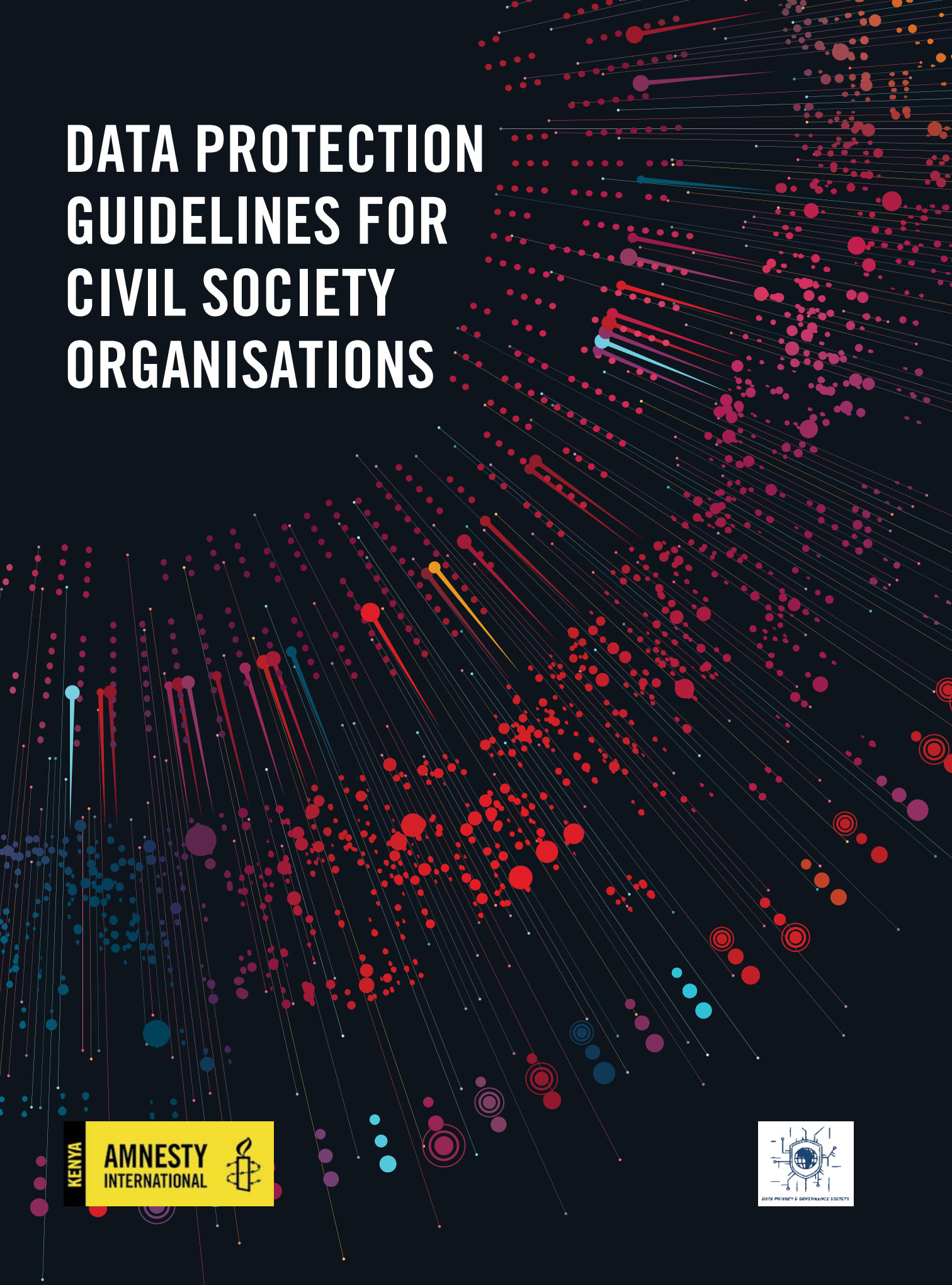
DATA PROTECTION GUIDELINES FOR CIVIL SOCIETY ORGANISATIONS



KENYA AMNESTY INTERNATIONAL

DATA PRIVACY & GOVERNANCE SOCIETY

TABLE OF CONTENTS

EXECUTIVE SUMMARY **4**

ACKNOWLEDGEMENT **5**

LIST OF ABBREVIATIONS **6**

KEY DEFINITIONS **7**

SCOPE & OBJECTIVES **8**

LEGAL FRAMEWORK **9**

1.1. The Constitution of Kenya, 2010 9

1.2. Public Benefit Organisations Act, 2013 9

1.3. Data Protection Act, 2019 10

1.4. Access to Information Act, 2016 11

1.5. Computer Misuse and Cybercrimes Act, 2018 12

DATA GOVERNANCE IN CIVIL SOCIETY ORGANISATIONS **13**

1. Legal Obligation under the Data Protection Act, 2019 13

2. Protection of Beneficiaries and Vulnerable Groups 13

3. Public and Donor Trust 14

4. Digital Transformation and Data-Driven Programming 14

5. Strengthening Civil Society's Role in Promoting Digital Rights 14

KEY COMPONENTS OF DATA GOVERNANCE FOR CIVIL SOCIETY **16**

DATA PROTECTION PRINCIPLES UNDER THE DATA PROTECTION ACT, 2019 **18**

RIGHTS OF A DATA SUBJECT **24**

LAWFUL BASIS FOR PROCESSING PERSONAL DATA **29**

Consent 29

Contract with the Data Subject 30

Legal Obligations 30

Vital Interests of the Data Subject or another person 31

Public Interest 31

Legitimate interests 32

Research 32

RULES FOR PROCESSING SENSITIVE PERSONAL DATA UNDER THE DATA PROTECTION ACT, 2019 **33**

RULES FOR TRANSFERRING PERSONAL DATA OUTSIDE OF KENYA UNDER THE DATA PROTECTION ACT, 2019 34
Requirement to Obtain Consent 34
Transfer based on Appropriate Data Protection Safeguards 35
Transfer based on an Adequacy Decision made by the Data Commissioner 36
Transfer based on a Necessity 36

DATA PROTECTION IMPACT ASSESSMENT (DPIA) 37
Processing Activities Requiring a Data Protection Impact Assessment 37
The Contents of a Data Protection Impact Assessment 38

THE OFFICE OF THE DATA PROTECTION COMMISSIONER (ODPC) 39
The Mandate of the Office of the Data Protection Commissioner (ODPC) 39
Registration as a Data Controller or Processor 40
The Process of Registration as a Data Controller or Processor or both 40
Mandatory Registration 42
Format of a Complaint 42
Enforcement Notices 42
Fines & Penalties 43
The Right to Appeal 43

SETTING UP A PRIVACY PROGRAM 44
Data Map / Data Analysis 44
Develop Data Protection Policies & Notices 45
Protection Policies 45
Privacy Notice 46
C. Regular data protection training and awareness for staff 47
D. Procure the services of DPO 47
E. Design Data Management protocols 47
The Data Lifecycle 48
Vendor assessment and management 49

TECHNICAL & ORGANISATIONAL MEASURES TO MITIGATE DATA PROTECTION RISKS 50

EXECUTIVE SUMMARY

Amnesty International Kenya, in collaboration with the Data Privacy and Governance Society of Kenya (DPGSK), has developed the Data Protection Guidelines for Civil Society Organisations (CSOs) in Kenya to support CSOs in understanding and complying with the Data Protection Act, 2019. These guidelines demystify data protection laws and practices by providing clear, accessible, and actionable guidance tailored to the operational realities of Kenyan civil society and public benefit organisations.

CSOs increasingly collect and process personal data as part of their human rights, humanitarian, development, and advocacy work. With the enactment of the Data Protection Act, 2019, and the establishment of the Office of the Data Protection Commissioner (ODPC), organisations must align their data practices with the law's requirements. However, many CSOs face limited capacity and resources to navigate the legal and technical complexity of data protection compliance. These guidelines address that challenge by providing simplified explanations, practical tools, and real-world scenarios that support rights-based and legally compliant data governance.

The guidelines outline key concepts and definitions, the legal and regulatory framework for data protection in Kenya, and the specific obligations of CSOs under the law. They detail the data protection principles, the rights of data subjects, and the lawful bases for processing personal and sensitive personal data. The guidelines also provide step-by-step guidance on cross-border data transfers, conducting Data Protection Impact Assessments (DPIAs), and engaging with the ODPC, including registration, complaint procedures, and enforcement processes.
Importantly, the guidelines offer a roadmap for establishing internal data governance systems within CSOs, including privacy programs, data lifecycle management, and the development of privacy notices and policies. They also underscore the essential role of CSOs not only as data controllers and processors, but as stewards of digital rights and accountability in Kenya's evolving data ecosystem.

