23.3 Any obligations under these Standard Clauses which, by their nature, are intended to continue after suspension or termination of the Legal Instrument, including obligations relating to confidentiality, security, cooperation with the Office of the Data Protection Commissioner, liability and the protection of retained personal data, shall remain in effect until they have been fully discharged.

Clause 24. Amendments

24.1 These Standard Clauses shall not be modified in a manner that reduces the level of protection afforded to data subjects under the Act, the Regulations or these Standard Clauses.

24.2 The Parties may incorporate additional contractual safeguards into the Legal Instrument, provided that such safeguards are not inconsistent with these Standard Clauses and do not directly or indirectly reduce the level of protection afforded to data subjects.

24.3 Any amendment to the Legal Instrument affecting the cross-border transfer of personal data or the processing activities carried out by the Data Processor shall be documented in writing.

Clause 25. Governing Law and Jurisdiction

25.1 These Standard Clauses shall be governed by the laws of Kenya.

25.2 Any dispute arising from or relating to these Standard Clauses shall be resolved in accordance with the dispute resolution mechanism contained in the Legal Instrument, provided that such mechanism does not prejudice the powers of the Office of the Data Protection Commissioner or the rights of data subjects under the Act.

25.3 Nothing in these Standard Clauses shall prevent the Office of the Data Protection Commissioner from exercising its statutory powers under the Act or affect the right of a data subject to lodge a complaint with the Office or seek any remedy available under the Act or any other applicable law.

ANNEXES

The Annexes form an integral part of these Standard Clauses and shall be completed by the Parties before the cross-border transfer of personal data takes place.

The Parties shall ensure that the information contained in the Annexes remains accurate, complete and up to date throughout the duration of the Legal Instrument and shall update the

Annexes where necessary to reflect any material changes affecting the transfer or the processing of personal data.

The Annexes shall be made available to the Office of the Data Protection Commissioner upon lawful request.

ANNEX I – DESCRIPTION OF THE CROSS-BORDER TRANSFER

(Controller to Processor)

This Annex shall contain the information necessary to describe the cross-border transfer of personal data, the Parties, the processing activities carried out by the Data Processor, and the safeguards applicable to the transfer.

A1. REFERENCE INFORMATION

Item	Description
Transfer Reference Number	
Legal Instrument	
Effective Date	
A2. PARTIES	

Data Controller

Item	Description
Name	
Address	
Contact Person	
Position	
Email	
Telephone	

Data Processor

Item	Description
Name	
Address	
Contact Person	
Position	
Email	
Telephone	
A3. DESCRIPTION OF THE TRANSFER	

Item	Description
Purpose(s) of the Transfer	
Processing Activities Performed by the Data Processor	
Categories of Personal Data	
Categories of Data Subjects	
Sensitive Personal Data (if applicable)	
A4. DESTINATION OF THE TRANSFER	

Item	Description
Destination Country(ies)	
Frequency of the Transfer	
Method of Transfer	
A5. LEGAL BASIS, PROCESSING INSTRUCTIONS AND RETENTION	

Item	Description
Legal Basis for the Transfer	
Documented Processing Instructions (reference or description)	
Retention Period	
Was a Data Protection Impact Assessment Conducted?	☐ Yes ☐ No
Date Completed	
A6. APPROPRIATE SAFEGUARDS	

Item	Description
Technical Safeguards	
Organisational Safeguards	
Contractual Safeguards	
Transfer Assessment Completed	☐ Yes ☐ No
Date Completed	
Supplementary Safeguards (if applicable)	
A7. SUB-PROCESSING	

Item	Description
Authorised Sub-processors (if applicable)	
Type of Authorisation (Specific / General)	
Countries of Sub-processors	
A8. DECLARATION	

The Parties confirm that the information contained in this Annex is complete and accurate and undertake to keep it up to date throughout the duration of the transfer.

SIGNATURES

DATA CONTROLLER	DATA PROCESSOR
Name:	Name:
Position:	Position:
Signature / Date:	Signature / Date:

ANNEX II – TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Parties shall describe the technical and organisational security measures implemented to protect the transferred personal data, taking into account the nature of the processing, the risks involved and the state of available technology.

A1. GOVERNANCE

Security Measure	**Description**
Information security policies	
Staff confidentiality obligations	
Staff training and awareness	
Other	
A2. ACCESS CONTROL	

Security Measure	**Description**
Authentication	
Authorisation	
Privileged access management	
Other	
A3. DATA SECURITY	

Security Measure	**Description**
Encryption	
Pseudonymisation (where applicable)	
Secure transmission	
Secure storage	
Backup and recovery	
Secure disposal	
A4. SYSTEM SECURITY	

Security Measure	**Description**
Logging and monitoring	
Network security	
Malware protection	
Vulnerability and patch management	
A5. PHYSICAL SECURITY	

Security Measure	**Description**
Physical access controls	
Environmental and infrastructure protection	
A6. INCIDENT MANAGEMENT	

Security Measure	Description
Incident response procedures	
Business continuity	
Disaster recovery	
A7. ADDITIONAL INFORMATION OR ANY OTHER SECURITY MEASURES	

DECLARATION

The Parties confirm that the technical and organisational security measures described in this Annex are appropriate to the risks presented by the transfer and shall be reviewed and updated where necessary to ensure continued protection of the transferred personal data.

SIGNATURES

TRANSFERRING ENTITY	DATA RECIPIENT
Name:	Name:
Position:	Position:
Signature / Date:	Signature / Date:

ANNEX III – REGISTER OF APPROVED SUB-PROCESSORS

Approved Sub-processors

Name of Sub-processor	Country	Processing Activities	Type of Authorisation (Specific / General)	Date of Authorisation	Safeguards Implemented	Status

ADDITIONAL INFORMATION

DECLARATION

The Data Processor confirms that all sub-processors identified in this Annex have been authorised in accordance with Clause 18 and are bound by contractual obligations providing a level of protection that is not lower than that required under these Standard Clauses. The Data Processor undertakes to maintain this Annex accurately and keep it up to date throughout the duration of the Legal Instrument.

SIGNATURE

DATA PROCESSOR	DATE
Name:	
Position:	
Signature:	