DATA PROTECTION MANUAL FOR NON-PROFIT ORGANISATIONS IN KENYA

A Practical Toolkit for Managing Privacy Within Your Non-Profit Organisation

1ST EDITION 2026

dpo 360 | ICN DATA AND LEARNING | KENYA AMNESTY INTERNATIONAL

DATA PROTECTION MANUAL FOR NON-PROFIT ORGANISATIONS IN KENYA

A Practical Toolkit for Managing Privacy Within Your Non-Profit Organisation

1ST EDITION 2026

dpo 360 | ICN DATA AND LEARNING | KENYA AMNESTY INTERNATIONAL

TABLE OF CONTENTS

PREFACE

This book was conceived out of recognition that there remains a need for accessible, practical, and authoritative guidance on the subject of data protection. The purpose of this book is to provide non-profit organizations in Kenya with a practical framework for managing privacy and to bridge the gap between legal theory and real-world application. Data protection is of critical importance to non-profit organizations because the sector is built on relationships of trust with communities and vulnerable beneficiaries; handling their personal information responsibly is inseparable from ethical, accountable, and people-centred practice. This book is a proud initiative of Amnesty International Kenya, developed following years of supporting non-profit organizations to successfully comply with the Data Protection Act and safeguard the dignity, autonomy, and safety of the individuals they serve.

ACKNOWLEDGEMENT

The creation of this first edition of the toolkit has been a collaborative journey, and we wish to extend our deepest gratitude to everyone The creation of this first edition of the toolkit has been a collaborative journey, and we wish to extend our deepest gratitude to everyone who made it possible. We acknowledge and thank the authors Victor Ndede, Aurelia Miheso, Danford Momanyi, Philip Kisaka, Teresia Wanjiku, Zeddy Misiga, and Mary Angela Odhiambo for their vision, invaluable expertise, dedication, and tireless efforts over the last 9 months that have brought this project to fruition. Finally, we thank DPO 360 Africa Limited and ICON Data and Learning Labs for their seamless collaboration with Amnesty International Kenya to develop this essential resource for the non-profit sector in Kenya.

First Published September 2026
197 Lenana Place, Lenana Road
P.O. Box 1527-00606 Nairobi, Kenya
Tel: +254 020 – 4283000
Email: amnestykenya@amnesty.org
www.amnestykenya.org

ABOUT THE AUTHORS

Amnesty International Kenya

A leading human rights non-governmental organization in Kenya championing the promotion and protection of fundamental rights and freedoms. Since 2020, Amnesty Kenya has worked extensively to strengthen data governance across Kenya and East Africa. Through this work, the organization has supported non-profits across Kenya's 47 counties with data protection capacity-building training and technical support. In 2025, Amnesty Kenya co-published with DPGSK the Data Protection Guidelines for Civil Society Organisations (CSOs) in Kenya to support the non-profit sector in understanding and complying with the Data Protection Act, 2019.

DPO 360 Africa Limited

A specialised privacy, data protection and data governance consultancy supporting organisations across Africa to build practical and sustainable privacy programmes. The firm provides expert advisory, regulatory compliance support, privacy governance, risk management, policy development, training and practical privacy management solutions, helping institutions embed responsible data handling into their day-to-day operations and align with applicable data protection laws and recognised best practices. Learn More at www.dpo360.africa

ICON Data and Learning Labs (IDL)

A Kenya-based non-profit whose vision is promoting data-driven community transformation for sustainable development. IDL works with young people and grassroots organizations in the Lake Region to build capacity, governance, and public-interest technology innovations that puts communities in control of their own data. Through its Ijue Data Yako Initiative, IDL helps grassroots organizations move beyond registration with Kenya's Office of the Data Protection Commissioner (ODPC) toward genuine, operational compliance with the Data Protection Act (2019). They've equipped over 100 non-profits in the lake region of Kenya with practical, actionable steps for safeguarding the personal data entrusted to them by the communities they serve.

LIST OF ABBREVIATIONS

AU	African Union
BCRs	Binding Corporate Rules
CBO	Community Based Organisation
CBPR	Cross Border Privacy Rules
CII	Critical Information Infrastructure
CRM	Customer Relationship Management
DPA	Data Protection Act
DPGR	Data Protection (General) Regulations
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Data Sharing Agreement
DSR	Data Subject Request
EAC	East African Community
EEA	European Economic Area
EMR	Electronic Medical Records
EU	European Union
GBV	Gender-Based Violence
GDPR	General Data Protection Regulation
GPS	Global Positioning System
IaaS	Infrastructure as a Service
ICCPR	International Covenant on Civil and Political Rights
IDPs	Internally Displaced Persons
KES	Kenya Shillings
M&E	Monitoring and Evaluation
NGO	Non-Governmental Organisation
NIIMS	National Integrated Identity Management System
ODPC	Office of the Data Protection Commissioner
PaaS	Platform as a Service
PIA	Privacy Impact Assessment
RDPA	Reciprocal Data Protection Agreement
ROPA	Record of Processing Activities
SaaS	Software as a Service
SCCs	Standard Contractual Clauses
TIA	Transfer Impact Assessment
UDHR	Universal Declaration of Human Rights
WASH	Water, Sanitation and Hygiene

01.
Introduction to Privacy

About This Module

This module establishes the conceptual and practical foundation for understanding privacy within organizational and community-facing work. It is designed to begin not from legal doctrine or compliance requirements, but from the everyday experiences, risks, and responsibilities organizations encounter when working with people and handling information about them.

1.1 Introduction

Privacy is not an abstract or purely theoretical concept. It has direct and immediate implications for the dignity, safety, autonomy, and wellbeing of the individuals and communities that civil society organizations serve. Every day, across Kenya and across the continent, practitioners in community-facing organizations make decisions that affect the privacy of others when they collect information from beneficiaries, conduct surveys and assessments, manage case files, share data with partners and donors, take and publish photographs, and use digital communication platforms. Each of these activities creates privacy considerations that require informed, deliberate, and responsible decision-making.

The primary purpose of this module is to re-position privacy from being perceived as a technical or compliance-driven obligation to being understood as a human-centred principle that is inseparable from ethical, accountable, and people-centred practice.

Privacy is about how individuals are respected, protected, and empowered in relation to their personal information, their identities, their activities, their relationships, and their choices.
This module also prepares learners for the more technical and legal content in subsequent modules by introducing key privacy concepts and typologies in accessible terms.

An understanding of what privacy means, why it matters, and how it manifests in everyday organizational activities is the essential foundation for understanding why data protection laws exist, what they require, and how their requirements connect to professional and ethical obligations.

Reflective Practice

In the past week, how many times did your work involve collecting, using, storing, or sharing personal information about another person?

Note your examples. They may include intake forms, attendance registers, photographs, referral documents, case notes, survey responses, or digital communications.
Keep these examples in mind as you work through this module. They will serve as practical reference points for the concepts introduced in each section.

1.2 Objectives

This module has been designed to achieve the following objectives in relation to understanding privacy:

1. To introduce privacy as a human-centred principle rooted in the protection of individual dignity, autonomy, safety, and trust.
2. To identify the different dimensions or typologies of privacy and explain how they arise and intersect in non-profit work.
3. To distinguish privacy from secrecy, and to establish that privacy is about appropriate control, fairness, respect, and protection not the withholding of information.
4. To help participants recognize where privacy considerations and risks arise in routine organizational activities.
5. To introduce a practical privacy risk identification framework that participants can apply in their day-to-day work.
6. To establish that good privacy practice strengthens organizational effectiveness, ethical programming, community trust, and accountability.

1.3 Learning Outcomes

Upon completion of this module, the learner should be able to demonstrate the following competencies:

Outcome	Demonstrated Competence
Define privacy	Articulate privacy in practical, people-centred terms that connect it to the dignity, autonomy, safety, and trust of individuals and communities.
Explain why privacy matters	Link privacy to human dignity, personal autonomy, freedom of expression and association, safety, trust, accountability, and responsible organizational practice.
Identify types of privacy	Recognize and describe physical, decisional, behavioural, associational, intellectual, and informational privacy and explain how they connect to one another in practice.

Relate privacy to organizational work	Identify specific activities within their organization that generate privacy considerations and articulate why those considerations matter.
Identify common privacy risks	Recognize situations where personal information may be exposed, misused, overshared, inadequately protected, or improperly handled.
Distinguish privacy from secrecy	Explain that privacy is about appropriate control, fairness, respect, and protection not the concealment of information.
Understand privacy and trust	Explain how responsible privacy practices support ethical engagement, safer service delivery, and community confidence.
Apply basic privacy thinking	Use the Privacy Risk Spotter Checklist to identify privacy considerations when collecting, using, storing, or sharing personal information.

1.5 What Is Privacy?

Privacy is a person's ability to exercise appropriate control over access to themselves, their personal information, their physical space, their choices, their activities, their relationships, and their identities. It is not about absolute secrecy. It is about ensuring that information about a person is handled in ways that are fair, respectful, proportionate, and appropriate to the context in which it was shared.

At its core, privacy is a human right. It is recognized in international human rights instruments, in the constitutions of many countries, and in Kenya's Data Protection Act, 2019 as a foundational value underpinning the law. But beyond its legal recognition, privacy is a lived experience. It affects how individuals feel about the organizations they interact with, whether they are willing to share information, whether they trust the people and systems that hold information about them, and whether they feel treated with dignity and respect.

For community facing organizations, privacy matters because the work of the sector is built on relationships of trust with communities, beneficiaries, research participants, and with the broader public. When those relationships are grounded in responsible, respectful handling of personal information, they are stronger, more sustainable, and more effective. Where these considerations are overlooked, the consequences can be significant, including harm to individuals, loss of trust, reputational damage, legal exposure, and the weakening of the ethical principles that buttress the organizations' work.

Privacy is closely connected to several foundational values that are also central to non-profit practice:

Value	Connection to Privacy
Dignity	Privacy ensures that individuals are treated with respect and that their personal experiences, circumstances, or identities are not mishandled, exposed, or exploited, without consent or another relevant legal basis.
Autonomy	Privacy enables individuals to make informed decisions about how their information is collected, used, and shared. It preserves their capacity for self-determination.

Safety	Privacy protects individuals and communities from harm that may arise through disclosure, misuse, surveillance, discrimination, retaliation, or unauthorized access to information.
Trust	Responsible handling of personal information builds and maintains confidence between organizations and the people they engage with, which is a prerequisite for effective community-facing work.
Accountability	Privacy requires organizations to be intentional and transparent about how they handle information, which strengthens governance, ethical practice, and public confidence.
Privacy Risk Assessment	Good privacy practice ensures that programmes and operations do not unintentionally create risks for the individuals and communities they are designed to serve.

It is important to understand that privacy is not about preventing organisations from carrying out their work. Collecting information about the people you serve, conducting research, managing case files, and sharing data with partners are all legitimate and often essential activities.

The real question privacy seeks to answer is not whether these activities should take place, but how they should be undertaken. They must be carried out with appropriate safeguards, ensuring transparency, accountability, proportionality, and respect for individuals' rights. In essence, privacy is about enabling organisations to use personal data responsibly while maintaining the trust and dignity of the people whose information they hold.

Organizational Activity	**The Privacy Consideration It Raises**
A survivor shares details of gender-based violence during case intake	Handling sensitive personal information with respect, confidentiality, and appropriate security safeguards.
A participant shares location information during emergency response registration	Risks of surveillance, tracking, or physical harm if location information is inadequately protected.
A person joins an advocacy, support, or community network	Protection of associational privacy, the right to membership and affiliation without risk of exposure or retaliation.
An individual discloses medical history during health service provision.	Protection of sensitive health information from unauthorized access, disclosure, or misuse.
Staff share photographs of community activities online	The requirements of informed consent, dignity, and the potential for lasting harm from publicly identifying vulnerable individuals.
A registration form collects extensive personal details	The principle of data minimization whereby you collect only what is genuinely necessary for the stated purpose.

Research participants share opinions or experiences during interviews	Confidentiality of participants' views and experiences informed and voluntary participation, protection of personal and sensitive information, and safeguards against re-identification or harm arising from disclosure.
Staff communicate beneficiary details through messaging applications	Risks of unauthorized access, accidental disclosure, or inadequate data security.

Reflective Practice

Using the examples you identified at the start of this module, consider which of the activities in the table above most closely resemble your own organizational activities.

For each example you identified, note what personal information is involved, and what privacy consideration it raises.

You do not need to resolve these considerations now. The purpose of this exercise is to begin seeing privacy in your everyday work.

Privacy and Secrecy - Understanding the Distinction.

Secrecy is the withholding of information. Privacy is the appropriate control of it. These are not the same thing, and the distinction matters profoundly for community facing practitioners.

A secret exists to keep information from others, regardless of context or purpose. Privacy, by contrast, is not concerned with preventing access to information altogether. It is centred on ensuring that information flows appropriately: that it is collected for clear and justified reasons, used only for the purposes for which it was shared, protected from those who have no legitimate interest in it, and handled in ways that respect the dignity and autonomy of the individual to whom it belongs.

Consider a survivor of domestic violence who discloses her experiences to a social worker during a case intake interview. That information is not secret; it has been shared but it is private. The survivor has shared it within a specific relationship, for a specific purpose, with a reasonable expectation that it will be handled with care, used only to support her case, and not disclosed to parties who have no role in her protection. Privacy protects that expectation. Secrecy was never the point.

This distinction carries direct implications for how community facing organisations approach their work. An organisation that conflates privacy with secrecy may conclude that collecting and using personal information is inherently in tension with privacy, and that more open data practices mean less privacy protection, and vice versa. This is mistaken. A community facing organisation can collect detailed personal information from the communities it serves, maintain comprehensive case files, share data with referral partners, and report to donors and do all of these in full compliance with privacy principles, provided it

does so transparently, proportionately, with appropriate justification, and with genuine respect for the rights of the individuals concerned.

Privacy does not require that information never be gathered or shared. It requires that when information is gathered and shared, it is done with fairness, accountability, and respect for the reasonable expectations of the person whose information it is.

Privacy as a Fundamental Right

Privacy is not merely a professional standard or an organisational preference. It is a fundamental human right, recognised in international instruments including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the African Charter on Human and Peoples' Rights, as well as in the Constitution of Kenya, 2010 under Article 31, which provides that every person has the right to privacy.

Understanding privacy as a human right carries significant implications for organizations working in community-facing and non-profit contexts. It means that when organizations handle personal information carelessly, insufficiently, or without appropriate justification, they are not merely making a technical error or incurring a legal risk, they are potentially infringing upon a right that belongs to the individuals whose information they hold.

Privacy as a human right supports several other rights and freedoms that are particularly relevant to the communities served by non-profit organizations such as:

1. The right to human dignity, which requires that individuals are treated with respect and that their personal circumstances are not exposed or exploited.
2. The right to personal autonomy and freedom of decision-making, including decisions about participation, disclosure, and consent.
3. The freedom of association which can be severely compromised if membership in networks, groups, or organizations is disclosed without authorization.
4. The freedom of expression and participation which is undermined when individuals cannot engage with organizations, ideas, or communities without fear of surveillance or exposure.
5. The right to safety and protection from harm, including harm arising from discriminatory use of personal information, retaliation, or surveillance.
6. The right to be treated fairly and transparently by organizations that hold information about them.

The human rights dimension of privacy is especially significant in non-profit work as many of the individuals served by organizations are already in positions of heightened vulnerability. Displaced persons, survivors of violence, individuals living with stigmatized health conditions, members of marginalized communities, human rights defenders, and persons in conflict with the law are among those for whom privacy violations carry the most serious consequences. These consequences include physical danger, discrimination, social exclusion, and psychological harm.

Privacy Violations and Their Consequences

Poor privacy practices can expose individuals and communities to significant harm. These harms are not hypothetical. They arise from real operational failures in organizations that handle personal information without adequate care.

Discrimination: personal information relating to health status, political opinion, religious belief, sexual orientation, or ethnic identity may be used to discriminate against individuals in employment, service access, or social participation.

Stigma: disclosure of health conditions, family circumstances, or participation in support programmes may expose individuals to social stigma and exclusion.

Retaliation: advocacy participation, membership in networks, or engagement with justice processes may expose individuals to retaliation if records are inadequately protected.

Physical harm: location information, shelter details, or contact information relating to displaced persons, survivors, or individuals in conflict situations may create direct physical safety risks.
Loss of trust: breaches of privacy, however unintentional, can fundamentally undermine the trust between an organization and the community it serves with lasting consequences for programme effectiveness and community confidence.

Privacy in the Modern Organizational Environment

The challenges of privacy in organizational practice have become more complex and more urgent as organizations increasingly rely on digital systems, online platforms, mobile devices, cloud services, and data-driven processes. Information that was once contained in locked filing cabinets and accessible to a small number of staff can now be stored in cloud systems accessible from multiple devices, transmitted instantaneously across platforms and national boundaries, and duplicated many times without any visible trace.

This does not mean that digital tools and platforms should be avoided. They offer significant operational benefits, including improved data quality, faster communication, and more effective coordination. However, their use requires intentionality and awareness of the privacy risks they introduce. An organization that adopts digital tools without a corresponding commitment to responsible data practices may find that its operational efficiency comes at the cost of the safety and trust of the communities it serves.
The following table identifies common practices in modern community facing operations and the privacy risks they may introduce:

Modern Practice	Potential Privacy Risk
WhatsApp groups and messaging platforms for team communication	Accidental disclosure of beneficiary contacts, uncontrolled screenshot sharing, or exposure of sensitive conversations to unintended recipients.
Online registration forms for programme intake or event management	Collection of excessive or unnecessary personal information; inadequate data security on hosting platforms.
Cloud storage systems for organizational files	Unauthorized access due to weak access controls, data leaks, or lack of understanding of what third-party platform providers do with stored data.
Biometric registration or identity verification systems	Processing highly sensitive personal data with limited understanding of storage, access, and retention implications.
Social media posts and storytelling campaigns featuring community members	Exposure of individuals without informed consent; permanent digital presence of potentially identifying images.
Sharing beneficiary or programme data with partner organizations	Loss of control over how information is subsequently used, shared, or protected by partner organizations.
Online surveys and research data collection tools	Insecure collection or storage of responses; third-party access to raw data; inadequate informed consent processes.
Use of personal mobile devices for work-related communication	Increased risk of data loss, theft, or unauthorized access to work-related personal information.
Email communication containing personal data	Misrouting, unintended recipients, inadequate encryption, or forwarding to unauthorized parties.
Digital attendance or tracking systems	Systematic collection of behavioural information without participants full understanding of how it will be used.

A critical insight for practitioners is that privacy risks in the modern organizational environment frequently arise not from deliberate wrongdoing but from habitual or unconsidered practices. The staff member who sends a list of beneficiaries via WhatsApp for convenience, the programme officer who photographs community members without a formal consent process, and the administrator who retains old case files indefinitely without a disposal policy are not acting with malicious intent. They are acting without adequate awareness of the privacy implications of their actions and without institutional systems to guide better practice.

This is precisely why privacy education and awareness are essential. The goal is not to create fear or to paralyze operations, but to build a culture of informed, intentional, and responsible information handling that becomes embedded in everyday practice.

Typologies of Privacy

Privacy is multidimensional. It encompasses several distinct but closely interrelated dimensions that together describe the full range of a person's interest in controlling access to themselves and their information.