By equipping CSOs with knowledge and tools to comply with the Data Protection Act, this guide advances the twin goals of protecting individual privacy and strengthening public trust in the civic sector. It also reaffirms Amnesty International Kenya's commitment to strengthening data governance in Kenya and the region.

ACKNOWLEDGEMENTS

Amnesty International Kenya is a section of Amnesty International's global movement of over 10 million members and supporters committed to creating a future where human rights are enjoyed. United by our shared humanity, we know that the power to create positive change is within all of us.

Amnesty International Kenya extends gratitude to all those who contributed to the successful completion of the Data Protection Guidelines for Civil Society Organisations. These guidelines could not have been achieved without the invaluable support and insights provided by a range of dedicated individuals. We acknowledge the exceptional efforts of our staff authors & editors Victor Ndede, Benta Moige and Joel Maina for intellectual rigour in shaping these guidelines. We also extend gratitude to Patrick Lavince and Jane Awuor Ombiro, both from DPGSK for their candid feedback, thoughtful contributions, and willingness to share their perspectives that have significantly enhanced these guidelines.

First Published September 2025
197 Place, Lenana Road
P.O. Box 1527-00606 Nairobi, Kenya
Tel: +254 020 – 4283000
Email: amnestykenya@amnesty.org
www.amnestykenya.org

LIST OF ABBREVIATIONS

CBO	Community Based Organization
CSO	Civil Society Organization
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ODPC	Office of the Data Protection Commissioner
PBO	Public Benefit Organization

KEY DEFINITIONS

Key definitions under section 2 of the DPA, applicable to this guide include:

- Data controller is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purpose and means of processing of personal data. CSOs are data controllers because they decide certain key elements of processing, i.e. they define the why and how of processing. For example, when a CSO AB organises an event and collects attendees' personal data through an event registration form. AB will be considered a data controller because it collects, processes and uses data for purposes such as assessing needs and reimbursing attendees.
- Data processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the data controller. CSOs may seek the services of vendors or service providers to collect, store, analyse, and share personal data on their behalf. These institutions that would act on personal data on behalf of CSOs are data processors
- Data governance the overall management of the confidentiality, availability, usability, integrity, and security of data used in an organisation. Responsible data governance requires CSOs to develop policies, strategies, and procedures to ensure data is managed appropriately within an organisation.
- Data subject is a natural person who is the subject of personal data. The natural person can be identified directly or indirectly, by name, identification number, location data, and online identifier or to one or more factors specific such as the physical, physiological, genetic, mental, economic, cultural, or social or social identity.
- Personal data means any information relating to an identified or identifiable natural person such as name, identification number, location data, online identifiers, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity.
- Public benefit activity means an activity that supports or promotes public benefit by enhancing or promoting the economic, environmental, social or cultural development or protecting the environment or lobbying or advocating on issues of general public interest or the interest or well-being of the general public or a category of individuals or organizations.
- Sensitive personal data is 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.
- Data Processing is any operation or sets of operations performed on personal data or on sets of personal data, whether by automated means. The operations include activities 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.
- Technical measures includes physical and digital tools or procedures designed to protect data from unauthorized access, loss, or damage. Such as encryption, firewalls,, pseudonymisation, anti-virus software, etc.
- Organizational measures include policies, practices, and procedures that an organization adapts to ensure proper data management and compliance with legal requirements.

SCOPE & OBJECTIVES

This Guide provides guidelines for data protection for all Kenyan CSOs based on the provisions of the Kenya Data Protection Act, 2019 (DPA). It aims to facilitate the adoption and implementation of appropriate data protection practices in service delivery and organizational administration by the civil society sector for purposes of compliance with the DPA, other relevant legal and regulatory instruments while paying consideration to international best practice. This Guide recognizes the need for the civil society sector to ensure compliance with the DPA, and to uphold the right to privacy in their public benefit activities.

The primary objective of this Guide is to enable the legally compliant, responsible and effective management of data by CSOs by;

Upholding the right to privacy of all data subjects.

Promoting regulatory compliance

Promoting the integration of global data protection principles.

Ensuring data security and adequate risk management

Guiding data lifecycle management

Providing for continuous improvement in data protection

Examples provided in this Guide are for illustrative purposes. CSOs ought to tailor the examples to their specific needs.

LEGAL FRAMEWORK

The legal framework regulating the civil society sector in Kenya is guided by the Constituion of Kenya and acts of parliament. The Acts include: 2010, the Public Benefit Organisations Act, 2024, the Data Protection Act, 2019, Access to Information Act, 2016, and the Computer Misuse and Cybercrimes Act, 2018.

1.1. The Constitution of Kenya, 2010

All persons and organizations operating in Kenya are subject to the Constitution of Kenya as the Supreme law of the land. Article 31 of the Constitution provides for the right to privacy as follows:

'Every person has the right to privacy, which includes the right not to have—

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

(d) The privacy of their communications infringed.'

Although Article 31 does not explicitly mention it, this article governs data and personal information as these are considered by law as the property of individual data subjects. From this article emanates a constitutional obligation to respect, protect and promote the right to privacy.

Article 35 of the Constitution provides for the right to access information which grants every citizen the right to access information held by another person and required for the exercise or protection of any right or fundamental freedom. Further, Article 35 grants the right to the correction or deletion of untrue or misleading information that affects the person.

Data governance in the civil society sector is subject to the supremacy of the above constitutional provisions. It thus requires all CSOs to administer themselves and operate in a manner which upholds the right to privacy and the right to access information.

The Constitution is a binding document, and Civil Society Organisations are bound to enforce the same.

1.2. Public Benefit Organisations Act, 2013

This Act repeals and replaces the Non-Governmental Organisations Co-ordination Act, 1990 and is now the current governing law for all local and international civil society and non-governmental or non-profit organizations operating in Kenya. The Act also recognizes the important role that public benefit organizations play in serving the public good, supporting development, social cohesion and tolerance

within society; promoting democracy, respect for the rule of law, and providing accountability mechanisms that can contribute to improved governance. These accountability mechanisms include data protection and compliance measures.

1.3. Data Protection Act, 2019

The DPA was enacted to operationalise Article 31 of the Constitution. It regulates the processing of personal data, the rights of data subjects and the obligations of data controllers and processors.

Data processing is critical to the operation and administration of any CSOs. CSOs handle and shares personal information of their employees, funders or beneficiaries, as they execute their mandate. Their operations, therefore, falls under the purview of the DPA.

Key provisions of the Act

Section 5 of the DPA establishes the Office of the Data Protection Commissioner (ODPC) as Kenya's data protection regulator, a state corporation with legal entity status, meaning it can be sued.

Section 18 provides for the requirement to register as a data controller, a data processor, or both.

Section 25 provides for the principles of data protection.

Section 26 of the DPA spells out the rights of a data subject

Section 30 provides for the lawful bases for processing personal data

Section 31 provides for the requirements to carry out a Data Protection Impact Assessment

Section 44 provides the grounds to process personal data

Section 48 provides for the conditions to transfer personal data outside Kenya

Section 56 provides for lodging of complaints with the data commissioner

Section 58 provides for enforcement

Section 62 deals with penalty notices

Section 65 provides for the compensation of data subjects

To give effect to the DPA, there exist subsidiary regulations in place, being; the Data Protection (General) Regulations, 2021, the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021, and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

1.4. Access to Information Act, 2016

This Act operationalizes Article 35 of the Constitution on the right of access to information.

Key provisions

Section 4 obligates CSOs to heed any requests by a data subject to access information held by the organization "where that information is required for the exercise or protection of any right or fundamental freedom." This directly upholds the right of a data subject to access their personal data in the custody of the organisation.

Section 6 provides for the limitation of the right to access information, which limits the right to access information if it involves the unwarranted invasion of the privacy of an individual.

1.5. Computer Misuse and Cybercrimes Act, 2018

The Act makes provisions for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; to facilitate international cooperation in dealing with computer and cybercrime matters

CSOs should ensure that their systems are protected in such a way that they do not facilitate crimes under the Act. On the other hand, CSOs should be able to detect, contain, assess, mitigate and report any attacks on their systems or any such cybercrimes to the National Computer and Cybercrime Coordination Committee and the ODPC.

Data Protection for Civil Society Organisations and Public Benefit Organisations in Kenya operates at the forefront of promoting human rights, social justice, humanitarian aid, governance, and development. In doing so, they frequently collect, store, and process personal data, including information on beneficiaries, donors, staff, and research data. With the enforcement of the Data Protection Act, 2019 (DPA), these organisations must now ensure that their data practices align with legal obligations designed to protect individuals' privacy and personal information.

Prioritising data protection compliance is not only a technical or administrative issue, it is a matter of legal accountability, public trust, and organisational resilience. There are key reasons why CSOs and PBOs must place data protection at the core of their operations.