Understanding these dimensions enables the learner to recognize privacy considerations across the full breadth of their organizational activities, not only those involving obvious data collection processes, but also those involving physical space, research engagement, community relationships, and digital interaction. The following table describes the principal typologies of privacy and illustrates how each connects to informational privacy in practical non-profit and community-facing contexts:

Type of Privacy	Meaning	How It Connects to Organisational Practice	Practical Example
Physical Privacy	Protection of a person's body, personal space, and physical integrity.	Information about a person's body, health condition, disability, physical appearance, or location may be collected, recorded, or transmitted as part of organizational activities.	Conducting private intake interviews, managing health-related records, or sharing location information during emergency response coordination.
Decisional Privacy	The freedom to make personal choices without interference, coercion, or pressure.	Decisions individuals make about participation, consent, disclosure, or engagement may be documented and may be compromised where individuals are not given genuine free choice.	Choosing whether to participate in a programme, survey, research activity, or community initiative.
Behavioural Privacy	Protection from monitoring, tracking, or observation of a person's activities and patterns.	Monitoring and tracking activities may generate data revealing habits, movements, preferences, patterns of participation, or associational networks.	Tracking attendance records, monitoring online activity, or analysing participation trends across multiple programmes.
Associational Privacy	Protection of a person's relationships, memberships, affiliations, and social connections.	Records identifying organizational memberships, advocacy affiliations, network participation, or social relationships may expose individuals to risk if inadequately protected.	Membership in a survivors' support group, an advocacy network, or a community organization.

Intellectual Privacy	Freedom of thought, belief, inquiry, learning, and access to ideas without surveillance or interference.	Information about what individuals believe, research, discuss, or engage with, may be captured through organizational systems, research activities, or digital platforms.	Research participation, workshop engagement, training records, or access to organizational resources and ideas.
Informational Privacy	The protection and appropriate control over personal information relating to all aspects of a person's life.	Informational privacy is the practical dimension through which data about a person's body, decisions, behaviour, relationships, beliefs, and activities is collected, used, stored, shared, and protected in organizational settings.	Records, databases, surveys, case management systems, digital communications, and all organizational files containing personal information.

A critical insight in understanding privacy typologies is that they rarely arise in isolation. In practice, a single organizational activity may implicate several forms of privacy simultaneously. Consider the following examples:

1. A beneficiary registration form may involve informational privacy (through the data collected), decisional privacy (through the consent process), and associational privacy (through records of programme participation).
2. A photograph taken at a community event and published on social media may implicate physical privacy (through identifiable images), informational privacy (through public identification), and potentially associational privacy (through identification of community membership).
3. Monitoring programme participation patterns may implicate behavioural privacy and associational privacy, as well as informational privacy through the records generated.
4. Collecting medical information during health service delivery may implicate physical privacy and informational privacy simultaneously, with significant consequences for the individual's safety and dignity if inadequately protected.

This multidimensional character of privacy is particularly important for community facing learners as they need to understand this, due to the potential impact of any given decision on what information to collect, how to store it, with whom to share it, may be broader than it initially appears.

Responsible privacy practice requires seeing beyond the immediate visible activity to the full range of interests and risks that it may affect.

Informational Privacy as the Operational Hub

Community-facing organisations primarily interact with people's personal information. Decisions about that information can influence not only informational privacy, but also other aspects of privacy, such as bodily privacy, psychological privacy, social privacy, and autonomy. As a result, informational privacy is often the main route through which privacy risks arise in practice.

As organisations increasingly interact with individuals through information and data-processing activities, the way they handle personal information directly affects not only confidentiality but also safety, autonomy, participation, dignity, and trust.

Poor handling of personal information can therefore affect multiple dimensions of a person's privacy simultaneously, with consequences that extend well beyond the immediate data protection concern.

Reflective Practice

Select one programme or organizational activity in your organization that involves collecting or using personal information.

Working through the six typologies in the table above, identify which forms of privacy are implicated by that activity.

Are any of the individuals involved particularly vulnerable in ways that increase the potential impact of a privacy violation?

This exercise will be developed further in the assessment section of this module.

1.8 Key Takeaways

KEY TAKEAWAYS

1. Privacy is a value, not a formality - Privacy is not a box to tick before a project begins. It is a human-centred value rooted in dignity, autonomy, safety, and trust, and it shapes how you engage with the communities your organisation serves, not just how you fill in a form.
2. Privacy risk hides in ordinary practice - Privacy risk rarely announces itself as a dramatic breach. It surfaces quietly in everyday activities such as a fundraising photograph, a WhatsApp referral, or an advocacy register, making everyday vigilance more important than periodic audits.
3. The six typologies of privacy give you the language to name risks that would otherwise go unrecognised. Once you can name a risk, you can act on it.
4. Privacy protects your mission, not just your compliance record - A privacy-conscious organisation earns and keeps the trust of the people it serves. That trust is the foundation on which every programme, partnership, and intervention depends.

1.9 Assessment

Part A: Knowledge and conceptual understanding

1. Define privacy in your own words. How does your definition connect privacy to dignity, autonomy, safety, and trust?
2. Explain why privacy is described as a human right. What international and Kenyan legal instruments recognize privacy as a right?
3. What is the difference between privacy and secrecy? Why is this distinction important for non-profit practitioners?
4. Name and describe the typologies of privacy introduced in this module. For each one, give an example from non-profit or community-facing work.
5. How does good privacy practice strengthen organizational effectiveness?

Part B: Applied analysis

1. A community health organization conducts home visits to provide nutritional support to children under five. During visits, health workers collect the names, ages, and health status of all household members, including adults. Identify the types of privacy implicated and the risks that may arise if this information is inadequately protected.
2. A human rights organization maintains a list of individuals who have participated in advocacy training activities. It stores this list in an unprotected shared drive accessible to all staff and volunteers. Identify the specific privacy concerns raised by this practice.

Part C: Organizational reflection

1. Identify one activity in your organization that involves handling personal information about community members or beneficiaries. Conduct a risk identification exercise for that activity and document your findings.
2. Does your organization have any existing policies, processes, or practices that address privacy or data protection? What are the most significant gaps you have identified after completing this module?

02.
Informational Privacy and Data Protection

About This Module

This module builds on Module 1: Introduction to Privacy. It moves from the conceptual understanding of privacy as a human-centred principle into the more practical and operational area of personal data protection.

2.1. Introduction

Non-Profit work is increasingly data driven. Whether delivering community programmes, conducting research, undertaking advocacy, managing humanitarian responses, providing legal aid, or administering organisational operations, non-profit organisations routinely interact with individuals through the collection, use, and management of personal information. The quality and integrity of that interaction, its fairness, its proportionality, and its accountability is what data protection law and practice seeks to ensure.

Module 1 established that privacy is a fundamental human right, grounded in dignity, autonomy, safety, and trust. This module takes that foundation and builds a practical operational framework upon it. It introduces learners to the specific categories of information that attract data protection obligations, the principles governing responsible data handling, the lifecycle through which personal data moves within organisational systems, and the responsibilities that organisations carry as custodians of information about the people they serve.

A central insight of this module is that not all information carries the same level of risk. Some information may appear relatively harmless in isolation, yet it becomes significantly sensitive when combined with other data points, shared more widely than intended, or linked to individuals in vulnerable circumstances. Understanding these distinctions and developing the practical capacity to act on them is essential for responsible data stewardship in non-profit organisations.

This module also clarifies three concepts that are frequently used interchangeably but carry distinct meanings: privacy, data protection, and data security. Understanding how these concepts relate to one another and where each applies is an important prerequisite for engaging with subsequent modules.

Reflective Practice

Identify one organisational activity that involves the collection, storage, use, or sharing of personal information about community members, beneficiaries.

As you work through this module, apply each concept introduced such as the data categories, the data lifecycle, risk levels etc, to that activity.

By the end of the module, you should be able to describe what personal data is involved, what risks arise, and what safeguards are or should be in place.

2.2. Objectives

This module has been designed to achieve the following objectives in relation to understanding informational privacy:

1. To establish a clear understanding of data as it exists in different forms within modern organisational environments.
2. To define personal data and explain how individuals may be identified directly or indirectly through the information organisations hold.
3. To introduce and explain sensitive personal data and the categories of information that attract heightened legal obligations and ethical responsibilities.
4. To clarify the distinctions between privacy, data protection, and data security, and explain how they relate in practice.
5. To introduce the concept of the data lifecycle, enabling learners to identify where risks and responsibilities arise at each stage of information handling.
6. To develop the capacity for data mapping and the ability to trace how personal data moves through organisational systems and identify the privacy and data protection implications at each point.
7. To emphasize intentional, proportionate, and accountable decision-making about data collection, use, sharing, retention, and disposal.

2.3. Learning Outcomes

Outcome	Demonstrated Competence
Define data	Describe data in both its physical and digital forms and recognize the range of formats in which personal information may exist within organizational environments.
Identify personal data	Recognize information that directly or indirectly identifies an individual, including indirect identifiers that may become identifying when combined with other data.

Identify sensitive personal data	Name the categories of information that attract heightened legal obligations, explain why they carry elevated risk, and identify examples relevant to non-profit practice.
Distinguish privacy, data protection, and data security	Explain how the three concepts differ, how they relate to one another, and why technical security measures alone do not constitute adequate data protection.
Recognise data protection risks	Identify situations in which poor data handling may expose individuals, communities, or organisations to harm.
Understand the data lifecycle	Describe the stages through which personal data moves within organizational systems, from collection to disposal, and identify the specific responsibilities at each stage.
Map data within organizational activities	Trace how personal data enters, moves through, and exits an identified organizational process, using the basic data mapping template. Identify situations in which organizations may be collecting excessive or unnecessary information and explain why minimization is both a legal requirement and an ethical obligation.
Identify organizational data responsibilities	Explain the importance of access control, responsible sharing, accountability, and secure handling in non-profit data management.
Connect data practice to trust and accountability	Articulate how responsible data handling supports ethical engagement, safer operations, and the confidence of communities in the organisations that serve them.

2.4. Privacy, Data Protection, and Data Security - Understanding the Distinctions

These three terms are frequently used interchangeably in discussions about responsible information privacy, data protection, and data security but they describe distinct concepts with different scopes, implications, and responsibilities. Understanding these distinctions is essential for practitioners who need to navigate both ethical obligations and legal requirements in their data management practices.

Concept	Definition	What It Addresses	Non-profit example
Privacy	The right of individuals to exercise appropriate control over their personal information, identities, choices, and activities, and to have that information handled with fairness, respect, and proportionality.	How individuals are treated in relation to their personal information, their dignity, autonomy, and right to appropriate control.	Asking a programme participant whether they are comfortable having their photograph used in public communications and respecting their decision.

Data Protection	The legal and procedural framework governing how personal data is collected, used, stored, shared, retained, and disposed of within organizational processes.	The rules and principles that guide how personal data should be collected, used, stored, shared, and protected in a lawful and responsible way. These include using data for a clear purpose, collecting only what is necessary, having a valid reason for processing it, and respecting the rights of the individuals whose data is being used.	Making sure that personal information collected when registering beneficiaries is used only for the purpose it was collected. If the organisation later wants to use it for a different purpose, such as research or sending communications, it must have a separate valid reason or obtain the necessary permission.
Data Security	The security measures taken to protect personal data from unauthorized access, use loss, alteration, theft, destruction, or disclosure.	The safeguards both technical and procedural that are put in place to protect information from unauthorized use, disclosure, loss etc, once it is in the organization's possession.	Password-protecting devices containing personal data, encrypting sensitive files, restricting access to case records to authorized staff only, and maintaining secure physical storage for paper files.

The Critical Relationship Between These Three Concepts

Data security is a necessary but not sufficient component of responsible data practice. An organisation may have strong passwords, encrypted devices, secure servers, and restricted access controls and still be in violation of privacy and data protection obligations if it collects more information than it needs, uses data for purposes individuals did not expect, retains information indefinitely without justification, or fails to provide individuals with adequate information about how their data is handled. Conversely, where an organization is transparent about its use of personal data and only collects what is necessary, individuals may still be exposed to harm if the organization fails to put in place adequate measures to keep that data safe.

Responsible data practices require organizations to respect privacy, follow good data handling practices, and put effective measures in place to protect personal information.

2.5 What Is Data?

Data, in its broadest sense, is any information that has been captured, recorded, or stored in a form that can be retrieved, communicated, or processed.

In the context of organisational work, data encompasses a far wider range of materials than is commonly assumed. It is not limited to databases, spreadsheets, or digital files. It includes any form of recorded information physical or digital through which facts, observations, communications, or records about individuals, events, or activities are captured and held.

Fornon-profit organisations, data may exist in the following forms:

Outcome	Demonstrated Competence
Paper records and physical files	Intake forms, case notes, consent documents, registration sheets, referral letters, complaint records. Example; When a family first seeks assistance, the organization collects basic details such as the name of the beneficiary, contact information, family background, and the type of support needed (for example, food assistance, education support, or medical assistance).
Digital documents and databases	Electronic case management systems, programme databases, spreadsheets, beneficiary registries. Example, A non-profit organization running a youth empowerment programme maintains a digital beneficiary database containing participants' names, ages, education levels, training attendance, skills acquired, and employment outcomes to track programme impact and prepare donor reports.
Audio recordings	Recorded interviews, voice notes, telephone recordings, radio broadcasts captured for monitoring purposes. Example A child protection organization records interviews with community members to document experiences of child protection challenges and use the information to improve awareness programmes and advocacy initiatives.
Video recordings	Filmed interviews, CCTV footage, documentation of community events, and advocacy recordings. Example; A non-profit conducting a community health campaign records videos of health education sessions, community outreach activities, and beneficiary testimonials to demonstrate programme impact to donors and stakeholders.
Photographs and visual materials	Images of community members, programme activities or beneficiaries collected for documentation, communications, or fundraising. Example; A non-profit conducting a community health campaign records videos of health education sessions, community outreach activities, and beneficiary testimonials to demonstrate programme impact to donors and stakeholders (with appropriate consent).

Email and written communications	Correspondence containing personal information about clients, staff, partners, or community members. Example; A beneficiary sends an email to non-profit requesting emergency assistance with information such as their names, contact details, personal circumstances, and supporting documents needed to assess their request.
Messaging platforms and group communications	WhatsApp, Telegram, Slack, Instant Messaging or similar platforms used for team coordination, beneficiary communication, or community engagements. Example; A community-based organization uses a WhatsApp group to coordinate volunteers during a disaster response programme and information collected may include volunteers' phone numbers, locations, updates on affected households, and requests for assistance.
and survey tools	Digital registration forms, feedback surveys, monitoring questionnaires, evaluation tools. Example; A non-profit providing entrepreneurship training uses an online registration form where applicants provide their name, contact details, business information, and training needs before being enrolled into the programme.
Attendance registers and sign-in sheets	Physical or digital records of participation in training, events, community activities, or services. Example; An NGO conducting financial literacy training asks participants to sign an attendance sheet capturing their names, phone numbers, organization/community affiliation, and attendance dates to monitor participation and prepare programme reports.
Cloud storage and shared drives	Platforms such as Google Drive, Dropbox, or OneDrive used to store organisational documents and data. Example; A non-profit stores beneficiary assessment reports, grant applications, monitoring reports, staff records, and project documents on a shared Google Drive accessible to authorised programme staff.
GPS and location-based information	Location data generated by mobile devices, field mapping tools, or tracking systems used in humanitarian or development programming. Example; An organization responding to drought uses GPS-enabled mobile applications to map communities receiving water support and record the locations of water distribution points to ensure resources reach targeted areas.
Biometric systems	Fingerprints, facial recognition data, or iris scans used for identity verification or beneficiary registration. Example; A humanitarian organization providing cash assistance uses fingerprint verification to confirm the identity of registered beneficiaries and reduce duplicate registrations during relief distribution.
Social media activity	Posts, comments, or interactions on social media platforms that capture or reveal personal information. Example; A non-profit running a fundraising campaign collects information from comments and direct messages on its social media pages when individuals request assistance, volunteer opportunities, or information about programmes.

Several important observations follow from this broad understanding of data. First, personal information held by non-profit organisations is not always recognized as data by the staff who hold it. A handwritten case note, a photograph stored on a mobile phone, or a voice note sent over WhatsApp is data and it has data protection implications. Second, the ease with which digital data can be duplicated, forwarded, and shared means that risks can multiply rapidly and unexpectedly once information leaves a controlled environment.

2.6 What Is Personal Data?

Personal data is any information relating to an identified or identifiable natural person. A person is identified where information directly names or singles out that individual. A person is identifiable where information does not directly name them but could, alone or in combination with other data, be used to identify them. The concept of identifiability is broader than most learners initially assume, and it is the source of some of the most significant practical data protection in non-profit work.

The following table distinguishes direct and indirect identifiers and illustrates the range of information that constitutes personal data in organizational contexts:

Direct identifier	Indirect identifier
Full name	Gender, ethnicity, nationality, family relationships, religion (in some cases)
National identification or passport number	Nationality, country of residence, age/date of birth (where encoded), gender (where encoded), geographic registration area (depending on numbering system)
Telephone number	Country, geographic location, network provider, employer affiliation (for work numbers), socioeconomic status (in limited circumstances), age group (through usage patterns), social connections, communication habits
Email address	Employer or organization affiliation, nickname, age group, interests, location, profession, gender (if reflected in the address)
Photograph or video image	Gender, approximate age, race/ethnicity, physical appearance, disability status, location, social circumstances, clothing style, religious affiliation (e.g., religious dress)
Biometric identifier (fingerprint, facial image, iris scan)	Physical characteristics, possible race, age estimation, health indicators in some cases
Handwritten signature	Writing style, language, education level, possible physical characteristics or disabilities affecting handwriting
Staff identification number	Employer affiliation, department, role, seniority level, location, employment status

The critical analytical principle is that identifiability must be assessed in context. Information that appears low risk in isolation may become identifying and therefore attract full data protection obligations when combined with other available information. Consider the following examples:

1. A first name alone may not identify an individual. However, when combined with an organization's name, job title and office location, it may be possible to identify a specific person. For example, "Mary, Finance Manager, Kisumu Office" may clearly point to a single individual within a small organization.
2. A photograph taken at a community event may appear harmless in isolation. However, when combined with social media posts indicating the event's date, location and attendees, the individuals in the image may become readily identifiable.
3. An email address that uses a pseudonym may not immediately reveal a person's identity. However, when combined with employment records, social media profiles or previous correspondence, it may be linked to a specific individual.
4. Information that a person is a 34-year-old female living in a particular village may seem non-identifying. However, if the village is small and only one resident matches those characteristics, the individual may be easily identified.
5. A staff identification number may appear to be merely an internal reference. However, when combined with an employer's personnel database, it can be used to identify a specific employee and access additional personal information about them.

The Aggregation Risks

One of the most important and least intuitive concepts in personal data identification is the aggregation risk: the risk that combining multiple pieces of individually low-sensitive information produces a data set that is highly sensitive or highly identifying.

Non-profit organizations often underestimate this risk as they assess the privacy implications of each piece of information they hold in isolation, rather than considering the cumulative effect of all the information they hold about a given individual.

A comprehensive beneficiary profile combining name, location, health status, case history, family composition, and programme participation history may be highly sensitive even if each field, taken individually, appears relatively harmless

Data minimization which means collecting only what is genuinely necessary is the most effective safeguard against this risk.

Reflective Exercise

Return to the organizational activity you identified at the start of this module.
List all the categories of information collected or processed during that activity.

For each item, assess: Is this a direct identifier, an indirect identifier

2.7 Sensitive Personal Data

Certain categories of personal data carry a materially elevated level of risk. Information in these categories is more likely, if exposed, misused, lost, or inadequately protected, to cause significant harm to the individuals concerned. That harm may take the form of discrimination, stigma, retaliation, physical danger, financial loss, exclusion, or psychological distress.

For this reason, data protection law and practice including under the Data Protection Act, 2019, impose stronger obligations and require additional legal justification before sensitive personal data is processed. Understanding which categories of information are treated as sensitive is a practical prerequisite for identifying when heightened care and specific legal considerations are required.

Category of Sensitive Data	Why It Carries Elevated Risk	Non-profit Examples
Health and medical information	Disclosure may result in stigma, discrimination in employment or service access, or direct physical harm in contexts where certain conditions are stigmatized.	HIV status, disability records, mental health history, nutritional assessments, reproductive health information.
Biometric data	Biometric identifiers are unique to the individual and cannot be changed if compromised. Misuse may enable identity fraud, surveillance, or tracking.	Fingerprints, facial recognition images, iris scans used in beneficiary registration or identity verification.
Political opinions or affiliations	Disclosure may expose individuals to retaliation, surveillance, exclusion, or harm in contexts of political tension or authoritarianism.	Participation in advocacy activities, civic engagements, or political movements documented in organizational records.
Religious or belief information	Disclosure may attract discrimination, violence, or exclusion in contexts of religious tension.	Faith-based support activities, religious affiliation records, or documentation of participation in religious community programmes.

Sexual orientation and gender identity	Criminalization and social stigma in many contexts mean that unauthorized disclosure may create serious physical, legal, and social risks.	Participation in LGBTI support or inclusion programmes; documentation in protection or healthcare contexts.
Children's information	Children cannot provide consent and are generally more vulnerable and are unable to understand, anticipate, or protect themselves from the consequences of how their information is collected, used, shared, or retained.	Child protection records, educational information, guardian details, photographs, and health data relating to minors.
Financial information	Disclosure may facilitate fraud, exploitation, or theft, and may reveal circumstances of poverty or financial vulnerability.	Bank account balances, cash transfer records, income assessments, household financial data.
Location and movement information	In humanitarian, protection, and conflict contexts, location disclosure may create direct physical safety risks.	Safe house addresses, residential address, displacement route records, shelter locations, GPS tracking data.
Ethnic or community identity	May attract discrimination, targeted harm, or exclusion in contexts of inter-community tension.	Ethnic demographic data, community membership records, or information about minority group participation.
Case management and protection records	Records of vulnerability, harm, and support-seeking individuals are among the most sensitive information held by non-profit organisations.	Survivor support records, case details, complaint and grievance files, referral histories, and protection case documentation.

It is also important to recognize that sensitivity is not determined solely by the category of information. Context and circumstance are equally significant. Location data is not inherently sensitive in all contexts. In a protection, conflict, or humanitarian context, however, it may be among the most sensitive information an organization holds. Similarly, information about political participation may carry minimal risk in a stable democratic context but significant risk in a context of political repression or civil unrest.

Context-Dependent Sensitivity

Non-profit organisations should not assess the sensitivity of personal data solely by reference to its category. The surrounding context the operational environment, the vulnerability of the individuals concerned, and the potential consequences of disclosure must also be considered.

In humanitarian settings: location data, movement records, and contact information may all create safety risks for displaced or at-risk individuals.

In advocacy and human rights contexts: records of participation, membership, and engagement may expose individuals to surveillance, retaliation, or criminalization.

In health and support contexts: any information that reveals vulnerability, help-seeking behaviour, or stigmatized conditions requires heightened care, regardless of whether it falls within a formally designated sensitive category.

2.8 The Data Lifecycle

The data lifecycle is a framework that describes how personal data moves through an organization, from the point of collection to its eventual deletion or disposal. Understanding the lifecycle is essential for responsible data management because risks and responsibilities do not arise solely at the point of collection. They arise at every stage through which personal data passes.

Non-profit organisations often focus primarily on collection the moment when information is gathered while giving less attention to what happens to information once it has been collected. The data lifecycle framework redirects attention to the full duration and scope of an organisation's engagement with personal information.

Stage	Description	Key Responsibilities and Questions
Collection	The initial gathering of personal information from or about individuals, whether through forms, interviews, observations, digital tools, or other means.	Is this information genuinely necessary for the stated purpose? Do individuals understand why it is being collected? Is there a lawful basis for collection? Are we collecting the only what we need/ require?
Recording	The capturing or documenting of collected information in a form that can be stored, retrieved, and used.	Are we recording information accurately and proportionately? Are we avoiding excessive, irrelevant, or speculative details? Is the recording format appropriate to the sensitivity of the information being collected?
Storage	The holding of personal information in physical or digital systems over time.	Where is the information stored? Who has access? Are appropriate physical and digital safeguards in place? Is the storage platform trusted and secure? Do third-party platform service providers have access to the data?

Use	The application of personal information to the purposes for which it was collected, including programme delivery, case management, reporting, and administration.	Are we using information only for the purpose for which it was collected and communicated to individuals? Are we applying appropriate access restrictions so that only those who need the information can access it?
Sharing	The disclosure or transfer of personal information to other parties, including partner organizations, donors, service providers, government bodies, or the public.	Do we have a lawful basis for sharing? Have the data subjects been informed that their information may be shared? Are there appropriate data-sharing agreements in place? Does the receiving party have adequate safeguards?
Retention	The period for which personal information is held before it is reviewed for disposal.	How long do we genuinely need this information? Has a retention period been established and communicated? Is retention reviewed at regular intervals?
Disposal or Deletion	The secure and irreversible removal of personal information when it is no longer required for its stated purpose.	Is information being deleted or destroyed in a manner that is complete and irreversible? Are paper records shredded rather than discarded? Are digital files permanently deleted rather than merely moved to a recycle bin?

A critical insight of the data lifecycle framework is that information does not stop being personal data once it has been collected and put to its initial use. It remains personal data with all its associated legal and ethical obligations for the entire period during which the organization holds it. The obligation to protect personal data extends throughout its journey within the organization, not at the point of collection.

Good Practice: Proportionate Retention

One of the most common data protection failures in non-profit organizations is the indefinite retention of personal data that is no longer needed. Case files from programmes that ended years ago, attendee lists from long-past events, and beneficiary databases from previous funding cycles are all examples of personal data that may be held well beyond any legitimate purpose.

Establishing retention periods and specific time limits after which categories of data are reviewed and disposed of is a fundamental element of responsible data management. Retention periods should be proportionate to the purpose for which data was collected and to any applicable legal or regulatory requirements.

Where information must be retained for accountability or regulatory purposes, consider whether full personal data is necessary or whether anonymized or aggregated records would serve the same purpose.

Reflective Practice

Using the activity, you identified at the start of this module, trace the full data lifecycle for the personal information involved.

At which stages do information enter, move through, and leave your organization's systems?
At which stages are risks most significant? Where are the gaps in your organization's current practices?
This exercise forms the foundation for the data mapping activity below.

2.9 Data Mapping: Tracing Information Through Organizational Processes

Data mapping is the practical exercise of tracing how personal data moves through specific organizational processes from collection to disposal as well as identifying at each stage what information is involved, how it is handled, who has access to it, with whom it is shared, and what risks arise. It is one of the most useful operational tools available to non-profit organizations seeking to understand and improve their data protection practices.

Data mapping serves several purposes. It enables organizations to identify precisely where personal data exists within their systems and processes including locations that that were not considered. It facilitates assessment of whether data minimization principles are being applied at each stage. It supports the identification of access control and security gaps. It also provides the foundation for producing and maintaining a data processing register, which is a legal requirement under the Data Protection Act, 2019.

The following analytical framework provides the questions that a data mapping exercise should address.

Analytical Question	Purpose of the Question
What information is being collected?	Identify all categories of personal data involved in the process, including those that may not be immediately obvious.
Is all the information genuinely necessary?	Apply data minimization and critically assess whether each category of data serves a clear and legitimate purpose.

Why is the information being collected?	Establish the purpose of processing and the lawful basis under which it is justified.
Who provides the information?	Identify the data subjects who are the individuals whose information is involved and any vulnerability conditions that may apply.
How is the information collected?	Examine the methods, tools, and channels through which information is gathered, and assess whether they are appropriate and secure.
Who has access to the information?	Identify everyone who can access the information within and outside the organization and assess whether that access is justified.
Where is the information stored?	Identify all physical and digital storage locations, including third-party platforms, shared drives, and mobile devices.
Is the information shared internally or externally?	Identify all instances in which information is transferred to other parties and assess the basis and safeguards for that sharing.
How long is the information retained?	Establish or review the applicable retention period and assess current disposal practices.
What could go wrong at each stage?	Identify the specific privacy and data protection risks at each point in the process.
Which individuals or communities could be most affected?	Assess the potential harm to data subjects, with particular attention to vulnerability conditions.
What safeguards currently exist?	Document existing controls, policies, organisational and technical measures.
What additional safeguards are needed?	Identify gaps and priority actions for improvement.

The Basic Data Mapping Template provides a structured format for recording the outputs of this exercise. To be inserted.

Data mapping is not a one-time exercise. It should be reviewed whenever a new programme is initiated, an existing programme is modified, a new digital platform is adopted, or a new data-sharing arrangement is established. Maintaining current and accurate data maps is an important component of ongoing accountability for responsible data management.

2.10 Why Data Protection and Privacy Matters and Why Responsible Data Handling Is Essential for Ethical, Safe, and Accountable Organisational Practice

Every day, non-profit organisations collect, use, store, and share personal information about employees, beneficiaries, donors, volunteers, partners, and members of the communities they serve. The decisions

made about that information have direct consequences for people's safety, dignity, autonomy, and rights. Responsible data handling means managing personal information with care, purpose, and accountability throughout its lifecycle. It involves collecting only the information that is genuinely necessary, using it only for legitimate and clearly defined purposes, protecting it from unauthorized access, disclosure, or misuse, and securely disposing of it when it is no longer required. Importantly, responsible data handling is not solely an IT/M&E function or a compliance exercise delegated to a single officer. It is a shared organizational responsibility that should be reflected in every programme, process, and interaction with individuals. The importance of responsible data handling becomes clear when things go wrong. Poor data practices can expose individuals to discrimination, stigma, retaliation, exploitation, financial loss, or even physical harm. They can undermine community confidence, damage an organisation's reputation, disrupt programmes, and result in legal or regulatory consequences. In some cases, the very people an organization seeks to support may be placed at greater risk because their information was not adequately protected.

This is particularly important for non-profit organisations because they often work with individuals and communities whose circumstances make them especially vulnerable to privacy harms. Survivors of violence, displaced persons, persons with disability, children, individuals living with stigmatized health conditions, marginalized communities, and persons in conflict with the law may all face significant consequences if their personal information is mishandled.
Data protection laws, including Kenya's Data Protection Act, 2019, recognize these risks and set out safeguards to ensure that personal information is handled responsibly. These laws are built on a broader principle: privacy is a fundamental human right. Respecting privacy means respecting the dignity, autonomy, and safety of the people whose personal information an organization collects and holds.

Fornon profit organizations, privacy and effective service delivery are inseparable. Communities share personal information because they trust that it will be used to support them, not expose them to harm. That trust is one of an organisation's most valuable assets. Once lost, it can be difficult to rebuild, and without it, an organisation's ability to fulfil its mission may be significantly compromised.

Data protection and privacy are not simply legal or administrative requirements; they are fundamental to ethical and accountable organisational practice. Every member of an organisation plays a role in ensuring that personal information is handled responsibly. By collecting only what is necessary, using information appropriately, protecting it from harm, and respecting the rights of individuals, organisations safeguard the people they serve while strengthening trust, credibility, and effectiveness. Ultimately, good data protection practices help ensure that organisational efforts to support communities do not unintentionally create risks for the very people they are meant to help

KEY TAKEAWAYS

1. Data takes more forms than you expect – Personal data is not confined to a spreadsheet or a database. It lives in paper registers, photographs, verbal disclosures, and informal digital messages, and each of these carries the same obligations as a formal system.

2. Small details combine into big risks – Indirect identifiers may seem harmless in isolation, but the aggregation risk means that combining several of them can re-identify an individual. What

looks anonymous rarely stays that way.

3. Not all data carries equal weight – Sensitive personal data attracts heightened obligations because the harm from its exposure is more severe. Recognising which data falls into this category shapes how carefully it must be handled.

4. Security is necessary but not sufficient – Locking data down is not the same as handling it lawfully or ethically. Genuine data protection requires attention at every stage of the data lifecycle, not just at the point of storage.

2.11 Assessment

Part A: Knowledge and Conceptual Understanding

1. What is personal data? Explain the difference between a direct identifier and an indirect identifier and give examples of each.
2. What is the associated risk, and why is it particularly relevant to non-profit organizations that hold beneficiary records?
3. Name five categories of sensitive personal data and explain, for each, why it attracts heightened data protection obligations.
4. Explain the distinction between privacy, data protection, and data security. Why is data security alone insufficient to ensure adequate data protection?
5. Describe the seven stages of the data lifecycle. For each stage, identify one key question that an organization should ask about the personal data passing through that stage.

Part B: Applied Analysis

1. An organisation maintains a beneficiary database containing names, household composition, GPS coordinates of home locations, HIV status, and programme participation history for over 5,000 individuals. The database is stored on a shared drive accessible to all 45 staff members. Conduct a data protection risk assessment of this situation, identifying at least four specific risks. Your organisation is about to launch a new mobile data collection system for field monitoring. Using the data lifecycle framework, identify the specific data protection considerations that should be addressed at each stage of the lifecycle for the data that will be collected through this system.

2. A donor has requested a full dataset of individual beneficiary records, including names and contact details, as part of a programme evaluation. The beneficiary records were collected under a consent form that described the data as being used for programme management and coordination. Analyse the data protection issues arising and describe what the organisation should do.

Part C: Organisational Application

1. Using the Basic Data Mapping Template conduct a data mapping exercise for the organisational activity you identified at the start of this module. Document your findings and identify the three most significant data protection risks arising from that activity.

2. Review your organization's current practices at each stage of the data lifecycle; That is from collection and use to storage, sharing, retention, and secure disposal. Which stages are well managed, and where are there gaps? What actions would you take to improve data protection throughout the lifecycle?

03.
Legal and Regulatory Framework

About This Module

This module provides a comprehensive overview of Kenya's legal and regulatory framework on data protection, examining the constitutional, statutory, regional and international instruments that govern the collection, processing, storage, sharing and protection of personal data. Learners will explore the constitutional right to privacy under Article 31 of the Constitution of Kenya, 2010, the Data Protection Act, 2019 and the subsidiary regulations enacted to support its implementation. The module further examines the influence of international and regional frameworks such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the African Union Malabo Convention and the European Union's General Data Protection Regulation (GDPR) on Kenya's data protection landscape.

3.1. Introduction

Different jurisdictions across the globe have initiated a variety of measures in a bid to safeguard the interests of their citizens regarding the vast amounts of personal data held by different individuals, organizations and corporations collectively referred to as data handlers. Many countries have, for instance, enacted data protection laws or have amended existing data protection legislation to ensure its ongoing relevance in the face of technological change and rapid globalization. These measures are founded on the recognition that the protection of personal data is a fundamental human right and, as such, requires robust legal and institutional safeguards.

Consequently, there is a heightened necessity for strong legal and institutional safeguards to prevent unauthorized access, misuse, or processing of personal data by third parties. These safeguards are not tailored at completely inhibiting the collection and processing of data, rather, they are aimed at facilitating transparency, accountability and safety in handling and processing of personal data. This is done with the view of establishing guardrails that insulate the data from unauthorized access and misuse, transfer of personal data both at intra and inter-state level and facilitating commerce. This furthers the role of data protection norms in not only protecting individual persons but also maintaining democracy through protection of the right to privacy.

The right to privacy has evolved to include state obligations related to the protection of personal data. This has crystallized into a whole regime of data protection characterized by international instruments weaved into domestic laws. This module presents a concise analysis of Kenya's legal and regulatory framework for data protection, offering brief, structured descriptions of the key laws, policies and institutional mechanisms that shape the protection of data in Kenya.

3.2 Objectives

This module has been designed to achieve the following objectives in relation to understanding the legal and regulatory frameworks:

1. To familiarize learners with the constitutional foundations of data protection in Kenya.
2. To examine the international and regional instruments influencing data protection in Kenya.
3. To provide an overview of the Data Protection Act, 2019.

3.3 Learning Outcomes

Upon completion of this module, learners should be able to demonstrate the following competencies:

Outcome	Demonstrated Competence
Understand the legal and regulatory framework for data protection	Describe the key laws, regulations, and instruments that together form Kenya's data protection framework, and explain how they interact to govern the handling of personal data.
Understand Article 31 of the Constitution as a foundation of data privacy	Explain the content of Article 31 and articulate its relevance as the constitutional basis for data protection and privacy rights in Kenya.
Understand the contribution of international and regional instruments to Kenya's data protection framework	Identify the UDHR, ICCPR, GDPR, and Malabo Convention, and explain how each has shaped or informed the development of Kenya's data protection framework.

3.4 The Constitution of Kenya, 2010

The Constitution lays the foundation for basic rights and freedoms through Chapter Four on the Bill of Rights. These rights must be honoured, observed, respected, protected, promoted, and fulfilled by every entity and agency within the government as well as its citizens.

The right to privacy is provided under article 31 which guarantees every person protection against arbitrary or unlawful interference with their personal sphere and autonomy. This right safeguards individuals from unnecessary collection, disclosure, or exposure of information relating to their family life or private affairs. In addition, the right to privacy extends to the protection of communications, ensuring that personal correspondence and exchanges are not unlawfully intercepted, monitored, or infringed upon. This right forms the foundation of data protection in Kenya because personal data is intrinsically linked to an individual's dignity, autonomy and freedom.
As digital technologies increasingly enable the large-scale collection, processing and dissemination of personal information, the constitutional right to privacy provides both the legal and normative foundation upon which data protection frameworks are constructed. In Kenya, this right is given practical effect through the Data Protection Act, 2019, which regulates the collection, processing, storage, sharing and transfer of personal data. The Act establishes clear obligations for data controllers and data processors to ensure that personal information is handled in a lawful, fair, transparent, and secure manner. Additionally, it confers enforceable rights upon data subjects, including the rights to access personal data, seek rectification of inaccurate information, withdraw consent, and request the deletion of data where appropriate.

Further, the Constitution also safeguards the right to privacy by incorporating international law into Kenya's domestic legal framework. Article 2(5) provides that the general rules of international law form part of the law of Kenya, while Article 2(6) stipulates that any treaty or convention ratified by Kenya shall constitute part of Kenyan law under the Constitution. Additionally, Article 21 (4) obligates the State to enact and implement legislation to fulfil its international obligations relating to human rights and fundamental freedoms.

3.5 Universal Declaration of Human Rights (UDHR)

The modern privacy benchmark at the international level can be found in the 1948 Universal Declaration of Human Rights (UDHR) which was aptly described by Professor Richard Lillich as the "Magna Carta" of contemporary international human rights law.