DATA GOVERNANCE IN CIVIL SOCIETY ORGANISATIONS

1. Legal Obligation under the Data Protection Act, 2019

The DPA establishes a legal framework that applies to any person or entity that processes personal data within Kenya or outside Kenya where the data relates to individuals within Kenya. CSOs and PBOs are not exempt from this law.

Organisations are required to:

- Register with the Office of the Data Protection Commissioner (ODPC) as data controllers or processors.
- Ensure lawful, fair, and transparent processing of personal data.
- Implement data protection principles, including purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality.
- Obtain consent for data processing, especially for sensitive personal data.
- Conduct Data Protection Impact Assessments (DPIAs) for high-risk data activities.

Non-compliance can result in fines, enforcement notices, and reputational damage, ultimately undermining donor relationships and operational sustainability.

2.Protection of Beneficiaries and Vulnerable Groups

Many CSOs work with marginalised, at-risk, or vulnerable populations such as children, survivors of violence, refugees, persons with disabilities, or political dissidents. Mishandling of their personal data can expose them to harm, discrimination, or fatal consequences.

Prioritising data protection helps:

- Safeguard the dignity, privacy, and safety of individuals.
- Reduce risks of identity theft, surveillance, exploitation, or secondary victimisation.
- Enhance ethical standards in programme design, implementation, and evaluation.

By embedding data protection into their work, CSOs reinforce their role as defenders of rights both offline and online.

3. Public and Donor Trust

Trust is the lifeblood of civil society. Stakeholders including communities, donors, partners, and the public expect organisations to handle personal data with integrity and responsibility.

Data protection compliance:

- Demonstrates commitment to transparency and accountability.
- Signals organisational maturity and risk awareness to funders.
- Enhances credibility in advocacy for digital rights and ethical technology use.

Organisations that handle data irresponsibly risk losing funding, partnerships, and legitimacy especially in an environment where privacy and data rights are becoming central to democratic governance.

4. Digital Transformation and Data-Driven Programming

As CSOs increasingly rely on digital tools for communication, fundraising, monitoring and evaluation, and service delivery, they become data-driven entities. This transformation amplifies the need for clear, robust data governance frameworks.

Prioritising data protection ensures:

- Responsible innovation and ethical use of data technologies.
- Clear protocols for handling data breaches, consent management, and third-party vendors.
- Organisational agility in adapting to emerging regulations and international data standards.

This proactive approach reduces operational risks and aligns organisations with global trends in data privacy and responsible data use.

5. Strengthening Civil Society's Role in Promoting Digital Rights

CSOs are key actors in shaping the discourse and policies on human rights in the digital age. By modelling good data governance practices, they:

- Set standards for ethical data use in development and humanitarian sectors.
- Build stronger cases in advocating for privacy rights and digital freedoms.
- Contribute to a culture of accountability and democratic governance in Kenya's data ecosystem

Data protection is not just a compliance checkbox; it is a strategic, ethical, and operational imperative for civil society and public benefit organisations in Kenya. In an era of growing digital surveillance, cybercrime, and information misuse, CSOs must lead by example in protecting the rights and data of the people they serve. By prioritising compliance with the Data Protection Act, 2019, organisations not only meet legal requirements but also strengthen their integrity, credibility, and long-term impact.

KEY COMPONENTS OF DATA GOVERNANCE FOR CIVIL SOCIETY

The key components of data governance for CSOs include:
Data collection and storage: CSOs must collect and store data securely while ensuring that they comply with data privacy regulations. This includes implementing appropriate technical and organizational measures to ensure the security of data in their custody.

Data usage and access:
CSOs must define who has access to their data and how it can be used. This includes developing clear data usage policies and procedures and training staff on these policies.

Data sharing and collaboration:
CSOs often share data with funders, partners and third-party vendors.
It is important to establish protocols for sharing data safely and securely.

Data retention and disposal:
CSOs must define how long they will retain data and when and how it will be disposed of. This includes developing data retention policies and procedures and securely destroying data that is no longer needed Data in Custody of CSOs

The DPA governs personal data which is defined under the Data Protection Act as “any information relating to an identified or identifiable natural person. The term ‘natural person’ is a legal term used to distinguish between a living human being and a legal or corporate entity (an unnatural person). CSOs mostly handle personal data of their employees, staff, members, beneficiaries, partners, and third-party vendors or contractors with whom they do business.

Section 25 of the DPA **outlines the requirements for processing personal data.**

This broad definition under the DPA is further categorised into personal data and sensitive personal data. The Act defines sensitive personal data as, "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." This can be understood by CSOs to refer to personal information, which on the face of it can be used to discriminate. Due to its sensitive nature, this type of data is subject to more stringent rules for processing compared to personal data.

Section 44 of the Act provides that sensitive personal data shall not be processed unless under the grounds permitted in Section 45 and 46.

Table 1. A table on examples of personal data vs. sensitive personal data.

Personal data	Sensitive personal data
Name	Health status
Phone number	Ethnicity
Location	Religion
ID Number	Marital status
Postal Address	Biometric data

DATA PROTECTION PRINCIPLES UNDER THE DATA PROTECTION ACT, 2019

The principles of data protection are the overarching ideas which should guide the data governance of CSOs. The adoption, integration and implementation of these principles in the organisation promote compliance with the DPA.
Section 25 of the DPA provides the principles of data protection as follows;

The Right to Privacy

Section 25 (a) provides that **"Every data controller or data processor shall ensure that personal data is processed in accordance with the right to privacy of the data subject."**

CSOs must always bear in mind Article 31 of the Constitution which protects the right to privacy of individuals. This right to privacy extends from tangible property of the right holder to their personal data and information. This means that any data processed in a manner which violates or undermines the right to privacy of the data subject contravenes the DPA. This could result in fines or criminal sanctions being imposed on the part of the data processor or controller.

Lawfulness, Fairness, and Transparency

Section 25 (b) provides that '**Every data controller or data processor shall ensure that personal data is processed lawfully, fairly and in a transparent manner in relation to any data subject.'**

Lawful processing of personal data:
Lawfulness refers to the requirement that processing must be conducted in accordance with a valid legal provision, such as consent, vital interest, or contract performance. Processing is considered lawful only when one of these legal grounds is present. At least one legal basis must apply to the processing operations.

Fair processing of personal data:
When processing personal data, CSOs should bear in mind provisions of Article 27 of the Constitution. Every data subject should be treated equally and should not be discriminated against directly or indirectly on any ground that may include race, sex, pregnancy, marital status, health status, ethnic or social origin, colour, age, disability, religion, conscience, belief, culture, dress, language, or birth. CSOs should not process personal data in a manner that is unduly detrimental, unexpected or misleading to the data subjects.

Transparent processing of personal data:
Before processing of personal data, CSOs must inform data subjects of the following:

What specific personal data do they collect.
Why they need to collect personal data.
How they collect personal data.
How they will use the personal data collected.
How they store the personal data.
The period for which the personal data will be stored.
The measures in place to keep the personal data safe.
Whether they share the personal data with third parties.
The rights of the data subjects and how they can be exercised

Legitimate Purpose

Section 25 (c) provides that, **'Every data controller or data processor shall ensure that personal data is collected for explicit, specified, and legitimate purposes and not further processed in a manner incompatible with those purposes.'**

Explicit and specified purposes: CSOs must expressly inform data subjects of the purposes for which they seek to process their personal data. Example: Organization A: is organizing a free sensitization session on data protection. It informs all the prospective participants that their personal data will be processed solely for the purpose of monitoring attendance. CSOs

Legitimate purposes:
A legitimate purpose for processing data under the DPA is considered to mean a lawful purpose. This means that CSOs must establish a lawful/legitimate purpose prior to processing data.

Section 30 of the DPA outlines the legitimate and lawful purposes for processing data as follows; where the data subject has consented, or where processing is necessary.

Data Minimisation

Section 25 (d) provides that **'Every data controller or data processor shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.'**

This places an obligation on CSOs to process only data which is necessary to achieve a specific purpose. CSOs should not collect more data than is necessary. For example, a CSO conducting a workshop may collect the personal data of attendees for the purpose of keeping a record of attendance and to process travel reimbursement. The attendance form here should be limited to information which is necessary to record the number of attendees, and the details required to process payment. Any information which is not necessary beyond the scope of attendance records and payment should not be collected or processed.

The extent of data minimisation is dependent on the specific functions of the organisation and will naturally vary from one organisation to another. An organisation mandated to work with specific beneficiaries such as women may need to collect the gender data of attendees while an organisation working on animal rights may not need to record the gender of attendees.

Valid Explanation

Section 25 (e) provides that **'Every data controller or data processor shall ensure that personal data is collected only where a valid explanation is provided whenever information relating to family or private affairs is required.'**

This places an obligation on CSOs to inform data subjects on the reasons for which they are seeking information relating to the family or private affairs of the data subject. The valid reasons provided must relate to the legitimate functions of the organisation and must fall under the legitimate purposes for processing outlined under Section 30 of the DPA.

Accuracy

Section 25 (f) provides that **'Every data controller or data processor shall ensure that personal data is accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay.'**

This places an obligation on CSOs to ensure that the data in their custody is accurate, up to date and verifiable. Further, when an organisation keeps a record of inaccurate, unverified or incorrect data, this could become prejudicial to the data subject.

CSOs therefore need to record details accurately by verifying data collected, promptly making corrections where data is inaccurate and destroying false or misleading data.

Storage Limitation

Section 25 (g) provides that '**Every data controller or data processor shall ensure that personal data is kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected.'**

This places an obligation on CSOss to ensure that there is an established lifecycle for data in the custody of the organisation. This will include a data retention schedule for all personal data collected, and a disposal or deletion policy to destroy data at the end of its life cycle.

When developing a data management cycle, organisations must consider data retention principles, with particular emphasis on legal retention. This principle obligates organisations to retain personal data for specified durations, even if such data is not actively in use, to ensure compliance with applicable legal and regulatory requirements.

For example, under the Employment Act, an employee may lodge a claim for unfair dismissal up to three years following the termination of employment. Consequently, organisations must retain employee records for at least three years after the employees' departure. Similarly, the government of Kenya requires businesses to maintain essential business records, including contractual and accounting documents, for a minimum of seven years.

Moreover, the Limitation of Actions Act prescribes statutory timeframes for initiating legal actions. In alignment with these provisions, organisations may be required to retain personal data relevant to contractual commitments or potential criminal liability for periods corresponding to the limitations set out in the Act.

Due Diligence and Adequacy in Data Transfers

Section 25 (h) provides that **'Every data controller or data processor shall ensure that personal data is not transferred outside Kenya unless there is proof of**

adequate data protection safeguards or consent from the data subject.'

Section 48 of the DPA provides for the conditions under which personal data can be transferred outside Kenya. This places an obligation on CSOs sharing, processing or storing data outside of Kenya first to conduct due diligence to establish that the receiving entity has data protection safeguards adequate to those under Kenya's DPA, 2019.

CSOs are often engaged with funders, partners and third-party vendors outside of Kenya in their day-to-day business. Many organisations for example procure cloud storage from third-party vendors whose data centers are outside Kenya

RIGHTS OF A DATA SUBJECT

Section 26 of the DPA provides for the following data subject rights;

(a)	be informed of the use to which their personal data is to be put;
(b)	access their personal data in custody of data controller or data processor;
(c)	object to the processing of all or part of their personal data;
(d)	correction of false or misleading data; and
(e)	deletion of false or misleading data about them."

Where the data subject is unable to or incapable of exercising their rights under Section 26, these rights can be exercised on their behalf by a parent, guardian or a person duly authorised to act. According to Section 27 of the DPA, a data subject may be unable to or incapable of exercising their rights if they are a minor, or if they have any mental disorder or other disability rendering them incapable of exercising their right. Further, a data subject may legally authorise a person to act on their behalf in exercising their rights such as an administrator, or where there exists a power of attorney or any such legal authority.

The Right to be informed

Section 29 of the DPA outlines the information that should be provided to a data subject. CSO should inform a data subject of:

'(a)	the rights of a data subject specified under section 26 of the DPA.
(b)	the fact that personal data is being collected.
(c)	the purpose for which the personal data is being collected.
(d)	the third parties whose personal data has been or will be transferred to, including details of safeguards adopted.
(e)	the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data.
(f)	a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data.

(g)	the data being collected pursuant to any law and whether such collection is voluntary or mandatory.
(h)	the consequences if any, where the data subject fails to provide all or any part of the requested data.'

The organization should adhere to the data subject's right to be informed by providing all the information listed above within a privacy notice or consent form, which must be made available to the data subject before their personal data is collected and further processed. An organization's privacy notice must be made available in print form, or digitally for instance via email or uploaded on the organization website.

Where there are any future changes or updates to the privacy notice of an organization, the data subjects must be notified of this and must be furnished with the updated privacy notice.

The Right to Access Personal Data

A data subject reserves the right to access personal data in the custody of CSOs. As per the Data Protection (General) Regulations, 2021, a request to access personal data may be made by the data subject or their representative via Form DPG 2. This form is found in the First Schedule of the Data Protection (General) Regulations, 2021.

The above request may include a request for information on;

- the purposes of the processing.
- the categories of personal data concerned.
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, including recipients in other countries or territories.
- where possible, the envisaged period for which the personal data may be stored, or, if not possible, the criteria used to determine that period.
- where the personal data is not collected from the data subject, any available information as to the source of collection.

Following this, the organisation receiving such a request must either comply with the request for access or provide (in writing) a legal justification for refusal to comply with the request within seven (7) days of receiving the request. In legal terms, a request will be considered received once it has been duly posted to the correct address if by post, or once it has been sent if by digital means.

The Right to Object to Processing

Section 34 of the DPA provides that a data subject may restrict the processing of their personal data where;

- the accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data;
- personal data is no longer required for the purpose of the processing, unless the data controller or data processor requires the personal data for the establishment, exercise, or defence of a legal claim;
- processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or
- data subject has objected to the processing, pending verification as to whether the legitimate interests of the data controller or data processor overrides those of the data subject.

Section 36 of the DPA provides that a data subject may object to the processing of their personal data unless a CSO can demonstrate compelling legitimate interests for processing which override the data subject's interests, or where the processing is necessary for the establishment, exercise or defence of a legal claim. However, CSOs should take note that Regulation 8 of the Data Protection (General) Regulations, 2021 indicates that the right to object to processing operates as an absolute right where the objection is regarding processing personal data for direct marketing purposes.

A data subject may exercise this right to object to the processing of their personal data by making a request under Form DPG1 as provided for under the First Schedule of the Data Protection (General) Regulations, 2021.

Following this, organisations should comply with the request or provide (in writing) legal justifications for refusal to comply within fourteen (14) days of receipt of the request.

The Right to not be Subject to Automated Decision Making

Section 35 of the DPA provides that **"every data subject has a right to not be subject to a decision based solely on an automated decision-making process including profiling, which produces legal effects concerning or significantly affects the data subject."**

This places a responsibility on CSOs utilizing automated decision making processes or algorithms to assess the legal and other significant effects of their processes on the data subject. As per Section 35 (3), where a CSO takes such a decision based solely on automated decision-making processes and which produces legal effects or significantly impacts the data subject, the organization must promptly notify the data subject in writing.

The right to object to this Section shall not apply where the decision is necessary for performing contractual obligations, or authorised by law, or where the data subject has consented after being properly informed.

Example
Some non-governmental organisations which specialise in the protection of human rights defenders (HRDs) may receive a high volume of requests for assistance. In such cases, it may be necessary to employ computer systems to filter and identify candidates who meet the established criteria for protection. However, it is essential that, because this decision involves an automated system, a mandatory human review from a protection officer or a designated officer is employed for this system. This will ensure that the essential aspects of this application, which the computer system might overlook, are identified and corrected by a human before a final determination is made.

The Right to Correction of False or Misleading Information

Section 40 of the DPA states that a data subject has the right to correct or rectify personal data in the custody of CSOs where the information is inaccurate, out-of-date, incomplete or misleading.

A data subject can exercise this right by making a request under Form DPG 3 set out in the First Schedule of the Data Protection (General) Regulations, 2021. This request for rectification may be supported by any relevant documentation.

Upon receipt, CSOs should comply with the request within fourteen (14) days, or may provide (in writing) reasons for refusal to comply within seven (7) days of the request.

The Right to Deletion

Section 40 of the DPA provides for the right to erasure, also known as the right to deletion or more commonly, the right to be forgotten.

CSOs should erase, delete or destroy personal data where it is no longer authorised to retain the data, or where consent has been withdrawn or where the data is no longer relevant, or where the data collected was excessive or was obtained unlawfully.

Under Regulation 12 of the Data Protection (General) Regulations, 2021, a right of erasure may apply where:

'(a)	the personal data is no longer necessary for the purpose which it was collected;
(b)	the data subject withdraws their consent that was the lawful basis for retaining the personal data;
(c)	the data subject objects to the processing of their data and there is no overriding legitimate interest to continue the processing;
(d)	the processing of personal data is for direct marketing purposes and the individual objects to that processing;
(e)	the processing of personal data is unlawful including in breach of the lawfulness requirement; or
(f)	the erasure is necessary to comply with a legal obligation.'