The UDHR is not a legally binding treaty, but a resolution adopted by the UN General Assembly as a common standard of achievement, meaning a universal set of goals and values that all nations and peoples should strive towards. The UDHR was originally formulated as soft law, being aspirational and not legally binding. Its lack of legal status has not prevented its significant influence in formulating legislation worldwide. While it does not require ratification by states, it is considered the global blueprint and foundation of international human rights law. Kenya has recognized the Universal Declaration of Human Rights and has demonstrated its commitment to the principles and standards embodied in the Declaration through the development of its constitutional, legislative and institutional framework.

Article 12 of the UDHR states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of law against such interference or attacks." When the right to privacy was recognized as an international human right in the UDHR, it had not been included in any state constitution. In the years after World War II, state constitutions protected only aspects of privacy, such as the inviolability of the home and of correspondence and unreasonable searches of the body. Such an umbrella "privacy" term was new, and the UDHR drafters were likely not aware that the term would open the door for the protection of further aspects of privacy not mentioned, nor even imagined at the time, in the codification process.

3.6 International Covenant on Civil and Political Rights (ICCPR)

The International Covenant on Civil and Political Rights (ICCPR) serves as a fundamental international legal framework for data protection, particularly through the lens of human rights, privacy, and freedom of expression in the digital age. Eighteen years after the adoption of the UDHR, privacy was recognized in Article 17 of the ICCPR using a similar language to Article 12 of the UDHR.

Article 17 of the ICCPR establishes the fundamental principle that individuals are entitled to protection against arbitrary or unlawful interference with their privacy, family, home, or correspondence, as well as against unlawful attacks on their honour and reputation. It further affirms that all persons have a right to legal protection against such intrusions or violations.

This provision underscores the centrality of personal dignity and the integrity of private life, while simultaneously imposing an obligation on the state to enact and enforce legal safeguards that prevent, address, and remedy infringements of these rights. Kenya has ratified the International Covenant on Civil and Political Rights (ICCPR), which upholds the right to privacy. The Human Rights Committee has noted that state parties to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against [arbitrary or unlawful interferences with the right to privacy]," regardless of "whether they emanate from State authorities or from natural or legal persons," and to protect the right to privacy itself.

3.7 General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, is a European Union data protection legislation that establishes comprehensive safeguards for the privacy and security of personal data relating to individuals within the European Economic Area (EEA). Its scope extends not only to organizations operating within EEA member states but also to certain entities outside the EEA that process the personal data of individuals located within the region. Specifically, the GDPR applies to the collection and use of personal data where such processing occurs in the context of activities carried out within the EEA, relates to the offering of goods or services to individuals in the EEA, or involves the monitoring of their behaviour. It also conditions data transfers outside the EU on third states having adequate (meaning essentially equivalent) data protection standards.

Under the GDPR, this burden shifts to non-EU countries. That is, the GDPR contains provisions that apply extraterritorially: non-EU countries processing EU data can be subject to GDPR penalties for failing to protect data according to EU standards. As a result, to maintain (unpenalized) digital trade and interaction with European Union countries, other countries have a strong incentive under the GDPR to at least approximate European data protection standards. This exemplifies the "Brussels effect" to mean Europe's assertion of "unilateral power to regulate global markets" through "legal institutions and standards." Countries in the EAC for example did not start passing domestic data protection laws until after the adoption of the GDPR, suggesting that these countries are sensitive to European regulatory pressure.

The GDPR without doubt informed the text of Kenya's Data Protection Act, 2019. From matters relating to classification of data, data subjects' rights, the statutory duties of data controllers and data processors, legitimate processing of data, pseudonymization and anonymization, notification of breaches and enforcement provisions among others seem to have a strong tinge of the GDPR.

3.8 Malabo Convention

The African Union (AU) Convention on Cyber Security and Personal Data Protection, commonly known as the Malabo Convention, was adopted on 27 June 2014, in Malabo, Equatorial Guinea. The Convention is Africa's first international instrument on data protection which was passed in 2014. The Convention seeks to, among other objectives, harmonize the laws of member states on data protection and encourage member states to create frameworks to protect personal data within the continent. Article 36 of the Malabo Convention states that the treaty would come into effect once 15 ratifications are achieved. In May 2023, Mauritania ratified the Convention, bringing it into effect 30 days later, on 8 June 2023. As of July 2026, Kenya is not yet a formal signatory to the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), but it is in the process of acceding to it. Following Cabinet approval, the Office of the Data Protection Commissioner (ODPC) has initiated stakeholder consultations regarding accession to the treaty.

3.9 Data Protection Act, 2019

The enactment of the Data Protection Act on 25 November 2019 marked a significant milestone in the development of Kenya's data protection framework. Read together with Article 31 of the Constitution of Kenya, 2010, the Act provides the principal legislative foundation for the protection of the right to privacy in the digital era. Prior to its enactment, the protection of privacy rights in Kenya remained fragmented, largely dependent on scattered statutory provisions and evolving judicial interpretation, with no comprehensive legal regime specifically dedicated to the regulation of personal data.
The Act therefore fills this legislative gap by establishing a coherent framework governing the collection, processing, storage, and sharing of personal data. It further imposes obligations on data handlers operating within Kenya, as well as those processing the personal data of individuals residing in Kenya. It simultaneously guarantees data subjects with enforceable rights and remedies aimed at safeguarding their personal information against unlawful or arbitrary interference.

The Act establishes a robust legal framework that imposes clear statutory obligations and consequences upon both public and private sector actors who process personal data in contravention of its provisions. Beyond regulating the processing of personal information, the Act significantly strengthens the constitutional right to privacy by reflecting Kenya's commitment to international human rights standards and by aligning national data protection laws with the principles embodied in the UDHR and the ICCPR.

KEY TAKEAWAYS

1. Data privacy is a fundamental human right that requires legal and institutional safeguards.
   Data privacy is not a technical or administrative concern. As a fundamental human right, it imposes obligations on governments, organizations, and individuals to respect, protect, promote, and fulfil the right to privacy through appropriate legal, institutional, and practical safeguards.

2. The constitutional foundation of data protection in Kenya is Article 31 of the Constitution.
   The right to privacy protects individuals from unlawful collection, use, disclosure, and interference with their personal information and serves as the cornerstone of Kenya's data protection framework.

3. Kenya's data protection framework is shaped by both international and regional instruments.
   Instruments such as the United Nations's Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the General Data Protection Regulation, and the Malabo Convention have significantly influenced the development of Kenya's data protection laws.

z

4. The Data Protection Act, 2019 provides the primary legal framework for data protection in Kenya.
   The Act regulates the collection, processing, storage, sharing, and transfer of personal data, establishes rights for data subjects, and imposes obligations on data controllers and processors.

ASSESSMENT QUESTIONS

1. Discuss the significance of Article 31 of the Constitution of Kenya, 2010 in establishing the legal foundation for data protection and privacy in Kenya.

2. Discuss the influence of international and regional instruments such as the UDHR, ICCPR, GDPR, and the Malabo Convention on Kenya's data protection framework.

3. Describe the purpose of the Data Protection (General) Regulations, 2021 and explain how they support the implementation of the Data Protection Act, 2019.

4. Describe the purpose of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 and explain how they support the implementation of the Data Protection Act, 2019.

04.
The Data Protection Act 2019

About This Module

This module introduces the Data Protection Act, 2019 as the principal legislation enacted to operationalize Article 31 of the Constitution of Kenya. It examines the context that necessitated the enactment of the Act, providing learners with a foundation for understanding both its purpose and significance beyond its textual provisions.

4.1. Introduction

The Data Protection Act 2019 (DPA) was enacted on 8th November 2019 as the legislative expression of the constitutional right to privacy guaranteed under Article 31 of the Constitution of Kenya. While Article 31 establishes privacy as a fundamental right, it does not prescribe the detailed legal framework necessary to regulate the processing of personal data or to provide mechanisms for its protection and enforcement. The Act was therefore enacted to operationalize Article 31 by translating the constitutional guarantee into a practical and comprehensive statutory framework governing the collection, use, storage, disclosure, transfer, and disposal of personal data.

The object and purpose of the Act is to establish a comprehensive legal framework governing the processing of personal data. The Act is divided into eleven parts namely;

1. Part 1 is the preliminary
2. Part 2 provides for the establishment of the Office of the Data Protection Commissioner.
3. Part 3 regulates registration of data controllers and data processors.
4. Part 4 sets out principles and obligations of personal data protection.
5. Part 5 provides grounds for processing sensitive personal data.
6. Part 6 regulates transfer of personal data outside Kenya.
7. Part 7 sets out exemptions.
8. Part 8 sets out enforcement provisions.
9. Part 9 is on financial provisions.
10. Part 10 provides for enactment of regulations.
11. Part 11 sets out miscellaneous provisions.

The Act therefore bridges the gap between constitutional principles and practical implementation. Together with its accompanying Regulations, it forms the cornerstone of Kenya's data protection and privacy framework. While the Act sets out the overarching legal principles, rights, obligations, and institutional framework, the Regulations operationalize these provisions by prescribing the procedures, standards, and compliance requirements necessary for their effective implementation.

4.2 Objectives

This module has been designed to achieve the following objectives in relation to understanding the Data Protection Act:

1. To trace the legislative journey leading to the enactment of the Data Protection Act, 2019.
2. To introduce the purpose, scope, and practical application of the Data Protection Act.
3. To promote a contextual understanding of legislation as a product of social, political, economic, and technological realities.
4. To examine the purpose, scope and practical application of the Data Protection Regulations in operationalizing the Data Protection Act, 2019.

4.3 Learning Outcomes

Upon completion of this module, learners should be able to demonstrate the following competencies:

Outcome	Demonstrated Competence
Explain the historical and legal developments leading to the Data Protection Act, 2019	Identify the key events that created the need for a dedicated data protection law in Kenya.
Understand the constitutional foundations of data protection and privacy	Identify the constitutional provisions that underpin data protection and privacy rights and explain how they anchor the subsequent statutory framework.
Understand how legal provisions derive meaning from historical and policy context	Explain why interpreting a law requires understanding the circumstances and objectives behind its enactment, rather than reading its text in isolation.
Recognize the importance of the Data Protection Act, 2019	Articulate the specific problems the Act was designed to address and describe how it strengthens the protection of privacy in Kenya.

4.4 The Object and Purpose of the Act

The section on object and purpose is important because it serves as the legislative guiding light explicitly stating what the Act aims to achieve and why it was enacted.

Section 3: Object and purpose of the Act

The object and purpose of this Act is—

(a) to regulate the processing of personal data;
(b) to ensure that the processing of personal data of a data subject is guided by the principles set out in section 25;
(c) to protect the privacy of individuals;
(d) to establish the legal and institutional mechanism to protect personal data; and
(e) to provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with this Act.

4.5 Key Definitions in the Act

The Data Protection Act, 2019 establishes a clear legal framework for the protection of personal data and the regulation of its processing in Kenya. Understanding the key definitions under the Act is essential because they provide the foundation for interpreting and applying its substantive provisions. The following are some of the key definitions that underpin Kenya's data protection framework.

Data means information which—

(a) is processed by means of equipment operating automatically in response to instructions given for that purpose;
(b) is recorded with intention that it should be processed by means of such equipment;
(c) is recorded as part of a relevant filing system;
(d) where it does not fall under paragraphs (a), (b) or (c), forms part of an accessible record; or(e)is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

Personal data means any information relating to an identified or identifiable natural person;
Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
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; and

Biometric data means personal data resulting from specific technical processing based on physical, physiological or behavioural characterization including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition;

Health data means data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services

Identifiable natural person means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;
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 of personal data;

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

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

(a) collection, recording, organization, structuring;
(b) storage, adaptation or alteration;
(c) retrieval, consultation or use;
(d) disclosure by transmission, dissemination, or otherwise making available; or
(e) alignment or combination, restriction, erasure or destruction.

4.5 The legislative journey leading to the enactment of the Data Protection Act, 2019.

The journey towards the Data Protection Act began long before the Act itself was conceived. A major turning point occurred with the promulgation of the Constitution of Kenya, 2010. This fundamentally transformed Kenya's legal and governance architecture by introducing an expansive Bill of Rights.

Of particular significance was Article 31, which expressly guarantees every person's right to privacy. For the first time in Kenya's constitutional history, privacy received explicit constitutional recognition.
Although Article 31 did not specifically refer to "data protection," it created a constitutional obligation upon the State to protect informational privacy. The Constitution therefore established the legal basis upon which future data protection legislation would be developed. It also signalled a broader shift toward rights-based governance and accountability.

4.6 The Brussels Effect and its influence on Kenya's Data Protection Act, 2019

Predictions of EU decline, driven by Brexit, an assertive Russia, terrorism, and the refugee crisis stemming from the war in Ukraine, tend to overlook a critical counternarrative: the EU remains one of the world's most powerful regulatory forces. This influence, known as the "Brussels effect," is most visible in international trade, and increasingly, in data protection.

The Brussels effect describes the EU's unique capacity to shape global markets and regulatory standards unilaterally, without needing formal international agreements. It is most pronounced in data protection, consumer rights, and environmental regulation, areas where the EU's market size gives it outsized leverage. Understanding the Brussels effect requires first understanding the legal distinction between "de facto" and "de jure." De facto, meaning "in fact" or "in practice," describes something that operates regardless of formal legal recognition. De jure, meaning "by law" or "by right," describes something that exists because it is formally authorized or required by law.

The Brussels effect operates in these two forms. The first, de facto, occurs when multinational corporations voluntarily adopt EU standards across their global operations, not out of legal obligation, but to preserve seamless access to the EU market. The practical effect is that EU law governs corporate behaviour far beyond EU borders, even in jurisdictions with no formal requirement to comply.

The second, de jure, occurs when foreign governments formally legislate EU-style rules into domestic law. This shift is often driven by corporate lobbying, as businesses that have already aligned with EU standards push for a level playing field, ensuring competitors bear the same compliance costs rather than gaining an advantage by ignoring them.

Since its implementation in 2018, the General Data Protection Regulation (GDPR) has triggered a global de jure Brussels effect in privacy law. Countries across the world have adopted or incorporated GDPR-style protections into their own legal systems, a trend that directly serves the European Data Protection Board's stated ambition of establishing EU data protection as the global benchmark.

Kenya's Data Protection Act, though developed outside the EU's jurisdiction, bears clear markers of GDPR influence in its underlying concepts and regulatory design. This is not incidental. It reflects the practical incentives driving the Brussels effect: facilitating trade with EU partners, attracting foreign investment, and securing Kenya's place in the global digital economy.

4.7 The Huduma Namba

The enactment of the Data Protection Act, 2019 cannot be understood without appreciating the role played by the National Integrated Identity Management System (NIIMS), which was then known as Huduma Namba. While discussions on data protection had been ongoing in Kenya for several years, the launch of Huduma Namba in 2019 brought issues of privacy, personal data protection, surveillance and state accountability into sharp public focus.

The initiative exposed significant gaps in Kenya's legal framework governing the collection and processing of personal data and accelerated the demand for a comprehensive data protection law. Consequently, the controversy surrounding Huduma Namba became one of the most significant catalysts for the enactment and operationalization of the DPA.

Huduma Namba was conceived as a centralized digital identity system intended to consolidate personal information held across various government databases into a single repository. Through the system, the government sought to collect and process extensive personal information relating to citizens and residents,

including names, dates of birth, identity details, residential information, and biometric data such as fingerprints and facial images. The stated objectives of the initiative included enhancing service delivery, eliminating duplication of records, improving national security, and promoting administrative efficiency. This prompted constitutional petitions consolidated in the Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 8 others (The Nubian Case) where it was argued that the government was embarking on one of the largest data collection exercises in Kenya's history without the existence of a comprehensive legal framework governing the collection, storage, processing, sharing, and protection of personal data. At the time, Kenya lacked a dedicated data protection law, meaning that citizens had limited legal protections.

Ultimately, the Courts acknowledged the legitimate objectives underlying the government's efforts to modernize data collection and public service delivery but also noted that any large-scale processing of personal data must be accompanied by adequate legal and institutional safeguards capable of protecting the privacy and rights of individuals.

As a result, the enactment of the Data Protection Act, 2019 came in to fill in the gaps identified by the Court in the Nubian Case. The Act established a comprehensive legal framework governing the processing of personal data and created the Office of the Data Protection Commissioner to provide independent oversight and enforcement. It also introduced clear obligations for data controllers and data processors, established safeguards for the processing of sensitive personal data, and created mechanisms for accountability and redress.

4.8 Normative Framework in the Data Protection Act

The Act provides principles of data protection which establish the normative framework of data protection by providing the foundational standards that govern how personal data should be collected, processed, stored, shared, and disposed of. These principles give practical effect to the constitutional right to privacy under Article 31 by ensuring that personal data is handled in a lawful, fair, and transparent manner.

4.9 Subsidiary Regulations

To give effect to the Act and to translate the Act's broad requirements into clear, actionable and enforcement measures, the Cabinet Secretary, Ministry of Information, Communication, Technology, Innovation and Youth Affairs exercising powers granted under section 71 of the Act has since published four Regulations under the Act. These are as listed below.

1. The Data Protection (Civil Registration) Regulations; Legal Notice No. 196 of 2020
   These Regulations govern the collection, processing and storage of personal data for civil registration, including births, deaths, adoptions, registration of persons, issuance of passports, registration of marriages, registration of deaths and issuance of any document of identity. These regulations prescribe obligations to civil registration entities as well as impose security safeguards.

2. The Data Protection (General) Regulations; Legal Notice No. 263 of 2021
   These Regulations enable the rights of a data subject, provide for, restriction on the commercial use of personal data, obligations of data controllers and data processors, elements to implement

data protection by design or by default, notification of personal data breaches, transfer of personal data outside Kenya, data protection impact assessment, and exemptions under the Act.

3. The Data Protection (Complaints Handling Procedure and Enforcement) Regulations; Legal Notice No. 264 of 2021
   These Regulations outline the procedure for lodging, admission and response to complaints plus enforcement provisions, all with the object and purpose of facilitating a fair, impartial, just, expeditious, proportionate and affordable determination of complaints lodged with the Data Commissioner, providing for issuance of enforcement notices and issuance of penalty notices as contemplated under the Act.

4. The Data Protection (Registration of Data Controllers and Data Processors) Regulations; Legal Notice No. 265 of 2021
   These Regulations provide for the procedure for registration of data controllers and data processors as provided under section 18 of the Act.

KEY TAKEAWAYS

- The Data Protection Act, 2019 gives practical effect to Article 31 and serves as the principal legislation governing the collection, processing, storage, sharing, and transfer of personal data in Kenya.

- The GDPR through the Brussels Effect, positioned data protection as a global standard, and influenced the development of Kenya's Data Protection Act, 2019, demonstrating how global privacy standards shape national data protection frameworks and promote responsible handling of personal data. The Huduma Namba initiative highlighted the risks associated with large-scale collection and processing of personal data and underscored the need for a comprehensive legal framework to protect privacy and personal information.

- The Act establishes a normative framework by providing the foundational standards that govern how personal data should be collected, processed, stored, shared, and disposed of.

- The subsidiary regulations operationalize the Data Protection Act and provide practical compliance mechanisms. The regulations address key areas including civil registration, data subject rights, data breach notification, cross-border data transfers, complaint resolution, enforcement procedures, and registration requirements for data controllers and processors.

ASSESSMENT QUESTIONS

Part A: Knowledge and Legal Understanding

1. The DPA did not emerge in isolation. Trace the legislative journey that led to its enactment, beginning with the Constitution of Kenya, 2010 and Article 31, moving through the Huduma Namba controversy and the Nubian Rights Forum case, and arriving at the Act itself. What role did each of these developments play in shaping Kenya's data protection framework?