For an erasure request, a data subject is to make a request under Form DPG 5 set out in the First Schedule of the Data Protection (General) Regulations, 2021. The application may be supported by documentation to support the request for erasure.

CSOs are required to comply with the request for deletion within fourteen (14) days of the request without charging the data subject any fee. Such a request may also be denied where legitimate and justifiable reasons can be provided to the data subject.

The right to erasure may be justifiably denied where the processing is necessary;

- to exercise the right to freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research, historical research, or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise, or defence of a legal claim.

CSOs must be aware that data subjects exercise their rights by other avenues such as sending emails, or making phone calls, as a result CSOs must then train their staff to be able to identify when a right has been exercised to have internal procedures that guide how the staff can escalate those requests to the relevant officer in charge of handling them. This is because most data subjects do not use the forms to exercise their rights.

LAWFUL BASIS FOR PROCESSING PERSONAL DATA

CSOs should not process any personal data unless they have established a lawful basis for processing personal data. The DPA provides seven lawful bases for processing personal data under Section 30. These include;

Consent

CSOs can process personal data lawfully after duly informing the data subject of the specified legitimate purpose for processing and obtaining their consent. Consent must be explicit, informed and voluntary. This means that the data subject must explicitly and voluntarily express consent to a data processing activity which they are duly informed about, and this consent must be obtained by the data controller or processor before the processing activity.

Section 32 (2) allows a data subject to withdraw consent at any time. Furthermore, if a data subject withdraws their consent, this withdrawal shall not affect any previous processing activities. This means that at the point of withdrawal of consent, this will only hinder further processing activities but does not affect previous lawful processing activities.

Minors and mentally incapacitated persons cannot legally consent. Section 27 of the DPA allows a legal guardian or representative to consent on behalf of an incapable data subject.

Section 32 of the DPA places an evidentiary obligation on CSOs as the data controllers or processors to bear the burden of proving that a data subject's consent to the processing of their personal data.

Regulation 4.2 of the Data Protection General Regulations 2021 permits various methods of obtaining consent. Consent forms are an effective way for CSOS to demonstrate that consent was duly obtained. A consent form should be dated and should include the name, age and signature of the data subject. Furthermore, the consent form should expressly include a declaration by the data subject that they have been duly informed of the fact that their personal data is being collected, and explicitly state what personal data is being collected and the extent to which this data will be processed.

Regulation 4 of the Data Protection (General) Regulations, 2021, provides for the contents of a standard consent form. That is

(a) the identity of the data controller or data processor.

(b) The purpose of each of the processing operations for which consent is sought.

(c) the type of personal data that is collected and used.

(d) information about the use of the personal data for automated decision-making, where relevant.

(e) the possible risks of data transfers due to absence of an adequacy decision or appropriate safeguards.

(f) whether the personal data processed shall be shared with third parties.

(g) the right to withdraw consent.

(h) the implications of providing, withholding, or withdrawing consent.

Contract with the Data Subject

The performance of a contract is one of the lawful basis and legitimate purposes for processing personal data under the DPA.

Section 30 (1) allows a data controller or processor to collect personal data **"where the processing of the data is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract."**

An existing contract signed by the data subject and data controller or processor is considered a lawful basis for processing personal data . Further, a CSO may collect personal data with the permission of a data subject for the purposes of entering into a contract with them. Example: CSOs process employee personal data under contractual necessity as the lawful basis.

Legal Obligations

A data controller or processor is allowed to process the personal data of a data subject where this is necessary to comply with a legal obligation. The term 'legal obligation' here includes compliance with court orders, regulatory compliance and compliance with existing laws which the data controller or processor is subject to. The understanding here is that the data controller or processor shall process personal data in order to adhere to a legal requirement.

Example:
A CSO implementing a program is required by the employment law and tax regulations to collect and retain personal data of its staff and interns including ID numbers, PIN certificates, and bank details or payroll processing, statutory deductions, and reporting to government agencies such as the Kenya Revenue

Authority (KRA) and the National Social Security Fund (NSSF).
In this case, the processing is based on a legal obligation, not consent, because the organisation is required by law to process this data to comply with employment and tax laws.

Vital Interests of the Data Subject or another person

A data controller or processor may process personal data where this is necessary to protect the vital interests of the data subject or another natural person. This means that CSOs can process personal data to protect the vital interests of data subjects or other individuals in situations where immediate and essential action is required to safeguard their rights and freedoms.

Example:
A CSO providing emergency relief during a natural disaster collects personal data including names, medical conditions, and next of kin contacts from injured or unconscious individuals to coordinate urgent medical treatment and family tracing. In this situation, the processing is necessary to protect the vital interests of the data subject, particularly their life and physical wellbeing. Because the individual may be unable to give consent due to the emergency, the CSO is permitted to process their data without prior consent, provided it is strictly necessary for the life-saving intervention.

Public Interest

Another lawful basis for processing personal data is the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or processor. This means that CSOS can process personal data under the legal basis of performing a task in the public interest.

For example,
A CSO monitoring elections collects personal data such as names, phone numbers, and polling experiences from volunteer election observers across the country to document and report on electoral integrity.
This processing serves a public interest purpose by promoting transparency, democratic accountability, and credible elections. It meets the criteria under the Data Protection Act, 2019, for lawful processing without requiring individual consent, provided the data is necessary for performing a task carried out in the public interest and appropriate safeguards are in place.

Legitimate interests

Another lawful basis for processing personal data is the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed. A third party contracted by the data controller may process the personal data of a data subject for a legitimate interest.

CSOs(or their contracted third parties) can establish the lawful basis of legitimate interests by processing personal data in situations where there is an existing relationship with the data subject, and the processing is necessary to achieve a legitimate purpose without infringing on the data subject's rights. Legitimate interest can serve as a legal basis for processing personal data in various scenarios including fraud prevention and safety and security. Before relying on this legal ground, CSOs should conduct and document a legitimate interest assessment.

Example
A CSO that runs a membership-based civic engagement platform sends periodic email updates to its registered members about upcoming advocacy events, policy briefs, and opportunities to participate in campaigns.
The CSO processes members' names and email addresses based on its legitimate interest in engaging its community and fulfilling its organisational mandate. The processing is expected, has minimal privacy impact, and members can reasonably object or opt out at any time.

Research

The seventh legitimate purpose for processing personal data is where this is necessary for historical, statistical, journalistic, literature and art or scientific research purposes. This provision recognizes the importance of these activities in contributing to societal knowledge, preserving history, and fostering cultural and scientific advancement. Such processing must comply with data protection principles, including purpose limitation, data minimization, and ensuring that the rights and freedoms of data subjects are not unduly affected.

RULES FOR PROCESSING SENSITIVE PERSONAL DATA UNDER THE DATA PROTECTION ACT, 2019

Section 45 of the DPA, sets out the grounds under which sensitive personal data can be processed. They include:

1. Processing carried out during legitimate activities by foundations, associations or not-for-profit bodies with apolitical, philosophical, religious or trade union aim. However, the processing must relate solely to the members of the body or to persons who have regular contact with the body and the personal data is not disclosed outside the body without the consent of the data subject.

2. The processing relates to personal data which has been made public by the data subject.

3. The processing is necessary for the following purposes;

i) To establish, exercise or defend a legal claim;

ii) To carry out the obligations and exercise specific rights of the data controller or the data subject;

iii) To protect the vital interest of the data subject or another person.

These restrictions on sensitive personal data take into account the nature of this kind of data. This is because processing sensitive personal data poses a risk of significant harm to the data subject.

RULES FOR TRANSFERRING PERSONAL DATA OUTSIDE OF KENYA UNDER THE DATA PROTECTION ACT, 2019

Personal data cannot be transferred outside Kenya unless the transferring organization has obtained consent from the data subject to transfer the data. This means that where CSOs intend to transfer data beyond the Kenyan boundaries, they must adhere to the consent requirement under the Act, by duly informing the data subject of the transfer and obtaining their consent for the transfer.

Under Section 49 of the DPA, processing of sensitive personal data outside of Kenya can only be done with the consent of the data subject. The DPA imposes an obligation on civil society to ensure that personal data is not transferred outside Kenya unless there is proof of adequate data protection safeguards and consent from the data subject. CSOs transferring data outside Kenya therefore have an obligation to conduct due diligence to ensure the adequacy of data protection safeguards on the receiving party's end. This means that the data protection laws, policies, and frameworks of the party receiving the data must meet the standards set by Kenya's Data Protection Act, 2019.

Requirement to Obtain Consent

Regulation 46 of the Data Protection (General) Regulations 2021 places emphasis on the obligation to obtain consent before transferring personal data outside of the country if an adequacy decision is absent, appropriate safeguards or prerequisite for transfer as a necessity A data subject must explicitly consent to the proposed transfer and he/she must be informed of the possible risks of the transfer.

Example:
A CSO has received a request from its US-based donor to share personal data of project beneficiaries to fulfil reporting obligations. Before proceeding with any data transfer, the CSO must obtain explicit consent from the project's beneficiaries.

Section 48 of the DPA outlines the conditions for transferring personal data outside Kenya.

1. The transfer may be made where there is proof provided to the Data Commissioner that appropriate safeguards exist with respect to the security of the personal data.

2. The data will be transferred to a country with data protection laws similar to those in Kenya.

3. The transfer is necessary for

   3.1. Performance of a contract.

   3.2. Public interest.

   3.3. For judicial purposes.

   3.4. To protect the vital interests of a data subject.

   3.5.For compelling legitimate interests.

Regulation 40 of the Data Protection (General) Regulations 2021 mirrors the data transfer provisions found in the Data Protection Act, 2019.

Transfer based on Appropriate Data Protection Safeguards

According to Regulation 41 (1) of the Data Protection (General) Regulations 2021, 'appropriate data protection safeguards' are demonstrated where;

- The data recipient outside Kenya is subject to an existing legal instrument containing data protection rules and safeguards that is equivalent to Kenya's Data Protection Act; or

- The transferring entity having assessed all the circumstances surrounding transfers of that type of personal data to another country or relevant international organization, concludes that appropriate safeguards exist to protect the data.

Regulation 42 of the Data Protection (General) Regulations 2021 provides that 'appropriate data protection safeguards' can be assumed to exist where the country of the receiving entity has

(a) ratified the African Union Convention on Cyber Security and Personal Data Protection;

(b) a reciprocal data protection agreement with Kenya; or

(c) a contractual binding corporate rules among a concerned group of undertakings or enterprises

It is therefore the responsibility of CSO to conduct due diligence exercise which should establish that they are satisfied that the entity to which the data is being transferred, has data protection safeguards which meet the standards under the DPA. Example: A Kenyan based CSO intends to transfer personal data of its employees to its subsidiary in Angola. Before proceeding with the transfer, the appointed DPO conducts due diligence on Angola's data protection framework. The DPO confirms that Angola has ratified the African Union Convention on Cybersecurity and Personal Data Protection. Based on this finding, the CSO concludes that appropriate safeguards are in place, allowing the data transfer to proceed

Transfer based on an Adequacy Decision made by the Data Commissioner

An adequacy decision is a declaration by the data commissioner that a country, territory within a country or relevant international organization has satisfied an adequate level of personal data protection equivalent to Kenya.

The ODPC is mandated to publish a list of the countries, territories and specified sectors within that other country and relevant international organization for which the Data Commissioner has decided that an adequate level of protection is guaranteed. (However, ODPC is yet to publish this list

Transfer based on a Necessity

Regulation 45 of the Data Protection (General) Regulations 2021 provides that transfer may be lawful on the basis on necessity where such a transfer is necessary;

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

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

(iii) for any matter of public interest;

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

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

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

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

In law, when an activity is reasonably expected to negatively or substantially impact specific human, environmental, or social rights, an impact assessment is conducted to mitigate those risks.

The Data Protection Impact Assessment (DPIA) refers to the process designed to identify risks associated with the processing of personal data. The aim of conducting a DPIA is to identify and to minimise the risks as far and as early as possible.

Section 31(5) of the DPA requires a data processor or controller to submit the DPIA report to the ODPC within 60 days before the processing activity.

Processing Activities Requiring a Data Protection Impact Assessment

Under Section 31 of the DPA, it is a mandatory requirement for all organisations engaged in processing operations that are likely to result in high risk to the rights and freedoms of a data subject, to carry out a data protection impact assessment and submit the same to the Data Protection Commissioner prior to the processing. Regulation 49 of the Data Protection (General Regulations) 2021 provides clarity on the circumstances under which a DPIA must be conducted. This Regulation provides that processing activities considered as likely to result in high risk to the rights and freedoms of a data subject include the following;

(a) automated decision making with legal or similar significant effect that includes the use of profiling or algorithmic means or use of sensitive personal data as an element to determine access to services or that results in legal or similarly significant effects;

(b) use of personal data on a large-scale for a purpose other than that for which the data was initially collected;

(c) processing biometric or genetic data;

(d) where there is a change in any aspect of the processing that may result in higher risk to data subjects;

(e) processing sensitive personal data or data relating to children or vulnerable groups;

(f) combining, linking or cross-referencing separate datasets where the data sets are combined from different sources and where processing is carried out for different purposes;

(g) large scale processing of personal data;

(h) a systematic monitoring of a publicly accessible area on a large scale;

(i) innovative use or application of new technological or organizational solutions; or

(j) where the processing prevents a data subject from exercising a right.

The Contents of a Data Protection Impact Assessment

Where a DPIA is required, a data controller or processor shall conduct the DPIA in the template set out in the Third Schedule of the Data Protection (General) Regulations 2021 and in the ODPC Guidance note on Data Protection Impact Assessments.

From the template of a DPIA as set out in the Third Schedule of the General Regulations, the ODPC requires a proper and comprehensive DPIA to have the following;

- A comprehensive explanation of the intended processing activities and goals,
- An evaluation of the necessity and proportionality of the processing in relation to the established legitimate purposes for processing;
- An analysis of the potential threats to data subjects' rights;
- The measures guaranteed to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the DPA, considering the rights, and legitimate interests of data subjects and other persons concerned.
- Upon conducting DPIA, CSOs should generate a DPIA report and submit it to ODPC

Example:
A CSO conducting a nationwide survey on access to healthcare services among people living with HIV collects sensitive health data and geolocation information from thousands of individuals across multiple counties.
Because the activity involves large-scale processing of sensitive personal data, including health status and potentially identifiable location data, it would require a Data Protection Impact Assessment (DPIA) under Section 31 of the Data Protection Act, 2019 and the Data Protection (General) Regulations, 2021.
This example highlights high-risk processing due to the nature of the data (health), the scale of processing, and the potential impact on data subjects, key factors that trigger the DPIA requirement.

THE OFFICE OF THE DATA PROTECTION COMMISSIONER (ODPC)

The Office of the Data Protection Commissioner, commonly referred to as the ODPC, is the Kenyan regulatory authority responsible for governing data protection. The ODPC is established under the DPA and has the power to oversee enforcement the provisions of the Act.

The Mandate of the Office of the Data Protection Commissioner (ODPC)

Provided for under Section 8 of the DPA and includes:-

i. To oversee the implementation of and be responsible for the enforcement of the Act;

ii. To establish and maintain a register of data controllers and data processors;

iii. To exercise oversight on data processing operations, either on its own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with the Act;

iv. To promote self-regulation among data controllers and data processors;

v. To conduct an assessment, on its own initiative of a public or private body, or at the request of a private or public body for the purpose of ascertaining whether information is processed according to the provisions of this Act or any other relevant law;

vi. To receive and investigate any complaint by any person on infringements of the rights under the Act;

vii. To take such measures as may be necessary to bring the provisions of this Act to the knowledge of the public;

viii. To carry out inspections of public and private entities with a view to evaluating the processing of personal data;

ix. To promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements;

x. To undertake research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals

Registration as a Data Controller or Processor

Section 18 of the DPA stipulates that no person shall act as a data controller or data processor unless they are registered with the Data Commissioner. This means that all data controllers and data processors must register unless they can clearly demonstrate that they fall within an exemption.

Regulation 3.3 of the ODPC Guidelines on Registration as a Data Controller or Processor stipulates that CSOS and such charitable organisations are required to register as a data controller or processor and must pay the prescribed fees. This registration is renewable after every two years where a prescribed renewal fee will be charged.

The Process of Registration as a Data Controller or Processor or both

A CSO have to determine whether it is a data controller or processor or both. The ODPC Guidance Note on Registration provides for the following checklist to determine whether one is a controller or processor;

Table 2. A table on distinct roles of a Data controller and a Data Processor

Are you a Data Controller? Yes if	Are you a Data Processor? Yes if
You decide to collect or process Personal Data.	You have a contract to handle Personal Data on behalf of another Entity.
You decide what the purpose or outcome of the Processing was to be.	You are following instructions from someone else regarding the Processing of Personal Data.
You decide what Personal Data should be collected.	You do not decide to collect Personal Data from individuals.
You decide which individuals to collect Personal Data about.	You do not decide what Personal Data should be collected from individuals.
You obtain a commercial gain or other benefit from the Processing, except for any payment for services from another controller	You do not decide the lawful basis for the use of that data.
You are Processing the Personal Data as a result of a contract between you and the Data Subject.	You do not decide what purpose or purposes the data will be used for.