2. The Act establishes a number of key definitions that form the foundation for interpreting all its substantive provisions. Explain the meaning of the following terms as defined in the Act, and for each one give a practical example drawn from non-profit work: personal data; sensitive personal data; data controller; data processor; and consent.

3. The Act is supplemented by four subsidiary Regulations that provide more detailed requirements for implementing and enforcing the Act. Identify each of the four Regulations and, for each one, briefly explain its purpose, scope, and the key aspect of data protection practice that it is intended to regulate.

Part B: Applied Analysis

1. An organisation is registering beneficiaries for a new food security programme. During registration, it collects names, national ID numbers, household composition, GPS coordinates of beneficiaries' homes and health information. A staff member argues that this is simply "programme data" and that the definitions under the Data Protection Act do not apply to a small NGO. Using the definitions in the Data Protection Act, assess the staff member's claim. Identify the different categories of data being collected and explain what the Act provides in relation to each category. What do these definitions mean for the organisation's data protection obligations?

2. A staff member at an organisation asks why the organisation needs to understand four separate Regulations when the Data Protection Act already sets out its main requirements. Explain the purpose of the four subsidiary Data Protection Regulations covered in this module.

Part C: Organisational Reflection

1. How does your organisation currently collect, use, store and share personal data?
2. What categories of personal data does your organisation handle, and which of these would be considered sensitive or high-risk?

05.
The Principles of Data Protection

About This Module

This module explains the basic rules for handling personal information, how to collect it, use it, store it, and dispose of it safely. These rules are called the Principles of Data Protection.
Instead of focusing on complex legal language, this module uses real examples from everyday community work to help you understand how these principles apply when you're working with people and their information.

5.1 Introduction

Laws can be built on two different foundations: rules or principles. Before anything else, it's important to understand which foundation the law your organisation operates under is built on, and why. Rule-based laws set out specific, prescriptive requirements (do X, don't do Y). These laws are specific, detailed and must be followed strictly. They offer clear and concrete boundaries. They're precise and easy to check against ("did we comply, yes or no?").

Principle-based laws set out broad standards or outcomes the law wants to achieve such as fairness or transparency and let organisations work out how to meet them. This approach relies on overarching values and ethical principles to guide actions allowing for flexibility and adaptability. Most modern data protection frameworks (international and national) are principle-based at their core. Ultimately, a principle-based approach places the data protection principles at the centre of decision-making. When organizations understand and apply these principles effectively, the specific rules and requirements become practical tools for achieving responsible and compliant data handling.
Why principles are the cardinal rules of data protection?

Principles sit at the foundation of data protection. They are not one component among many, but the standard against which everything else is measured. Specific rules, policies, and everyday decisions all derive their meaning from the principles behind them. This is what makes them cardinal they are first in importance, and everything else in data protection radiates outward from them.
Section 25 of the DPA sets out these principles. They are the overarching standards that inform

how non-profits govern their handling of personal data. Adopting, integrating, and consistently applying these principles is what allows an organisation to move beyond mere compliance and toward genuine data protection practice.

Reflective Practice

Every time your organization collects a piece of personal information such as a name, phone number, ID number, health detail, location, or any other identifying detail about someone in a community, a set of principles are at work.

Key questions to ask oneself are: Did you collect only what was necessary, or did the form ask for more? Did the person know why you needed it? Will it be kept only as long as it's needed, or indefinitely? Each of these questions directly leads the learner to a data protection principle.

Keep these examples in mind as you work through this module. They will serve as practical reference point for the concepts introduced in each section.

5.2 Objectives

This module has been designed to achieve the following objectives in relation to understanding principles of data protection:

1. To introduce the constitutional and legal foundation of the principles of data protection.
2. To describe in detail the nine data protection principles
3. To link the principles to day-to-day organisational data practices
4. To enable learners, apply the data protection principles by reviewing their organisation's data protection practices and identifying areas for improvement.

5.3 Learning outcomes:

By the end of this module, the learners should be able to:

Outcome	Desired competence
Name and explain the data protection principles	Identify the nine principles under section 25 of the Data Protection Act, 2019.
Explain the practical requirements of each principle	Describe, for each principle, the specific actions an organization must take to uphold it in day-to-day data handling
Distinguish compliant from non-compliant practice in reference to principles of data protection	Given a described data handling practice, correctly assess whether it satisfies or breaches a given principle, and explain the reasoning behind that assessment.

Identify violations in real scenarios	Analyse a community facing scenario to identify which principle(s) have been violated, explain how, and propose specific, actionable remedies to bring the practice into alignment.
Evaluate organizational practice against the principles	Apply the self-assessment checklist to their own organization's data practices, identifying areas of compliance.

5.4 Principles of Data Protection

5.4.1 Principle 1: Right to Privacy and valid explanation

Principle	**Legal Reference:** Section 25(a and e) | Article 31(c and d), Constitution of Kenya
Right to Privacy and valid explanation	Personal data must be processed in accordance with the data subject's right to privacy, and where information relates to family or private affairs, it may only be collected if a valid explanation is provided for why it is needed.
What it means for your organisation	Your organisation must consider whether collecting or using specific data could violate an individual's right to privacy. The rule of thumb is ensuring the data subject's right to privacy is respected at every stage of the data lifecycle.
How the principle can be demonstrated	Your organisation can demonstrate this principle through: 1. Purposeful collection: Only collecting personal data that are necessary for the stated purpose. 2. Providing a valid explanation in scenarios that require collection of sensitive data. 3. Clearly explaining to individuals what will be collected, why, and how it will be used, before collecting it so that individuals give informed consent. 4. Limiting access to personal data strictly to authorized personnel 5. Ensuring information is never discussed, referenced, or disclosed unnecessarily whether verbally, in writing, or in publications in a manner that identifies the individual 6. Actively assessing, at each stage of the data lifecycle, whether a proposed action such as a new data request, a reporting requirement, a donor ask) could violate a data subject's privacy.

Reflection	When a non-profit documents testimonies from survivors of gender-based violence, it must prioritize the survivor's right to privacy by ensuring that their personal information and experiences are handled with confidentiality, care, and respect. Information should only be collected, used, or shared where necessary and with appropriate safeguards to protect the survivor from potential harm. Every decision about how that information is handled must be measured against one question: does this uphold or undermine the survivor's right to privacy through the data life cycle.

5.4.2 Principle 2: Lawfulness, Fairness and Transparency

Principle	**Legal Reference: Section 25(b)**
Lawfulness, Fairness & Transparency	Data must be collected lawfully, treated fairly without discrimination, and data subjects must be informed about how their data will be used.
What it means for your organisation	Lawful: You must have a legal basis for processing data (e.g. consent, contract, vital interest). Fair: This means that personal data should be handled in a manner that is reasonable, ethical, and respects the rights of the data subject. It requires organizations to consider how their actions affect data subjects and avoid using personal data in ways that could cause harm, disadvantage, discrimination, or unexpected consequences. Transparent: Before collecting data, inform data subjects what you are collecting, why, how it is collected, how it will be used, how it will be stored and for long it will be kept, and who it may be shared with. This a involves the use of clear, simple and plain language to communicate with a data subject.
How the principle can be demonstrated	Your organisation can demonstrate lawfulness by: 1. Identifying and providing an appropriate legal basis clearly connected to the specific purpose of the processing. 2. Only do processing that is necessary for the purpose stated. 3. Ensuring the data subject is granted the highest degree of autonomy possible with respect to control over their personal data 4. Ensuring a data subject knows what they have agreed to. 5. Restricting processing where the lawful basis ceases to apply Your organisation can demonstrate fairness by: 1. Enabling a data subject to communicate and exercise their rights 2. Guarding against the exploitation of the needs or vulnerabilities of a data subject 3. Incorporating human intervention to minimise biases that automated decision-making processes may create

	Your organisation can demonstrate transparency by: 1. Use of clear, simple and plain language to communicate with a data subject 2. Providing the data subject with access to information regarding the processing of their personal data at the relevant time in the appropriate form. 3. Providing a fair understanding of the expectation to processing of personal data particularly for children or other vulnerable groups 4. Providing details of the use and disclosure of the personal data of a data subject
Reflection	An organisation, XYZ, registering participants for a workshop must provide an explanation informing participants why they are collecting the information in a clear and understandable language prior to the participants signing the registration form.

5.4.3 Principle 3: Purpose Limitation

Principle	**Legal Reference:** Section 25(c) of DPA 2019 Personal data must be collected for an explicit, specific, and legitimate purpose, and must not be used for anything incompatible with that purpose.
Purpose Limitation	Without a defined purpose, data collection has no natural limit during processing of the collected data. Organisations can end up gathering information exposing individuals to risks. This principle exists to ensure that every piece of personal data an organisation holds has a clear, justifiable reason for being processed, and that the data cannot be later used for unrelated purposes
What it means for your Organisation	You must decide and communicate the purpose of data collection before you collect it. You cannot later use the data for a different purpose without informing the data subject.
How the principle can be demonstrated	Your organisation can demonstrate this principle by: 1. Defining and documenting the purpose of data collection before any data is collected. 2. Communicating that purpose clearly to data subjects at the point of collection. 3. Reviewing any new or secondary use of existing data against the original stated purpose before proceeding to ensure compatibility. 4. Avoiding open-ended or non-explicit purposes in the data collection forms and consent forms.
Reflection	An organisation collects participants' contact details for a training event. It cannot then use those contacts to send fundraising communications without going back to participants, informing them of the new purpose.

5.4.4 Principle 4: Data Minimisation

Principle	**Legal Reference:** Section 25(d) of the DPA Only collect data that is adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.
Data Minimisation	Every additional piece of personal data collected is an additional point of risk for individuals. This means more data to secure, more data that could be misused, breached, or lost. This principle of data minimisation exists to reduce this risk at its source (point of collection).
What it means for your organization	Review all your data collection forms and systems. Remove any fields that are not necessary for the purpose. Every field of a data collection form or system must be justifiable.
How the principle can be demonstrated	Your organisation can demonstrate this principle by: 1. Limiting the amount of personal data collected to only what is necessary. 2. Maintaining the ability to demonstrate the relevance of data to the processing in question. 3. Avoiding the collection of personal data altogether when the collection is not necessary for the relevant purpose. 4. Pseudonymising personal data as soon as it is no longer necessary to have directly identifiable personal data, pseudonymised data and identification keys stored separately. 5. Anonymising or deleting personal data where it is no longer necessary for the purpose. 6. Making data flow efficient to avoid the creation of more copies or entry points for data collection than is necessary.
Reflection	You are running a training on digital security which needs to record attendance. The registration form should only ask for the name and organisation as the relevant details. Information such as bank details, marital status, date of birth or next of kin are not necessary for registration purposes.

5.4.5 Principle 5: Accuracy

Principle	**Legal Reference:** Section 25(f) Personal data must be accurate, kept up to date, and every reasonable step is taken to ensure that any inaccurate data is erased or rectified without delay.
Accuracy	Inaccurate data can lead to real risk or harm such as a beneficiary wrongly excluded from a programme due to an outdated record, a donor report built on wrong figures, or a survivor misidentified due to a data entry error.

	Accuracy protects both the integrity of an organisation's work and the individuals whose lives are affected by decisions made using processed data.
What it means for your organisation	Your organisation must take reasonable steps to ensure the personal data it holds is correct, and to update or rectify it when it changes or is found to be wrong. This includes giving data subjects a way to flag inaccuracies and request corrections.
How the principle can be demonstrated	Your organisation can demonstrate this principle by: 1. Ensuring data sources are reliable in terms of data accuracy 2. Verification of the correctness of personal data with the data subject before and at different stages of the processing. Erasing or rectifying inaccurate data without delay. 3. Giving data subjects reasonable access to personal data to control accuracy and rectify as needed. 4. Having personal data accurate at all stages of the processing and for accuracy at critical steps. 5. The use of technological and organisational design features to decrease inaccuracy.
Reflection	An organization maintains a beneficiary database. When a beneficiary reports a change in address or contact, the organization should update the record immediately and periodically review old records to remove or correct outdated information.

5.4.6 Principle 6: Storage Limitation

Principle	**Legal Reference:** Section 25(g) Every data controller or processor shall ensure that personal data is kept in a form which identifies the data subjects no longer than is necessary for the purposes of which it is collected.
Storage Limitation	Holding onto personal data indefinitely increases risk without value addition to the organisation. Old, unused records are a liability if breached. This principle requires organizations to treat data retention as a deliberate and time-bound decision.
What it means for your organisation	Develop a data retention schedule specifying how long different types of data are kept. Some legal requirements may require you to retain data for specific periods. At the end of the retention period, data must be securely deleted.

How the principle can be demonstrated	Your organization can demonstrate this principle by: 1. Having clear internal procedures for deletion 2. Determining what duration of storage of personal data is necessary for the purpose. 3. Formulating internal retention statements and implementing them 4. Ensuring that it is not possible to re-identify anonymised data or recover deleted data.
Example	A non-profit organisation provides financial assistance to vulnerable households and collects beneficiaries' identification documents, contact details, and assessment records to determine eligibility and provide support. The organisation should not keep these records indefinitely after the assistance programme ends. It should have a defined retention period (for example, keeping records for a specified number of years to meet reporting or audit requirements) and then securely dispose of the information when it is no longer required.

5.4.7 Principle 7: Due Diligence in Data Transfers

Principle	**Legal Reference:** Section 25(h) I Regulation 39-48 of General Regulations A data handler who is a transferring entity shall before transfer personal data out of Kenya ascertain that the transfer is based on (a) appropriate data protection safeguards (b) an adequacy decision made by the Data Commissioner (c) transfer as a necessity (d) consent of the data subject.
Due Diligence in Transfers	Once personal data leaves Kenya, it is no longer protected by the standards set out in the Data Protection Act. Different countries may have weaker (or no) data protection laws or less regulatory oversight. This principle exists to prevent organisations from exposing individuals to weaker standards of data protection.
What it means for your organisation	Many nonprofits use cloud storage, international platforms or work with foreign funders and partners. Before sharing personal data with any of these, you must verify that they have adequate data protection safeguards in place. Data Processing Agreements (DPAs) should be in place with all third-party data handlers.
How the principle can be demonstrated	Your organization can demonstrate this principle by: 1. Mapping data flows to identify every instance where personal data is transferred, stored, or processed outside Kenya. 2. Having data transfer agreements with international partners, donors, or service providers that specify how the data will be protected once transferred.

	3. Obtaining informed consent from data subjects where adequacy safeguards cannot be confirmed. 4. Assessing the data protection practices of any foreign-based software, cloud storage, or platform provider before adopting it. 5. Minimising unnecessary transfers and only sending the specific data needed by an international partner.
Reflection	A non-profit organisation partners with an international research institution to evaluate the impact of its health programme. Before sharing participant information outside Kenya, the organisation verifies that the transfer is necessary, confirms that the receiving institution has adequate measures to protect the data, and ensures that only relevant information required for the research is shared.

5.4.8 Principle 8: Confidentiality, Integrity and availability

Principle Confidentiality, Integrity and availability	**Legal Reference:** Regulation 32 of DPA General Regulations Data must be processed in a manner that ensures it remains secure, accurate, and accessible when needed. Organisations must implement appropriate measures to protect personal data against unauthorised access, disclosure, loss, misuse, alteration, or destruction, while ensuring that authorised individuals can access and use the data for legitimate purposes. The controller shall be responsible for and be able to demonstrate compliance with" all the other principles.
What it means for your organisation	Your organisation must put appropriate technical and organisational measures in place to protect personal data. The measures should be proportionate to the sensitivity of the data and the risks involved.
How the principle can be demonstrated	Your organisation can demonstrate this principle by: 1. Assessing the risks against the security of personal data and putting in place measures to counter identified risks 2. Ensuring only authorised personnel have access to the data necessary for their processing tasks 3. Ensuring transfers are secured against unauthorised access and changes 4. Securing data storage from unauthorised use, access and alterations 5. Protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data 6. Having in place routines and procedures to detect, handle, report, and learn from data breaches 7. Regularly reviewing and testing technical and organizational measures to uncover vulnerabilities.

Reflection	An organisation may use a cloud-based project management tool with different levels of access to beneficiary data. Before uploading any beneficiary data to that platform, the organization will put all implement necessary measures to enhance data security.

5.4.9 Principle 9: Accountability

Principle Accountability	**Legal Reference:** General Data Protection Regulations, Article 5 and Regulation 23 of General Regulations Data handlers must be able to demonstrate compliance with the data protection principles. Accountability is not a standalone action, but the organisation's overall responsibility to demonstrate, that it is upholding the principles. principles through documentation. This principle ensures organisations don't just intend to comply, but they are able to demonstrate compliance.
What it means for your organisation	Your organisation should establish and maintain a comprehensive privacy management programme that governs the entire lifecycle of personal data from the point it is collected until it is securely deleted or anonymised.
How the principle can be demonstrated	A robust accountability programme should include: 1. Clear data protection and information security policies and procedures. 2. Defined roles and responsibilities for handling personal data. 3. Appropriate technical and organisational measures to protect personal data, including access controls and secure systems. 4. Procedures for identifying, reporting, investigating, and managing personal data breaches. 5. Regular privacy risk assessments and, where necessary, Privacy Impact Assessments (PIAs). 6. Staff training and awareness on data protection obligations. 7. Documentation that demonstrates compliance, such as Records of Processing Activities (ROPAs), consent records, data processing agreements, retention schedules, and audit reports. 8. Registration with the ODPC where required, and maintaining evidence of that record
Reflection	When a donor asks a nonprofit to demonstrate how it protects the personal data of beneficiaries collected through its programmes, the organisation should be able to provide documented evidence of its compliance. This may include its data protection policy, records of staff data protection training, completed privacy risk or compliance assessments, and other relevant documentation that demonstrates appropriate safeguards are in place.

5.5 Case Studies: Applying the Principles of Data protection

Case Study 1: Maendeleo Community Based Organisation

Maendeleo CBO runs a programme supporting survivors of domestic violence. It collects participant details through an intake form that asks for name, national ID, phone number, physical address, employment status, number of children, health conditions, and immigration status. The forms are stored in an unlocked filing cabinet. Staff regularly share participant lists via personal WhatsApp accounts with partner organisations abroad. The organisation has never told participants where their data is collected or how long it will be kept. Identify which principles Maendeleo CBO is violating and what they should do differently.

Case Study 2: Pwani Community Based Organisation

Pwani Community Network is a mid-sized CBO based in Kilifi County working across four thematic areas child protection, women's economic empowerment, environmental conservation and community health outreach. The organisation collects personal data from beneficiaries, staff, volunteers and community members across its programmes. It uses a mix of paper-based records and digital tools including a WhatsApp group for staff coordination, Google Forms for beneficiary registration, a shared Google Drive for programme files, and Mailchimp for sending newsletters and programme up.

Using the below follow up prompts, identify what principle is being referred to, the relevant operational gap in line with the principle and how it can be addressed.

1. The organisation uses Google Forms to register beneficiaries for its child protection programme. The form was set up quickly by a programme officer and collects names, ages, school details, household composition and information about the nature of the protection concern. There is no privacy notice attached to the form. Beneficiaries, many of whom are parents or community members with limited digital literacy, do not know their data is being collected by Google, stored on Google's servers, or shared with anyone beyond the CBO.

2. The organisation collects beneficiary contact details (phone numbers and location information) during its women's economic empowerment programme for the stated purpose of sending participants updates about training sessions. Six months later, the programme coordinator shares the same contact list with a partner organisation running a microfinance programme, reasoning that the women would benefit from the loan products on offer.

3. Pwani's environmental conservation programme conducts community surveys to understand land use patterns and deforestation drivers. The survey form which was designed three years ago asks for the respondent's full name, national ID number, phone number, GPS coordinates of their homestead, details of their land holdings, details of any livestock owned, household income range, and whether any household member has been in contact with law enforcement over land disputes. When challenged, the programme officer explains that the organisation has always collected this information and that it helps build a "complete picture" of the community. The actual purpose of the survey is identifying which areas are most at risk of deforestation to inform their advocacy.

4. A community health worker registers a beneficiary, Mary Kadzo in the organisation's health outreach database in 2022 under the name Mary K. Charo with a phone number that has since been changed. In 2024, a new community health worker encounters the same beneficiary and registers her again under "Mary Kadzo" with her current phone number, creating a duplicate record. The two records contain conflicting information about her health status, the interventions she has received, and her household composition. When the programme coordinator prepares a report for the donor on the number of unique beneficiaries reached, Mary is counted twice. When the health team attempts to follow up with her after a referral, they call the wrong number and conclude she has dropped out of the programme.

5. Pwani Community Network CBO has been operating since 2014. Its shared Google Drive contains beneficiary registration forms, case files, community survey responses, medical referral letters and programme reports going back to the organisation's founding year. When a new programme officer joins the women's economic empowerment team, she is given full access to the entire drive including sensitive case files for beneficiaries who last engaged with the organisation in 2016 and who have long since left the programme. Separately, the organisation's Mailchimp list contains 847 contacts a mix of current partners, former donors, community members who attended a single event three years ago and people whose email addresses were added by a former staff member and who have never engaged with any communication. There is no process for removing inactive contacts.

6. Pwani's shared Google Drive is accessible to all 18 staff members and 12 active volunteers with a single shared login. The folder contains everything including a folder of child protection case files with the names, ages, schools and protection concerns of 43 children, a folder of GBV survivor testimonies collected as part of the women's empowerment programme, and a folder of community health records including HIV status information collected during the health outreach programme. A volunteer who joined three months ago to help with social media has the same access as the child protection programme officer.

KEY TAKEAWAYS

1. Principles based vs rule-based understanding- Data protection law which provides for the principles of data protection is not prescriptive but descriptive. The principles highlighted in Section 25 of the Data Protection Act (DPA), 2019 teach you how to think when unexpected field situations occur guiding your decisions even when no specific policy rule applies.

2. Applicable Across the Entire Data Lifecycle- The principles govern personal data from the when it is gathered to the moment it is permanently erased. All the stages of the data lifecycle operate within these legal guardrails.

3. Principles are not abstract concepts. Every paper registration sheet, event attendance list, WhatsApp group, beneficiary database, and photo capture reflects or violates core principles like such as data minimisation, purpose limitation, and transparency.

4. Upholding data principles protects the physical safety, dignity, and trust of the communities you serve. In non-profit operations, broken trust is almost impossible to rebuild.

5.6 Organisational Self-Assessment Checklist

Use this checklist to assess how well your organization currently applies the principles. Tick each item your organisation already does. Items left unchecked become your action priorities.

Right to Privacy and valid explanation

√	Action Item
☐	Our organisation considers the privacy impact before starting any new data collection activity.
☐	We have designated a staff member responsible for data protection oversight.
☐	We do not process personal data in ways that could expose, harm or embarrass a data subject.
☐	When we ask for sensitive or private information, we always explain why it is needed.
☐	The explanation we provide is linked clearly to our organisation's functions.
☐	We do not collect personal or family information out of routine without a clear justification.

Lawfulness, Fairness and Transparency

√	Action Item
☐	We have a privacy notice that we share with data subjects before collecting their data.
☐	Our privacy notice explains what data we collect, why, how it is used, how long it is kept, and who it is shared with.
☐	We have identified a lawful basis for every type of data we process.
☐	We do not process data in ways that discriminate against individuals on any protected ground.

Purpose limitation

√	Action Item
☐	We document the purpose of data collection before we begin collecting it.
☐	We do not repurpose personal data for activities beyond its original stated purpose without informing data subjects.
☐	Our stated purposes are linked to our organisation's mandate and lawful functions.

Data Minimisation

√	Action Item
☐	We have reviewed all our data collection forms and removed fields that are not strictly necessary.
☐	Staff understand why they should not collect more data than is needed.
☐	We conduct periodic reviews to check whether data we hold is still necessary.

Accuracy

√	Action Item
☐	We verify data at the point of collection.
☐	We have a process for data subjects to request corrections to their records.
☐	We conduct regular reviews of our databases to identify and correct outdated or inaccurate entries.
☐	We promptly delete or correct data found to be false or misleading.

Storage Limitation

√	Action Item
☐	We have a written data retention schedule that sets out how long each type of data is kept.
☐	We have a deletion or disposal policy and staff know how to apply it.
☐	We comply with legal minimum retention periods (e.g. employment records — 3 years; business records — 7 years).
☐	We securely delete digital records and physically destroy paper records at the end of the retention period.

Due Diligence in Data Transfers

√	Action Item
☐	We have identified all third parties (cloud platforms, partners, funders) who receive personal data from us.
☐	We have reviewed their data protection policies and confirmed they have adequate safeguards.
☐	We have Data Processing Agreements in place with all third-party processors.
☐	We inform data subjects when their data will be stored or processed outside Kenya.

Confidentiality, Integrity and availability

√	Action Item
☐	We assess the risks against the security of personal data and put in place measures to counter identified risks
☐	We have data protection policies and notices for information security in place.
☐	We have limited access for our personnel to only data necessary for their tasks.

Accountability

√	Action Item
☐	We have kept an updated Record of Processing Activities
☐	We have mapped out data flows within our organization.
☐	We have obtained a registration certificate as a data handler

06.
Lawful Bases for Data Processing

About This Module

Before an organization collects or uses a person's personal information, it must have a valid legal reason for doing so. This legal reason is called a lawful basis. In this module, you will learn what a lawful basis is, why it is important, the lawful bases recognized under the Data Protection Act, 2019, and how to determine which one applies to your organization's activities. You will also learn the consequences of processing personal data without a lawful basis.

6.1 Introduction

Community facing organizations occupy a distinctive position in Kenya's social landscape. They work directly with individuals and communities who are often among the most marginalized, vulnerable, and in need of protection. In carrying out this work, these organizations routinely collect, store, use, and share personal information such as names, contact details, health records, case histories, photographs, testimonies, and much more.

The Data Protection Act, 2019 (DPA) imposes a clear and enforceable legal obligation on all organisations that handle personal information. Before any such information is processed, the organisation must be able to identify and demonstrate a valid legal ground for doing so. That legal ground is referred to as a lawful basis. This obligation is not discretionary but mandatory.

This module provides a comprehensive examination of the lawful basis framework. It covers the legal foundations, the lawful bases available under Kenyan law, the specific obligations that apply to personal data, and the particular challenges that arise when personal data is processed in conditions of vulnerability, necessity, and dependency and circumstances that are directly relevant to much of the work undertaken by community-facing organizations.

Reflective Practice

Identify one specific activity within your organization that involves the collection or use of personal information about community members, beneficiaries, clients, or research participants.
Note the activity and keep it in mind as you work through this module. You will return to it at several points as a practical reference point.
Example activities: beneficiary registration, household surveys, case file management, referral documentation, program evaluation interviews, or the collection of photographs and testimonials.

Objectives

1. To introduce the concept of a lawful basis for processing personal data and explain its importance under the Data Protection Act, 2019.
2. To examine the lawful bases recognized under Kenyan data protection law and the circumstances in which each may be relied upon.
3. To provide practical guidance on selecting the most appropriate lawful basis for different data processing activities within community-facing organizations.
4. To explain the relationship between lawful basis, sensitive personal data, and the rights of data subjects under the Data Protection Act, 2019.
5. To equip organizations with the knowledge needed to identify, justify, and document lawful basis decisions as part of a compliant data protection programme.

6.2 Learning Outcomes

Upon completion of this module, the learners should be able to demonstrate the following;

Outcome	**Demonstrated Competence**
Define lawful basis and identify its legal foundation	articulate the meaning of lawful basis under Section 30(1) of the DPA and explain why it is a prerequisite to any processing activity.
Identify and distinguish the lawful bases	Name and describe each of the lawful bases, with reference to the applicable statutory provision, and identify the distinguishing features of each.
Apply lawful basis analysis to organisational activities	Identify the most appropriate lawful basis for specific data processing activities within their organisation, providing reasoned justification for their selection.

Document lawful basis decisions	Produce a lawful basis entry in a data processing register that is specific, demonstrable, and appropriately accounts for any vulnerability or dependency considerations.
Understand the relationship between lawful basis and data subject rights	Explain how the choice of lawful basis affects the rights available to data subjects, including the right to object and the right to erasure.
Identify sensitive personal data obligations	Recognise when a processing activity involves sensitive personal data and identify the additional conditions that must be satisfied alongside the lawful basis.
Navigate processing in conditions of vulnerability, necessity, and dependency	Apply heightened analytical rigour to lawful basis decisions where data subjects are in conditions that may compromise their capacity for genuine autonomous decision-making.

6.3 What Is Lawful Basis?

Lawful basis refers to the legal ground that authorises a data handler to process personal data. It is the answer to the foundational question that every organisation handling personal information must be able to answer before any processing activity begins which is; on what legal authority is this processing taking place?

A practical analytical framework for applying the lawful basis requirement in organisational contexts involves posing five preliminary questions before any processing activity commences:

Analytical Question	What It Determines
WHO is involved in this processing activity?	Identifies the roles of the organisation (data handler) and the category of data subjects whose information is involved.
WHAT data is to be processed?	Identifies the specific categories of personal data and determines whether this fall within the sensitive personal data classifications.
WHY is this processing taking place?	Establishes the purpose of the processing and provides the foundation for the lawful basis analysis.
WHEN does the processing begin and for how long will it continue?	Determines the temporal scope of the processing and the period for which a lawful basis must be maintained.
WHERE will the data be held and to whom may it be disclosed?	Establishes the geographic and institutional scope of the processing, including any cross-border transfers or disclosures to partner organisations.

Identify sensitive personal data obligations	Recognise when a processing activity involves sensitive personal data and identify the additional conditions that must be satisfied alongside the lawful basis.
Navigate processing in conditions of vulnerability, necessity, and dependency	Apply heightened analytical rigour to lawful basis decisions where data subjects are in conditions that may compromise their capacity for genuine autonomous decision-making.

Organisational Assessment

Apply these five questions to the processing activity you identified at the start of this module. Record your answers in writing. Where you find that you cannot answer a question, or can only answer it partially, note this as an area requiring further assessment before that processing activity commences or continues.

The inability to answer one or more of these questions is not an unusual finding. It pinpoints areas where your organisation's data protection practices require scrutiny.

6.4 The Principle of Lawfulness

The principle of lawfulness is one of the foundational principles of data protection. It requires that personal data be processed only where there is a valid legal justification for doing so. Organizations cannot collect, use, disclose, store, or otherwise process personal data simply because it is useful, convenient, or technologically possible. Every processing activity must be anchored on a recognized lawful basis. Lawfulness is therefore the legal foundation upon which all processing activities are built. Without a lawful basis, the processing is unlawful regardless of how secure, transparent, or beneficial it may be.

6.5 Foundational Considerations

It is important for all data handlers to understand the rules that govern the lawful basis. These rules are not procedural preferences but are legal obligations derived directly from law and shape every decision an organisation makes.

Regulation 5(2) of the Data Protection (General) Regulations, 2021 stipulates that the lawful basis must be established before the processing commences. This requirement is clear; an organisation shall not commence a data processing activity and then look for a justification after the fact. The lawful basis must be identified, assessed and documented before any processing begins.

Non-Profit organisations should identify the most appropriate lawful basis for each purpose they process personal data. They should not rely on multiple lawful bases for the same purpose as a form of legal

fallback. Where different processing activities serve different purposes, different lawful bases may apply. Each purpose should have a clearly identified and documented lawful basis that can be explained to data subjects and demonstrated to regulators.

Statutory Reference

Regulation 5(2), Data Protection (General) Regulations, 2021
Processing under sub regulation (1) shall only rely on one legal basis for processing at a time, which shall be established before the processing.

The legal basis relied on under sub regulation (1) shall always be demonstrable.

Regulation 5(2) further requires that the lawful basis relied upon shall always be demonstrable. This requirement pivots back to the broader principle of accountability under the Act.
An organization must be able to always show, which basis it has relied upon for a given processing activity, the reasons for that choice, and the documentation that supports it. Demonstrability requires written records, not just an internal decision making.

Section 30(2) of the DPA provides that further processing of personal data shall be in accordance with the purpose of collection. Where an organisation has collected personal data for one purpose and subsequently wishes to use it for a different purpose, it must assess whether that further use is compatible with the original purpose. Where it is not, a separate lawful basis must be identified and, in most cases, data subjects must be informed of the new processing purpose.

This is particularly relevant for organisations that collect data through program delivery and subsequently wish to use it for research, advocacy, fundraising, or donor reporting purposes. Each of these secondary uses requires its own processing.

Section 30 (2) Data Protection Act, 2019
Further processing of personal data shall be in accordance with the purpose of collection.

Take Note - Sensitive Personal Data
The Data Protection Act, 2019 designates certain categories of personal data as sensitive. These include data relating to health, race, ethnic origin, religion or belief, political opinion, financial information, genetic and biometric data, and sexual orientation.
The processing of sensitive personal data requires not only a valid lawful basis under Section 30(1), but also specific additional conditions. Both requirements must be satisfied before any processing commences.

Non-Profit organisations working in health, protection, legal aid, human rights, and community development contexts frequently handle sensitive personal data. The obligation to identify a lawful basis and meet the additional conditions specified, must be reflected in all relevant data processing registers and assessments.

6.5 Categories of Lawful Basis Under Section 30(1) of the DPA

Section 30 of the Data Protection Act, 2019 recognises two broad categories of lawful bases for processing personal data: necessity and consent. While consent is a standalone lawful basis, the necessity category comprises several lawful bases where processing is permitted because it is necessary for a particular legal, contractual, public, or legitimate purpose.

The lawful bases under the necessity category are:

1. Performance of a contract to which the data subject is a party.
2. Compliance with a legal obligation to which the data controller or data processor is subject.
3. Protection of the vital interests of the data subject or another person.
4. Performance of a task carried out in the public interest or in the exercise of official authority.
5. Pursuit of the legitimate interests of the data controller or a third party, provided those interests are not overridden by the rights and freedoms of the data subject.

6.5.2 Performance of a Contract

Section 30(1)(b)(i), Data Protection Act, 2019
The processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract.

The lawful basis of performance of a contract permits the processing of personal data where such processing is objectively necessary to fulfil a contractual relationship with the data subject or to take steps requested by the data subject before entering that relationship.

This basis recognizes that many interactions between individuals and organizations are founded upon contractual arrangements. In such circumstances, the processing of certain personal data is indispensable to enabling the parties to perform their respective rights and obligations. Without the processing, the contract could not be entered, administered, or fulfilled.

The key consideration is necessity. The processing must be genuinely required for the performance of the contract. It is not sufficient that the processing is useful, convenient, desirable, or beneficial to the organization. If the contractual purpose can reasonably be achieved without processing the personal data in question, this lawful basis may not apply.

For example, where an individual applies for employment, the organization may need to collect and process identification information, contact details, academic qualifications, banking information, tax information, emergency contact details, and payroll records to establish and administer the employment relationship. Similarly, where a consultant or contractor is engaged, the organization may need to process personal information necessary for onboarding, payment, communication, performance management, and contract administration.

Processing Prior to Contract Formation

This lawful basis is not limited to the performance of an existing contract. It also extends to processing that is necessary to take steps at the request of the data subject before entering into a contract.

For example:

- Reviewing a job application submitted by a prospective employee;
- Assessing an application for membership in an association;
- Evaluating an application for a grant or scholarship programme;
- Processing an application for a loan or financial assistance;
- Conducting due diligence requested by a prospective consultant or service provider.

In these situations, the processing is undertaken because the data subject has initiated a request that may lead to a contractual relationship.

Practical Examples

Processing Activity	Why Contractual Necessity Applies
Collecting bank details of employees	Necessary to pay salary
Collecting consultant tax information	Necessary to process payments and administer the engagement
Reviewing job applications	Necessary to assess suitability before entering employment
Maintaining membership records	Necessary to administer membership rights and obligations
Processing beneficiary applications for a funded programme	Necessary to determine eligibility and provide programme related services

Performance of a Contract Checklist

Question	YES/NO
Has the individual asked the organization for a service, benefit, membership, employment opportunity, or other engagement?	
Does the organization need the personal data to provide that service or fulfil that engagement?	
Would it be difficult or impossible to provide the service without the personal data?	
Is the organization only collecting information that is needed for that purpose?	
Is the processing directly connected to what the individual has requested?	
Can the organization explain to the individual why the information is needed?	

Performance of a Contract Checklist Quick Test:

Ask yourself:

"Do we need this information in order to provide what the person has asked for?"

- If yes, contractual necessity may apply.
- If No, another lawful basis should be considered.

6.5.3 Compliance with a Legal Obligation

Section 30(1)(b)(ii), Data Protection Act, 2019

The processing is necessary for compliance with any legal obligation to which the controller is subject.

The lawful basis of compliance with a legal obligation permits the processing of personal data where such processing is necessary for an organization to comply with a legal requirement imposed upon it by law. This basis recognizes that organizations are often required by legislation, regulations, court orders, regulatory directives, or other legally binding instruments to collect, use, retain, disclose, or otherwise process personal data.

The key consideration is, once again, necessity. The processing must be genuinely required to enable compliance with a specific legal obligation. It is not sufficient that the processing is merely useful, prudent, or aligned with good practice. There must be a clearly identifiable legal requirement that necessitates the processing activity.

An organization relying on this basis should be able to identify the precise legal provision, regulatory requirement, or court order giving rise to the obligation and demonstrate the connection between that obligation and the processing being undertaken. A vague belief that "the law requires it" or that "it is standard practice" will not be sufficient.

Sources of Legal Obligation

Legal obligations may arise from a variety of sources, including:

- Acts of Parliament;
- Subsidiary legislation and regulations;
- Employment laws;
- Tax laws;
- Anti-money laundering and counter-terrorist financing requirements;
- Charity and non-profit regulatory obligations;
- Court orders and judicial directives;
- Regulatory notices and directives issued by competent authorities;
- Health and safety requirements;
- Reporting obligations imposed by funding or oversight bodies where mandated by law.

Practical Examples

Processing Activity	Why Legal Obligation Applies
Maintaining employee payroll records	Required by employment and tax laws
Deducting and remitting statutory taxes	Required by tax legislation
Retaining financial records and supporting documentation	Required by financial and accounting laws
Disclosing information pursuant to a court order	Required by judicial directive
Responding to requests from regulators	Required by applicable regulatory framework
Maintaining statutory organizational records	Required by laws governing non-profit entities

Quick Test:

Ask yourself:

"Do we need this information in order to provide what the person has asked for?"