The Data Subjects are your employees.	You do not decide whether to disclose the data, or to whom.
You make decisions about the individuals concerned as part of or as a result of the Processing.	You do not decide how long to retain the data.
You exercise professional judgement in the Processing of Personal Data.	You may make some decisions on how data is processed but implement these decisions under a contract with another Entity.
You have a direct relationship with the Data Subjects.	
You have complete autonomy as to how Personal Data is processed.	
You have appointed the processors to process the Personal Data on your behalf.	

The main difference is that a controller is an entity which makes the decision to collect the personal data and further decides the purpose of collection. The data processor is an entity contracted by a controller which processes personal data under the instructions of a data controller. If a CSO is both a controller and a processor, they will be required to register twice under two separate applications and will be billed per application.

The process of registration is done online via the ODPC registration portal, and this process will require the following;

- Personal details of the organization's representative
- Basic details of the organization; name, postal address, county, phone number
- Establishment document of the organization; registration certificate
- Details of categories of personal data processed by the Organization
- List of sensitive personal data processed by the organization and the reasons for process; where applicable
- Countries where personal data is transferred outside of Kenya if applicable.
- List of risks and safeguards for personal data protection

A strong application for registration is exhaustive and comprehensive in listing the risks and safeguards for personal data protection.

Mandatory Registration

CSOs processing personal data for the activities listed below must register with the ODPC:

1. Education
2. Health administration and provision of patient care

Filing Complaints with the Office of the Data Protection Commissioner (ODPC) Provided for under Section 56 of the DPA where a data subject who is aggrieved by a decision of any person which violates any provision under the Act, may lodge a complaint with the Data Commissioner. This may be done online via the complaint's portal on the ODPC's website.

A data subject is a natural person whereas a CSO is a legal person. This means that a CSO cannot lodge a complaint, however a complaint can be lodged by an employee of the organisation as a data subject.

The reasoning is that only data subjects (as natural persons) under the DPA are afforded protection of their privacy rights, an organisation as a legal person is not a data subject under the DPA and therefore does not enjoy the rights, protections and freedoms under the Act.

On receipt of a complaint the ODPC initiate the investigations and it has the power to; summon any person or produce any document/ or any article relevant to the investigation. Further, in the process of investigation, the ODPC can order any person to provide a statement in writing or a sworn statement setting out any relevant information to the investigation. Section 56 (5) requires the ODPC to conclude investigations within 90 days.

Format of a Complaint

A complaint lodged with the ODPC can be made orally at their offices, in writing, or through any appropriate electronic means such as email, or through the complaint's portal on the ODPC's website. The complaint may be lodged by the complainant in person, or by a person who is duly authorised to act on behalf of the complainant; or a complaint can also be lodged anonymously.

Enforcement Notices

Upon completion of investigations, the ODPC must make a finding as to whether there was indeed a failure to comply with the provisions of the DPA. Where the ODPC is satisfied that there was a violation of the DPA, the Data Commissioner may serve an Enforcement Notice on the perpetrator requiring them to stop the violation and to take certain measures to remedy the violation. The purpose of an Enforcement Notice as provided for under the DPA is to propose corrective

measures allowing an accused party who has been deemed to have violated the Act towards the desired compliance with the Act.

Section 58 of the DPA further provides that any person who fails to comply with an Enforcement Notice commits an offence and can face fines of up to KES 5 million or 1% of their turnover, whichever is lower.

In the Roma School Uthiru case, the ODPC received a complaint from a parent who was concerned about the school's use of her child's image. The ODPC completed investigations and deemed that the school was in violation of the DPA and issued an enforcement notice, which was ignored by the school. This resulted in the ODPC issuing the school a fine of KES. 4.5 Million, which at the time was the highest fine ever issued by the ODPC.

An Enforcement Notice is deemed to have been received once it is properly delivered or posted to the correct address of any organisation. Whether or not the organisation has read the Enforcement Notice is immaterial; delivery alone will mean that the offending party has received the notice.

Fines & Penalties

Section 62 of the DPA provides that- where the ODPC finds that an offending party who was duly issued an Enforcement Notice has failed to comply, the ODPC has the powers to fine the offending party. The ODPC will issue a Penalty Notice requiring the offending party to pay the ODPC a specific amount in fines. The maximum amount the ODPC can impose on an offending party under Section 63 of DPA is KES.5Million.

In addition to fines, the ODPC has the power to order an offending party to pay compensation for damage suffered by the complainant. Section 65 of the DPA provides that any person who suffers damage due to a violation of the Act is entitled to compensation for that damage from the data controller or processor. This section further provides that the term damage includes financial loss as well as damage not including financial loss such as distress. To avoid liability for damages, the offending party would have to prove that they are not at all responsible for the resulting damage and violation of the DPA.

The Right to Appeal

Section 64 of the DPA provides that an offending party who disagrees with either an Enforcement Notice or a Penalty Notice issued by the ODPC can find recourse by appealing to the High Court for judicial review of the decision.

SETTING UP A PRIVACY PROGRAM

Establishing a privacy program is essential for organisationCSOss to safeguard the personal data they handle, meet their compliance obligations under the DPA, and ensure that the rights of a data subject are not violated. A well-structured privacy program not only ensures compliance with legal obligations but also enhances public trust and organizational credibility. The essence of the privacy program within an organization is to embed good data governance and privacy principles.

To set up a privacy program the civil society may follow the steps below;

i) Assess organisational data needs through a Data Map or Analysis or update data protection policies and proceduresorganisational obligations, data subject onsent managementretention and disposalImplement technical and organizational data protection controls and measures.

ii) Periodically review data privacy performance.

iii) Train staff on data protection.

Given the sensitive nature of data entrusted to CSOs and public benefit organisations, these entities must establish robust frameworks and structures to govern the collection, storage, and processing of such data. Establishing proper structures ensures CSO & PBO compliance with relevant legal standards, including the Data Protection Act, as covered in part 3 of these guidelines, while fostering trust and upholding ethical responsibility within their operations.

Institutionalized data protection frameworks provide demonstrable evidence that personal data is being processed in accordance with the requirements of the Data Protection Act (DPA). Such frameworks not only reinforce the organisation's commitment to compliance but also significantly mitigate the risk of infringing upon the data protection principles and the rights of data subjects. This can therefore mitigate against or reduce the number of complaints filed before ODPC.

Data Map / Data Analysis

A data map or data analysis is a systematic exercise that involves identifying, categorizing, and documenting the flow of data within an organization. It serves as a critical tool in understanding the data landscape of an organization by outlining where data originates, how it is processed, stored, and shared, and where it ultimately ends up. A data map can accurately help assess an organisation's data landscape by tracking the flow of data in an organisation.

It also helps identify high-risk processing activities that may pose privacy concerns, enabling the organization to take proactive measures to mitigate these risks. Further, data maps can inform the development of data protection policies by highlighting areas where data handling practices may be weak or non-compliant. Identifying these gaps is crucial for improving data security and ensuring that all personal data is adequately protected throughout its lifecycle. This allows

organizations to create targeted policies that address specific vulnerabilities, ensuring robust data protection practices are in place.

A good data map will indicate the following across a simple spreadsheet;

a. **Source of data:** This indicates where the data originates, such as from the Controller, Data Subject, or Processor.
b. **Categories of personal data:** Examples include Employment Details (such as bank account details, next of kin details, annual appraisals, education certificates, and annual leave).
c. **Purpose of processing:** This category outlines why the data is being processed, e.g., Administration, Processing employee benefits, Recordkeeping, Invoicing, and Marketing.
d. **Lawful basis for processing:** This includes legal justifications such as consent, contract, legal obligation, and vital interest.
e. **Condition for processing sensitive personal data:** This includes the conditions under Section 45 of the DPA such as legitimate activities of the organisation, publicly available data, and legal claims.
f. **Storage locations:** This specifies where the personal data is stored, such as Cabinet Files, CRM Systems, or Finance Payroll Systems.
g. **Data retention schedule:** This indicates how long the data is retained, for example, 6 months post-recruitment or 6 years post-employment
h. **Transfer of data outside of Kenya:** Lists the countries or regions where data may be transferred, such as Europe, India, or Ireland.

A data map can be accurately documented on spreadsheet applications such as Microsoft Excel or Google Sheets and periodically updated.
Develop Data Protection Policies & Notices

Protection Policies

A privacy policy is an inward facing legal document that outlines how an organization collects, uses, discloses, and protects personal data. A comprehensive privacy policy is essential for CSOs in Kenya to protect data subject rights and ensure compliance with the Data Protection Act, 2019. The privacy policy comprises of the internal rules which govern the way data is handled within an organization, and all people under the organization are subject to abide by the policy. It directs employees on data protection practices and ensures compliance with legal obligations. It is mainly used by the organization itself to manage and safeguard personal data in accordance with laws and regulations.