- If yes, contractual necessity may apply.
- If no, another lawful basis should be considered.

Transparency Obligations in Vulnerable Contexts

Good Practice: Informing Data Subjects of Mandatory Disclosure Obligations
Where an organization provides services to individuals in vulnerable circumstances including survivors of violence, persons seeking legal protection, or children those individuals may share sensitive personal information with a reasonable expectation of confidentiality.

Where the organization is subject to any legal obligation that may require the disclosure of information shared by clients such as mandatory reporting obligations in child protection contexts; data subjects must be informed of these obligations at the point of data collection, before they choose what to share.

Transparency regarding the limits of confidentiality is both a legal obligation and a fundamental ethical responsibility in community and social work practice.

6.5.3 Compliance with a Legal Obligation

Section 30(1)(b)(ii), Data Protection Act, 2019
The processing is necessary for compliance with any legal obligation to which the controller is subject.

The lawful basis of compliance with a legal obligation permits the processing of personal data where such processing is necessary for an organization to comply with a legal requirement imposed upon it by law. This basis recognizes that organizations are often required by legislation, regulations, court orders, regulatory directives, or other legally binding instruments to collect, use, retain, disclose, or otherwise process personal data.

The key consideration is, once again, necessity. The processing must be genuinely required to enable compliance with a specific legal obligation. It is not sufficient that the processing is useful, prudent, or aligned with good practice. There must be a clearly identifiable legal requirement that necessitates the processing activity.

An organization relying on this basis should be able to identify the precise legal provision, regulatory requirement, or court order giving rise to the obligation and demonstrate the connection between that obligation and the processing being undertaken. A vague belief that "the law requires it" or that "it is standard practice" will not be sufficient.

Sources of Legal Obligation

Legal obligations may arise from a variety of sources, including:

- Acts of Parliament;
- Anti-money laundering and counter-terrorist financing requirements;
- Charity and non-profit regulatory obligations;
- Court orders and judicial directives;
- Regulatory notices and directives issued by competent authorities;
- Health and safety requirements;
- Reporting obligations imposed by funding or oversight bodies where mandated by law.

Ask yourself:

- Is there a specific law, regulation, or legally binding requirement that requires us to process this personal data?
- Is the processing necessary to comply with that legal obligation?
- Can we identify the legal provision or regulatory requirement that requires the processing?
- If yes, the lawful basis of compliance with a legal obligation is likely to apply.
- If No, this lawful basis should not be relied upon, and another lawful basis should be considered.

Transparency Obligations in Vulnerable Contexts

Good Practice: Informing Data Subjects of Mandatory Disclosure Obligations
Where an organization provides services to individuals in vulnerable circumstances including survivors of violence, persons seeking legal protection, or children, those individuals may share sensitive personal information with a reasonable expectation of confidentiality.

Where the organization is subject to any legal obligation that may require the disclosure of information shared by such individuals such as mandatory reporting obligations in child protection contexts; data subjects must be informed of these obligations at the point of data collection, before they choose what to share.

Transparency regarding the limits of confidentiality is both a legal obligation and a fundamental ethical responsibility in community and social work practice.

A legal obligation must arise from a law, regulation, court order, or other legally binding requirement. Internal policies, contractual commitments, donor requirements, or organisational preferences do not, by themselves, constitute a legal obligation for the purposes of this lawful basis.

6.5.3 Exercise of Public Nature Functions

Section 30(1)(b)(vi), Data Protection Act, 2019
The processing is necessary for the exercise, by any person in the public interest, of any other functions of a public nature.

The lawful basis of exercise of public nature functions permits the processing of personal data where such processing is necessary for the exercise, by any person in the public interest, of any functions of a public nature. This ground may apply to nonprofit organisations that carry out functions of a genuinely public character in the public interest.

The key consideration is the nature of the function itself. The function must be genuinely of a public character, one that, in a different institutional context, might be discharged by a public body. It is not sufficient that the organisation serves a broadly beneficial or social purpose. The distinction lies in the character of the function, not its social utility. Processing that is incidental, convenient, or beneficial to the organisation's operations will not satisfy this standard.

For example, where an organisation operates a community legal aid programme, conducts systematic human rights monitoring and documentation, carries out public health outreach and education, or undertakes evidence-based advocacy on issues of public concern, it may be exercising functions of a public nature even though it is not itself a government body. Similarly, investigative journalism conducted in the public interest may fall within this basis where the processing of personal data is genuinely required to fulfil that journalistic function.

This basis does not apply to general programme delivery, service provision, or organisational administration because those activities serve the public good. The function must have an identifiable public character that goes beyond the organisation's internal purposes. Organisations should be prepared to identify and articulate the specific public function being exercised and to demonstrate why processing the relevant personal data is necessary to discharge it.

Functions that may qualify as public in nature include:

- Community legal aid services providing access to justice for individuals who would otherwise be unable to obtain legal representation;
- Systematic human rights monitoring, documentation, and reporting conducted in the public interest;
- Investigative journalism undertaken in the public interest, where processing is necessary to investigate and report on matters of genuine public concern;
- Public health outreach and education programmes that substitute for or supplement public health functions of the state;

Evidence-based advocacy and policy engagement on matters of public concern, where personal data underpins the research or documentation required to advance that advocacy.

Public Nature Functions Checklist

Question	YES/NO
Can the organisation identify a specific function of a genuinely public character that it is exercising?	
Is that function one that a public body might discharge in a different institutional context?	
Is the processing genuinely necessary to discharge that function, rather than it useful or convenient?	
Is the processing being carried out in the public interest, rather than for the organisation's own commercial or internal purposes?	
Can the organisation explain and document why this specific processing is necessary to carry out the identified public function?	

Good Practice: Public Nature Functions and Proportionality
Where this basis is relied upon to process the personal data of individuals in vulnerable circumstances including persons in conflict with the law, refugees and asylum seekers, survivors of human rights violations, or individuals accessing community legal aid the principle of proportionality and data minimization must be applied.

Collect only the personal data that is demonstrably necessary for the identified public function. The breadth of the function does not justify the breadth of the data collection.

Where the processing involves information that could create safety risks for the individuals concerned such as data relating to human rights defenders, informants, or witnesses, specific security safeguards must be in place before any processing activities.

6.5.7 Legitimate Interests

Legitimate interest means having a valid and reasonable reason for using someone's personal data. An organisation may use personal data where it has a genuine need to do so, if the use is fair and does not negatively affect the individual's rights and privacy.

It means that an organisation has a good reason to use this information, and it is fair to the person whose information it is.

Legitimate interests is the most flexible of the lawful bases and may be relied upon in a broad range of operational contexts. It is also the most analytically demanding, as it requires a structured assessment that includes a genuine balancing of the organisation's interests against those of the data subjects concerned.

Section 30(1)(b)(vii), Data Protection Act, 2019
The processing is necessary for the legitimate interests pursued by the data controller or data processor or a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject.

It permits the processing of personal data where the controller, processor, or a third party has a legitimate interest in the processing, that interest is necessary for the processing to take place, and the interest is not overridden by the rights and freedoms or legitimate interests of the data subject. Unlike most other lawful bases, this ground does not depend on the consent of the data subject or the performance of a specific legal or contractual obligation. Instead, it requires the organisation to conduct and document a structured three-part assessment.

The Three-Part Legitimate Interests Assessment

Reliance on legitimate interests requires the organisation to conduct and document a structured three-part assessment before processing commences:

Stage	The Assessment Required	What Documentation Should Record
1. Purpose Test	Does the organization have a genuine, specific, and clearly articulated legitimate interest in the processing? The interest must be real and identifiable, not vague, aspirational, or framed in terms of general organisational benefit.	A clear statement of the specific legitimate interest pursued, distinguishing it from institutional convenience.

2. Necessity Test	Is the processing of personal data necessary to pursue that legitimate interest? Could the same purpose be achieved without processing this data, or through less privacy-intrusive means?	An explanation of why the processing is necessary, and a statement that no less intrusive means of achieving the same purpose is available.
3. Balancing Test	Do the organisation's legitimate interests outweigh the rights, freedoms, and interests of the data subjects? This requires a genuine weighing of the potential impact on data subjects against the identified interest.	A documented balancing analysis that considers the nature of the data, the reasonable expectations of data subjects, and any factors that increase the weight of data subjects' interests including conditions of vulnerability, necessity, or dependency.

This basis cannot be used as a catch-all justification for any processing the organisation finds convenient. The assessment must be genuine, documented, and revisited where circumstances change. The basis is not available where a more specific lawful basis applies, and it should not be used to circumvent the requirements of other grounds.

Where the processing relates to vulnerable individuals or involves sensitive personal data, the balancing test will be weighted more heavily in favour of the data subjects and additional care must be taken. In such cases, the organisation should consider whether other safeguards or alternative lawful bases are more appropriate.

Practical Examples

Processing Activity	Why Legitimate Interests May Apply
Retaining contact details of former programme participants for follow-up or impact evaluation	Organisation has a legitimate interest in measuring programme impact; retention is necessary and participants would reasonably expect it
Sharing a donor's basic details with a partner organisation co-implementing a programme	Legitimate interest is in programme delivery; sharing is necessary and the intrusion is limited; balancing favours processing
Maintaining an internal fraud prevention register of individuals who have misrepresented their eligibility	Legitimate interest is in protecting programme integrity; retention is necessary and proportionate; balancing assessment should be documented
Processing employee performance records for internal management purposes beyond contractual requirements	Legitimate interest in effective workforce management; balancing assessment must consider employee privacy expectations

Legitimate Interests Checklist

Question	YES/NO
Can the organisation identify a specific, lawful, and genuine interest in carrying out the processing?	
Is the processing necessary to achieve that interest, and could the same goal be achieved with less personal data?	
Have the rights, freedoms, and legitimate interests of the data subjects been genuinely considered and weighed?	
Does the processing cause harm, prejudice, or unwarranted intrusion that outweighs the organisation's interest?	
Has the organisation documented its balancing assessment in writing?	

Legitimate Interests in Conditions of Vulnerability, Necessity, and Dependency

The balancing test under legitimate interests carries heightened significance and complexity in non-profits and community contexts. Where an organisation processes information of data subjects in conditions of vulnerability, necessity, or dependency, their rights and interests carry greater weight in the balance.

The Elevated Weight of Data Subjects' Interests in Vulnerable Contexts
The balancing test is not a formality. It requires an honest and contextualized assessment of the potential impact of processing of data relating to the specific individuals concerned.
Where data subjects are dependent on the organization for essential services, the potential for processing to cause harm including harm arising from stigma, surveillance, discriminatory use of information, or breach of confidentiality is typically elevated. This increases the weight of their interests in the balance.

An organisation cannot satisfy the balancing test simply by asserting that its program or administrative interests in processing the data are legitimate and significant. It must also show, by reference to the specific circumstances of the data subjects concerned, that the harm that processing may cause to them, does not outweigh those interests

Where the balancing test does not clearly favour the organisation, legitimate interests cannot be relied upon as a lawful basis for that processing activity.

Good Practice: Documenting the Legitimate Interests Assessment

1. Document the specific legitimate interest clearly and in concrete terms before processing begins.
2. Document the necessity analysis, explaining why the same purpose cannot be achieved with less data or through less intrusive means.
3. Document the balancing test, identifying the specific rights and interests of the data subjects, and explicitly addressing any vulnerability, necessity, or dependency conditions that increase the weight of those interests.

Review the documented assessment whenever the circumstances of the data subjects change materially, or when the processing activity is modified.

Reflective Practice

If legitimate interests is a potential basis for the processing activity you identified at the start of this module, work through the three-part assessment now.

Can you identify a specific, genuine legitimate interest? Is the processing necessary for it? When you conduct the balancing test and considering any vulnerability or dependency conditions do your organisation's interests prevail?

Record your analysis. This documentation is the foundation of your demonstrability obligation under Regulation 5(2).

6.5.8 Historical, Statistical, Journalistic, Literary, Artistic, and Scientific Research

Section 30(1)(b)(viii), Data Protection Act, 2019

The processing is necessary for the purpose of historical, statistical, journalistic, literature and art or scientific research.

The lawful basis of research purposes authorises the processing of personal data where that processing is necessary for a genuine research purpose falling within one of the categories recognised by the Act: historical, statistical, journalistic, literary and artistic, or scientific research. This basis reflects the recognised social value of research and the need for organisations engaged in research activities to be able to process personal data in support of those activities.

The key consideration is that the research purpose must be clearly defined and is connected to the processing activity. It is not sufficient that the organisation has a general interest in gathering information or improving its programmes. The research must be structured and purposeful, and the personal data processed must be necessary for it. This basis does not extend to the collection of personal data for general organisational purposes under the label of research.

For example, where an organisation systematically collects data on the characteristics and outcomes of programme participants for the purpose of evaluating programme effectiveness, or where it documents and analyses individual cases to produce statistical evidence in support of policy advocacy, this basis may apply. Similarly, it may extend to human rights documentation, public health research, and investigative journalism where the processing is necessary to the journalistic or research activity.

This basis applies only to the specific categories of research identified in the Act. Routine programme administration, general monitoring, or data collection for internal reporting purposes will not ordinarily qualify, even if those activities produce information that is useful to the organisation. Where this basis is relied upon, the organisation should be prepared to articulate the research purpose, demonstrate how the processing is connected to it, and show that data minimisation principle has been applied.

Research activities that may fall within this basis include:

- Systematic community research or programme monitoring and evaluation, where personal data is collected and analysed to produce evidence of programme outcomes;
- Human rights documentation involving the recording and analysis of individual cases for the purposes of producing statistical or historical evidence;
- Investigative journalism where the processing of personal data is necessary to investigate and report on a matter of public concern;
- Public health research involving the collection and analysis of data on health outcomes or the reach and effectiveness of health interventions;
- Evidence-based policy advocacy grounded in research that requires individual-level data to produce reliable statistical findings.

Practical Examples

Processing Activity	Why Research Purposes Apply
Collecting and analysing participant outcome data for a programme evaluation study	Necessary for a defined statistical research purpose; personal data is required to produce reliable outcome evidence
Recording individual human rights cases to build an evidence database for reporting	Necessary for historical and statistical research; processing is directly connected to the documented purpose
Processing personal details of research participants as part of a public health research study	Necessary for scientific research; data is used to produce findings that inform public health practice

Research Purposes Checklist

Question	YES/NO
Does the processing relate to a genuine research purpose falling within one of the categories in Section 30(1)(b)(viii)?	
Is the research purpose clearly defined and documented, rather than asserted?	
Is the processing of personal data connected to and necessary for the identified research purpose?	
Has data minimisation been applied, so that only the data necessary for the research is collected and retained?	

Research in Conditions of Vulnerability, Necessity, and Dependency

Research involving populations in vulnerable or marginalized circumstances carries elevated ethical and legal responsibilities. Non-profit organisations conducting research with displaced communities, survivors of violence, persons living in poverty, children, persons with disabilities, or members of other at-risk groups must apply a correspondingly heightened standard of care in the design, conduct, and dissemination of that research.

Research with Vulnerable and Dependent Populations: Critical Considerations
The voluntary character of research participation is fundamentally compromised where participants are in an ongoing service or support relationship with the researching organization. The dependency dynamic even where no explicit linkage is made between participation and continued service access may create sufficient pressure to undermine voluntariness.

Incentives or benefits provided in connection with research participation, particularly in contexts of material hardship, may create conditions of necessity that similarly compromise voluntariness. Anonymisation and pseudonymisation of personal data should be implemented at the earliest practicable stage of the research process and not reserved until the point of publication.

Research protocols involving vulnerable or at-risk populations should incorporate independent ethical review wherever this is practicable.

Publication of research findings must be approached with care to ensure that individuals cannot be identified, even in aggregated or anonymized data sets.

Good Practice: Ethical Research in Community Contexts
Apply the principle of do no harm as a foundational principle governing all stages of research design, data collection, analysis, storage, and dissemination.

Where the researching organisation also provides services to research participants, take structural measures to separate the research relationship from the service relationship, including, where practicable, using a different individual to conduct research engagement than the one responsible for service delivery.

Communicate clearly and specifically with research participants regarding the purposes of data collection, the identities of those with access to the data, retention periods, and the rights available to participants including the right to withdraw at any time without consequence.

Apply data minimization rigorously throughout the research process. Collect only the personal data that is necessary to meet the stated research purpose.

6.5.4 Protection of Vital Interests

Section 30(1)(b)(iii), Data Protection Act, 2019
The processing is necessary to protect the vital interests of the data subject or another natural person.

This basis is reserved for circumstances in which the processing of personal data is necessary to protect the life or immediate physical safety of the data subject or another individual. It is characterized by the presence of an imminent and serious threat that cannot be addressed through other means. As such, it is a narrow and exceptional lawful basis and should not be relied upon as a general justification for processing the personal data of vulnerable individuals or beneficiaries.

Given its limited scope and the specific considerations that apply to its use, the vital interests basis will be examined in greater detail in a subsequent module dedicated to special and exceptional circumstances of processing.

6.5.1 Consent

Consent is one of the lawful bases available for the processing of personal data under the Data Protection Act and is often the most widely recognized by data subjects and organisations alike. However, consent is frequently misunderstood and incorrectly applied. Its validity depends on the satisfaction of specific legal requirements and cannot be assumed because an individual has signed a form, ticked a box, or accepted a general clause within a registration document. Given its significance and the complexities surrounding its use, consent will also be examined in greater detail in the next module.

Section 30(1)(a) Data Protection Act, 2019
A data controller or data processor shall not process personal data unless the data subject consents to the processing for one or more specified purposes.

Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to them.

KEY TAKEAWAYS

1. A lawful basis is not optional – Processing personal data without an identifiable lawful basis is a criminal offence under the Data Protection Act, 2019. This is a legal requirement, not a best-practice suggestion.
2. The decision must come first, and it must be documented – A lawful basis is selected before processing begins, not justified after the fact. Being able to show your reasoning is as important as the reasoning itself.
3. Consent is one option among eight, not the default – The law recognises eight distinct lawful bases. Consent is frequently the wrong choice in conditions of vulnerability or dependency.
4. Sensitive data demands an extra step – Beyond identifying a general lawful basis, processing sensitive personal data requires satisfying an additional condition, reflecting the heightened risk it carries.

ASSESSMENT

Part A: Knowledge and Conceptual Understanding

1. What does "lawful basis" mean, and why is it required before personal data can be processed?
2. Name three of the eight lawful bases recognised under Section 30 of the Data Protection Act, 2019.
3. What happens under Section 30(3) of the Act if personal data is processed without a lawful basis?

Part B: Applied Analysis

1. A community organisation collects the names and phone numbers of beneficiaries to deliver food aid. Which lawful basis would most likely apply, and why?
2. An NGO shares a donor's contact details with a partner organisation without informing the donor. Identify the lawful basis question this raises and explain what the organisation should have done first.
3. A researcher collecting data from survivors of gender-based violence is also their support worker. What risk does this create for the voluntariness of any consent given?

Part C: Organisational Reflection

1. Pick one data processing activity your organisation carries out. Which lawful basis applies to it, and how do you know?
2. Does your organisation keep a record of which lawful basis applies to each processing activity? If not, what would you need to start doing to keep one?

07.
Consent and Vital Interests as Lawful Basis

About This Module

This module examines consent and vital interests as a lawful basis for processing personal data under Kenya's Data Protection Act, 2019. Learners will learn how to obtain and manage valid consent, protect the rights of vulnerable populations, and make lawful decisions during emergencies where consent cannot be obtained. The module provides practical guidance on consent management, emergency decision-making, accountability, and post-incident compliance.