According to Regulation 23 of the Data Protection (General) Regulations, a CSO as either a data controller or processor is obligated to develop, publish and regularly update a privacy policy reflecting the way the organization handles personal data. Regulation 23 (2) provides that a privacy policy should include;

(a) the nature of personal data collected and held;

(b) how a data subject may access their personal data and;

(c) complaints handling mechanisms;

(d) lawful purpose for processing personal data;

(e) obligations or requirements where personal data is to be transferred outside the country, to third parties, or other data controllers or data processors located outside Kenya and where possible, specify such recipients;

(f) the retention period and schedule contemplated under regulation 19; and

(g) the collection of personal data from children, and the criteria to be applied.

CSOs should be encouraged to develop additional guidelines which will explain and explore data handling procedures within the organization.

Privacy Notice

The privacy notice can be differentiated from the privacy policy in the sense that a privacy notice is 'out-ward' facing while a privacy policy is 'in-ward' facing. The key difference lies in their audience and purpose: the privacy policy is for internal use, while the privacy notice is for public disclosure

A privacy notice is a public-facing document intended to inform individuals (such as beneficiaries, training participants, partners, rights holders or website visitors) about how their data is collected, used, and protected. It details the rights of data subjects and the purposes for data processing, serving as a transparency tool to ensure individuals understand how their information is handled. The privacy notice is essentially a summary of the privacy policy for the benefit of informing individuals who interact with the organization.

A privacy notice may be published on a website or put up as a physical notice at the office, and should include the following;

a. the rights of a data subject specified under section 26 of the DPA.

b. the fact that personal data is being collected.

c. the purpose for which the personal data is being collected.

d. the third parties whom personal data has been or will be transferred to, including details of safeguards adopted

e. the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data.

f. a description of the technical and organisational security measures taken to ensure the integrity and confidentiality of the data.

g. the data being collected pursuant to any law and whether such collection is voluntary or mandatory.

h. the consequences if any, where the data subject fails to provide all or any part of the legally required data

C. Regular data protection training and awareness for staff
Civil Society Organizations (CSOs) should institute regular training programs for their staff, volunteers, agents, and partners on data protection. These trainings are essential to ensure that all individuals involved understand the types of data they handle, the legal frameworks governing data processing, and the appropriate measures to implement for maintaining data security. Furthermore, staff should be equipped with the necessary knowledge to identify, respond to, and report suspected data breaches in a timely and effective manner. To maintain a high standard of compliance and awareness, such training should be conducted on a continuous and periodic basis.

D. Procure the services of DPO
According to Section 24 of the DPA, a data protection officer (DPO) is a designated individual responsible for ensuring that an organization complies with the provisions of the Act regarding the processing and protection of personal data. A DPO may be a staff member within an organization tasked with overseeing the data protection strategy and its implementation to ensure compliance with data protection laws and regulations. Further, the Act allows a group of organizations to come together and appoint a single DPO who will serve them.

The Data Protection Act specifies that a DPO should have expert knowledge of data protection laws and practices. While the Act does not explicitly outline the qualifications, it implies that the DPO should possess a strong understanding of the legal, technical, and organizational aspects of data protection. Relevant qualifications might include experience in law, information security, or data management.

Section 24 (7) specifies the role of a DPO as follows;

(a) advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law;

(b) ensure on behalf of the data controller or data processor that this Act is complied with;

(c) facilitate capacity building of staff involved in data processing operations;

(d) provide advice on data protection impact assessment; and

(e) co-operate with the Data Commissioner and any other authority on matters relating to data protection

It is imperative to note that the appointment of a DPO is not mandatory for CSOs but is encouraged where an organisation deals with large volumes of personal or sensitive personal data

E. Design Data Management protocols
Data management refers to the practices which organizations implement to ensure the proper handling of data. This includes its collection, storage, processing, sharing, and deletion. For CSOs , effective data management is critical for maintaining data integrity, security, and accessibility, particularly in compliance with the DPA.

These protocal can be incorporated as a policy at the policy development stage. Here are some of the considerations for data management:

The Data Lifecycle

The data lifecycle represents the stages that data undergoes from its creation to its eventual disposal. For CSOsin Kenya, understanding and managing this lifecycle is essential to ensure compliance with the Data Protection Act and to protect the rights of individuals whose data is being processed.The data lifecycle for CSOs under Kenya's DPA involves the following key stages:

Data Collection:
This is the first stage, where personal data is gathered from various sources. The DPA mandates that this data be collected lawfully, fairly and in a transparent manner . Organizations must ensure that the data collected is necessary and relevant to the purpose for which it is being gathered.
Data Storage: Once collected, the data must be securely stored. The Act requires organizations to implement appropriate safeguards to protect personal data from unauthorized access, loss, or destruction. This includes both physical and digital security measures

Data Processing:
In this stage, the collected data is used to achieve specific organizational goals, such as advocacy, research, or service delivery. Processing must be done in compliance with the legal requirements, ensuring that the data is only used for the purposes it was collected for.

Data Sharing:
If data needs to be shared with third parties, such as partners or donors, CSOs must ensure that this is done in a manner that respects the privacy of data subjects and complies with the Data Protection Act. This often requires obtaining additional consent from the data subjects.

Data Retention:
CSOs must establish clear policies on how long personal data will be retained. The Data Protection Act mandates that data should not be kept longer than necessary for the purposes for which it was collected. Once data is no longer needed, it should be securely deleted.

Data Disposal:
The final stage involves the secure disposal or deletion of data that is no longer required. This ensures that the data is permanently removed and cannot be accessed or recovered, thus preventing any potential data breaches.

By following these stages, CSOs can effectively manage the data lifecycle and ensure compliance with Kenya's Data Protection Act, safeguarding the privacy and rights of individuals whose data they handle.This lifecycle is crucial for organizations to manage data responsibly and ensure compliance with data protection laws. Properly managing this lifecycle helps protect data subject rights

by ensuring that personal data is only retained as long as necessary. Section 39, the DPA obligates CSOs to retain data only for the period required to fulfill the purpose of its collection. Once the data is no longer needed, it must be securely disposed of to prevent unauthorized access and data misuse which would occasion a violation of the DPA and data subject rights.

Vendor assessment and management

Implementing these strategies demonstrates a culture of compliance, which can significantly shield organizations from legal and reputational damage when facing complaints with the ODPC.

Poor data governance frameworks will expose a CSO to significant reputational or legal risks, which could in turn negatively affect the organisation's finances. The risks associated with collection, processing, storing and transferring personal data are not abstract or far-fetched. CSOs that are lax or negligent with how they handle and process personal data, subject themselves to a reputational risk, which could result in media or internet exposés. Furthermore, in the long run, if an organisation is found to have mishandled personal data, it will likely experience diminished trust among donors, partners, and beneficiaries, ultimately affecting its overall longevity and future. Additionally, there is the financial risk of having to meet fines or defend legal action.

TECHNICAL & ORGANISATIONAL MEASURES TO MITIGATE DATA PROTECTION RISKS

Technical measures and organizational measures are two key categories of safeguards implemented to protect personal data within an organization.

Technical measures refer to physical and digital tools or procedures designed to protect data from unauthorized access, loss, or damage. Such as; encryption, firewalls, pseudonymisation, anti-virus software etc. Organisational measures refer to policies, practices, and procedures that an organisation adopts to ensure proper data management and compliance with legal requirements. These can include, employee trainings, data protection or privacy policies and notices, access control policies etc. In summary, while technical measures focus on the tools and systems used to protect data, organisational measures focus on the strategies and processes that guide data protection efforts within an organisation.

The Data Protection Act of Kenya requires organizations to implement both technical and organizational measures to mitigate data protection risks. Further, when registering with the ODPC as either a controller or processor, one must declare the existing risks and the technical or organisational measures to mitigate that risk.

For example:
Table 3. A table on Technical and organizational measures

Data Protection Risk	Technical Measure	Organizational Measure
Data Breach	Implementing encryption for all personal and sensitive data	Regular employee training on data protection and best practices
Unauthorized Access	Installing firewalls and intrusion detection systems	Implementing strict access control policies
Data Loss	Regular backups with secure storage solutions	Developing and enforcing a data retention and backup policy
Phishing Attacks	Implementing anti-phishing email filters	Conducting awareness programs on recognising phishing scams
Insider Threats	Deploying monitoring software to track data access	Conducting regular audits and role-based access reviews
Malware and Ransomware Attacks	Installing and updating anti-malware software	Developing a comprehensive incident response plan


AMNESTY
INTERNATIONAL

Amnesty International Kenya
Ground Floor,197 Lenana Place
Lenana Road, Kilimani
P.O Box 1527-00606
Nairobi, Kenya

AmnestyKenya

amnesty_kenya

Amnesty International Kenya