7.1 Introduction

This module provides a practical and structured examination of consent and vital interests as lawful bases for processing personal data under the Kenya's Data Protection Act 2019. It positions the basis not only as legal concepts but as operational tools that guide how organisations make responsible data decisions in different situations. It also explores how organisations can obtain, manage consent, and how to make lawful decisions in situations where consent cannot be obtained.

Learners will build a working understanding of how to obtain, assess, and manage valid consent, with attention to power imbalances and protection of vulnerable persons. The module further addresses scenarios where consent is not feasible, such as emergencies, and outlines how vital interest as a basis can be applied to support timely and lawful decision-making while safeguarding individual rights.

Understanding when to rely on consent and when vital interests apply is essential for protecting individuals' rights, maintaining trust, and ensuring ethical, people-centred service delivery especially within the non-profit operations.

7.2 Objectives

By the end of this module, learners will be able:

1. To explain the legal requirements for valid consent under Sections 30–32 of the DPA

2019 and the Data Protection (General) Regulations 2021.

2. To design and implement a consent management framework covering collection, documentation, storage, renewal, withdrawal, expiry and data sharing with third parties.
3. To identify the specific risks to consent when working with vulnerable populations and apply appropriate safeguards.
4. To apply a layered notice approach to consent communication in low-literacy and resource-constrained environments.
5. To recognize thresholds for invoking vital interests under Section 30(1) of the DPA 2019.
6. To apply a structured emergency decision-making framework, document justifications, and transition back to a consented processing regime post-incident.

7.3 Learning Outcomes

By the end of the session, learners will be able to demonstrate these competencies:

Processing Activity	Why Research Purposes Apply
Define and explain valid consent and vital interest	Explain the elements of valid consent and vital interests. Learners should learn to demonstrate and distinguish when to rely on valid consent versus vital interest
Identify consent and its risks in different settings	Assess consent risks in vulnerable settings, document emergency processing decisions and apply appropriate safeguards.
Understand and apply basic consent throughout its life cycle	Manage consent throughout its lifecycle and ensure compliance when sharing data with partners and third parties. Apply the different layered notice approach when obtaining consent in resource constrained and low literacy level settings
Recognize when to invoke vital interest	Identify and distinguish thresholds for invoking vital interests.
Understand and apply post-incidence compliance	Apply and conduct a post-incident compliance action after obtaining consent.

7.4: Consent

7.4.1 Legal Foundation: Consent Under the DPA 2019

Consent forms one of the primary legal bases under the Data Protection Act, 2019. It represents a direct expression of an individual's control over how their personal data is collected, used, and shared. Within the data protection framework, consent is a safeguard designed to ensure that data subjects can participate in decisions affecting their personal data.

Non-profit organisations are obligated as data controllers or data processors to process personal data lawfully, which requires establishing a valid legal basis before any processing activity begins. Consent is one of the six lawful bases available under Section 30(1) of the DPA 2019.

Statutory Reference: Section 30(1)(a) & Section 31, DPA 2019
A data controller may process personal data where the data subject has given consent. Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or clear affirmative action, signify agreement to the processing of personal data relating to them.

7.4.2 Disclosure Obligations When Relying on Consent

Disclosure obligations refer to the requirement for organisations to provide clear, accurate, and accessible information to data subjects before obtaining their consent to process personal data. This ensures that consent if informed by equipping individuals with a full understanding of what data is being collected, the purpose of processing, how the data will be used or shared, and potential risks involved.

Without adequate disclosure, consent cannot be met and may therefore be considered invalid under section 32 of the DPA 2019. For non-profits with programs involving communities, staff and volunteers, the organisation must inform the data subjects of the following before obtaining consent:

- The purpose of each processing operation for which consent is sought.
- The type of personal data to be collected and used.
- The identity of the data controller or data processor.
- Information about the use of personal data for automated decision-making, where relevant.
- The possible risks of data transfers in the absence of an adequacy decision or appropriate safeguards.
- Whether the personal data will be shared with third parties and, if so, with whom.
- The right to withdraw consent at any time.
- The implications of providing, withholding, or withdrawing consent.

7.4.3 Conditions for Valid Consent

The Data Protection (General) Regulations 2021 under regulation 4.3 prescribes the conditions that must be met for consent to be legally valid. It is important for non-profit organisations to understand what these requirements mean in practice. The key conditions are outlined below.

Condition	What This Means in Practice
Capacity	The data subject has the legal and mental capacity to give consent. In the case of a minor or a person who is mentally incapacitated, a legal guardian or authorized representative must consent on their behalf.
Voluntariness	Consent is freely given and not coerced. Services must not be conditional on consent where consent is not strictly necessary for the delivery of the service.
Specificity	Consent is obtained for each distinct processing purpose. A single approval covering multiple unrelated uses is not valid.

Explicit and Informed	The data subject is clearly told what personal data is being collected and the extent to which it will be processed before giving consent.
Unambiguous	Consent involves an affirmative action, and a declaration confirming the data subject has been duly informed. It is important to note that pre-ticked boxes or silence do not constitute consent.
Documented	The date, time, identity, and signature or equivalent of the data subject are recorded. Documentation proving consent was obtained must be retained.

7.4.4 Permitted Methods of Obtaining Consent

Regulation 4.2 of the Data Protection (General) Regulations 2021 permits various methods of obtaining consent, recognizing that non-profits operate in diverse environments. The permitted methods include the following:

- Written forms or notices (signed or initialized).
- Digital consent forms (with audit trail of completion).
- Oral statements, if these are independently witnessed and documented in parallel.
- Audio or video messages provided the content of the message meet all disclosure requirements.

7.4.5 Consent Under Conditions of Vulnerability, Necessity, and Dependency

Non-profit organizations in Kenya frequently serve populations whose circumstances may compromise the voluntariness of consent. These include refugees and internally displaced persons, survivors of gender-based violence, children and unaccompanied minors, communities dependent on humanitarian assistance, and communities with low literacy levels. Persons in these situations may have limited bargaining power, face economic hardship, or depend on the organization for essential services, making it more difficult for them to exercise genuine choice.

Power imbalances are a structural risk. When individuals believe that refusing or withholding consent will affect their access to essential services, consent cannot be considered freely given, regardless of how the consent form is worded.

7.4.6 Safeguards for Vulnerable Populations

Non-profits must implement additional safeguards when collecting consent from or on behalf of vulnerable individuals. The table below has a list of vulnerable populations, the types of risk they are likely to be exposed to and the required safeguard to address the risk for non-profits. This list of vulnerable populations is not exhaustive, and the listed categories have been borrowed from the defined vulnerable groups in Article 21of the Constitution of Kenya

Population	Specific Risk	Required Safeguard
Minors	Cannot legally consent; guardians may have conflicting interests.	Obtain consent from a legal guardian or authorized representative.
Refugees and IDPs	Fear of data sharing with authorities or armed actors.	Provide explicit, clear assurances about who the data will and will not be shared with. Avoid data collection that is not operationally necessary.
GBV Survivors	Risk of re-traumatisation; safety risks if data is disclosed.	Apply strict data minimization. Obtain specific consent for any sharing. Apply do-no-harm principles.
Low-literacy Populations	Cannot meaningfully understand written forms.	Use pictorial notices, translated verbal explanations, and witnessed oral consent with documentation. Ensure interpreters do not have a conflict of interest.
Persons with Disabilities	Inaccessible information, communication barriers, and potential undue influence may prevent informed and voluntary consent.	Provide information in accessible formats and offer reasonable accommodations (e.g., sign language, Braille, large print, or assistive technologies). Obtain consent directly from the individual wherever possible or a legal representative as deemed necessary.
Humanitarian Aid Recipients	Perceived conditionality between consent and aid.	Explicitly communicate in understandable language that service access is not conditional on consent. Document this communication.
Older Members of the Society	Cannot meaningfully understand written forms and will need another party to assist in interpretation	Use pictorial notices, translated verbal explanations, and witnessed oral consent with documentation. Ensure interpreters do not have a conflict of interest.

7.4.7 Consent Management Framework

The accountability principle under Section 25 of the DPA 2019 requires data handlers to be able to demonstrate compliance at any time. For consent, this means establishing clear, documented processes for obtaining, recording, storing, reviewing, and withdrawing consent.

A robust consent management framework must be embedded across the entire programme lifecycle, from design to closure. For non-profits, this framework should address the following:

a) how consent is obtained in different field contexts (written, oral, or digital),
b) how consent decisions are recorded and stored securely,
c) how consent is reviewed and renewed when programmes change or expand,

d) how consent withdrawals are received, processed, and communicated to downstream partners,
e) how consent records are retained or destroyed upon expiry.

The framework must also allocate clear responsibilities designating who within the organisation is accountable for consent management at each stage and ensuring that all staff and volunteers receive adequate training on their obligations.

CHECKLIST EXERCISE: Consent Management for Non-Profit Programs

This checklist is to be completed by the designated person before launching any data collection activity and reviewed at six-month intervals. Retain completed checklists as compliance evidence for audit purposes.

Ref	Checklist Item	Status / Notes
A1.1	GOVERNANCE & POLICY A data protection and privacy policy has been established and is accessible to all staff.	In place Draft Not yet Date adopted: _____
A1.2	A named individual has been assigned responsibility for data protection oversight (DPO or equivalent).	Assigned Name & role: _____
A1.3	Standardised consent forms and privacy notices have been developed and reviewed against DPA 2019 requirements.	Reviewed In progress (Date last reviewed): _____
A2.1	ETHICAL PROGRAMME DESIGN Power imbalances and vulnerability risks have been identified for the target population.	Assessed Not yet Risks identified: _____
A2.2	Programme services are not conditional on consent that is unnecessary for service delivery. An alternative service pathway exists.	Yes Under review
A2.3	Consent forms and privacy notices are available in relevant local languages and in accessible formats.	Available in relevant Languages: _____ Available in accessible formats: _____
A3.1	OPERATIONAL PRACTICES Consent forms use clear, plain language. Technical and legal terms are explained or avoided.	Yes Needs revision
A3.2	All required consent record elements are captured (date, time, purpose, categories of data, data subject identity, staff identity, signature).	All elements Partial Missing: _____
A3.3	Consent records are stored securely (digital: access-controlled; physical: locked cabinet) with defined retention periods.	Secure Partially Retention period: _____

A4.1	PARTICIPANT RIGHTS A simple, accessible consent withdrawal mechanism is in place and communicated to data subjects at the time of obtaining consent.	Yes Not yet Mechanism: _____
A4.2	Staff know how to process a withdrawal request and who to notify, including downstream partners.	Trained Not yet
A4.3	Data subjects are provided with a named contact point for questions, corrections, or complaints about their data.	Yes Not yet Contacted: _____
A5.1	DATA SHARING WITH PARTNERS All data sharing with partners is governed by a written Data Sharing Agreement or Data Processing Agreement.	All covered Gaps Missing partners: _____
A5.2	Original consent forms disclosed that data would be shared with the relevant partner categories.	Disclosed Not disclosed (re-consent required)
A5.3	Downstream partners have been instructed on consent limitations and have confirmed compliance in writing.	Confirmed Pending
A6.1	MONITORING & ACCOUNTABILITY Consent practices are reviewed at least every six months or when programme activities change.	Scheduled Next review date: _____
A6.2	Privacy notices and consent forms are updated when data users, partners, or processing activities change.	Process in place ☐ Not yet
A6.3	Periodic audits of data use are conducted to verify data is being processed only for consented purposes.	Scheduled Not yet Last audit: _____

Completed by: _____

Role: _____ Date: _____

Reviewed by Senior Management: _____

Date: _____

7.4.8 Consent Recording: Minimum Required Elements

When collecting or recording consent for non-profits there are minimum requirements needed. Each consent record must contain, at minimum:

- Date, time, and location of consent.
- The specific purpose(s) for which consent was given.
- The categories of personal data to be collected and processed.
- The identity of the data subject (name and unique programme ID).

- The identity of the person who obtained the consent (staff name and role).
- Signature, thumbprint, or other affirmative indicator from the data subject.

In cases of third-party consent (guardian/representative): identity and relationship of the consenting party.

In addition to these minimum elements, non-profits should document:

a) the method used to obtain consent (written form, oral statement witnessed, audio/video recording, or digital consent) as permitted under Regulation 4(2) of the Data Protection (General) Regulations 2021,
b) confirmation that the data subject was informed of their right to withdraw consent at any time,
c) the language in which the consent communication was provided,
d) any accommodations made for data subjects with other vulnerabilities.

This additional documentation serves as critical evidence of compliance with the requirement that consent be "informed" and "unambiguous" under Section 31 of the DPA 2019.

Section 32(1) of the DPA 2019 places the burden of proof for establishing consent on the data controller.

7.4.9 Consent Storage

For non-profits consent records must be stored in a manner that ensures their integrity, confidentiality, and accessibility throughout the retention period.

For digital records, non-profits should implement:

a) encryption for data at rest and in transit,
b) regular backups stored in separate secure locations,
c) access logs that track who have viewed or modified consent records and when,
d) role-based access controls that limit consent record access to staff who genuinely need it for programme delivery or compliance purposes.

For physical records, organisations should maintain a register of access indicating who accessed the records, when, and for what purpose.

Consent records whether digital or physical must be retrievable upon request by the data subject. As part of accountability obligation, data controllers must be able to demonstrate compliance at any time. It is important to note that the Data Commissioner retains the right to review consent records upon request. Non-profits should therefore establish clear record-keeping protocols that specify retention periods, storage locations, access procedures, and destruction of protocols.

The consent storage can be in the following formats:

- Digital records: cloud storage and computing services, secure, access-controlled databases with user-level permissions and audit logs.
- Physical records: locked cabinets in secure locations with a register of access.
- Records must be retained for the duration of the programme or as specified in the applicable grant agreement, whichever is longer.

7.4.10 Consent Withdrawal Mechanism

The right to withdraw consent at any time is expressly provided under Section 32(2) of the DPA 2019. Withdrawal of consent does not affect the lawfulness of processing based on prior consent before its withdrawal. However, once withdrawal is communicated, the organisation must cease all processing activities that rely on consent as their lawful basis. This includes stopping further collection, use, and sharing of the data subject's personal data.

For non-profits operating in low-resource and low-literacy settings, the withdrawal mechanism must be designed with the data subject's circumstances in mind. The options to consider include: (a) a designated community liaison point where data subjects can make verbal withdrawal requests; (b) a toll-free phone number or SMS short code; (c) a standardised withdrawal form available at programme sites; or (d) a trusted community representative authorised to receive and transmit withdrawal requests.

Whatever mechanism is chosen, it must be actively communicated to data subjects at the point of consent and reinforced through periodic reminders during program engagement.

Critically, when a data subject withdraws consent, the organisation must have systems in place to notify all downstream partners who hold that individual's data. Section 36 of the DPA 2019 and Regulation 18 of the Data Protection (General) Regulations 2021 require that processing by a data processor be governed by a binding contract. These agreements must include provisions for operationalising withdrawal requests across the entire data-sharing chain. Failure to notify partners of a withdrawal constitutes a breach of the data controller's obligations under the Act.

Every non-profit must establish a clear, accessible, and operational mechanism for data subjects to withdraw consent. The mechanism must:

- Be communicated to data subjects at the time of obtaining consent.
- Be simple enough to use without requiring literacy or digital access (e.g. a verbal request to a named contact, a community liaison point).
- Trigger a documented process that stops all non-essential processing activities within a reasonable period.
- Notify all downstream partners who hold the data subject's information.

Statutory Reference: Section 32(3), DPA 2019
A data subject may withdraw consent at any time. Withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal. The data controller must be able to demonstrate that a withdrawal mechanism exists and that it was communicated to the data subject at the time consent was obtained.

7.4.11 Consent Architecture: Layered Notice

The layered notice approach is particularly valuable for non-profits working with vulnerable populations in resource-constrained settings. It recognises that a single, comprehensive privacy notice while legally

sufficient may not be effective. By providing information in simple and structured layers, organisations can fulfil their disclosure obligations under Section 29 of the DPA 2019 and Regulation 4(1) of the Data Protection (General) Regulations 2021 while respecting the data subject's capacity to understand information.

A layered notice approach presents privacy information at multiple levels of detail, allowing individuals to quickly understand the essentials while accessing more information if needed.

Layer	When It Is Used	Content	Format Guidance
Layer 1: Short Notice	At the point of data collection	Brief plain-language summary: who collects, what is collected, why, and the right to withdraw.	Maximum 3–5 sentences. Available in local language. Can be pictorial.
Layer 2: Full Privacy Notice	Available on request or displayed at programme site	Complete disclosure: data uses, sharing partners, storage periods, data subject rights, contact for queries and complaints, withdrawal mechanism.	Plain language. Translated into relevant local languages. Posted visibly at programme sites.
Layer 3: Just-in-Time Notices	When specific or sensitive data is requested	Contextual explanation of why that specific data element is needed before asking.	Short, specific, and triggered by the data point being requested. Can be verbal or on-screen.

7.4.12 Consent Lifecycle

Stage	Key Actions	Common Risk for Non-Profits
1. Collection	Obtain informed, voluntary, specific consent before collecting personal data. Use the appropriate method for the context.	Rushing consent at intake; treating it as a form to be signed rather than a process to be understood.
2. Documentation	Record all consent decisions in secure systems with required elements.	Incomplete records; paper forms stored insecurely or lost.
3. Use	Ensure data is used only for the purposes for which consent was given. Any new use requires fresh consent or a different lawful basis.	Scope creep: using beneficiary data for donor reports or research without separate consent.

4. Renewal	Review whether consent remains valid when programs scale, new partners are involved, or new data uses are introduced.	If original consent covers all future uses.
5. Withdrawal	Maintain an operational withdrawal mechanism. Stop processing promptly upon withdrawal. Notify all relevant partners.	No clear process for withdrawal; staff unaware of obligation to act on withdrawal requests.
6. Expiry	Consent expires when the programme ends, the data retention period is reached, or the original purpose is no longer valid.	Continuing to hold and use data after programme closure without a legal basis.

7.4.13 Managing Consent Across Multiple Partners

Managing consent in multi-partner environments requires clear and structured data-sharing arrangements (binding contracts). The Data Protection Act, 2019 and its Regulations set firm expectations that any sharing of personal data with third parties must be governed by formal agreements. These agreements should clearly define what data is being processed, for what purpose, how long it will be used, and the safeguards in place to protect it.

The absence of a written Data Processing Agreement is itself a breach of the DPA 2019. Non-profits must therefore ensure that every partner with whom they share personal data has a signed, legally enforceable agreement in place before any data is transferred. Beyond the legal requirement for written agreements, non-profits should implement the following safeguards when managing consent across multiple partners:

- Maintain a comprehensive inventory of all partners who receive personal data, including the categories of data shared and the purposes for which it is shared.
- Include clear provisions in all partnership agreements regarding consent: (a) that the partner may only process data for the purposes covered by the original consent; (b) that the partner must immediately cease processing upon withdrawal of consent by the data subject; (c) that the partner must notify the data controller of any data breaches or security incidents; and (d) that the partner must delete or return data upon termination of the agreement or expiry of the consent.
- Conduct due diligence on partners before sharing data, assessing their data protection policies, technical and organizational security measures, including staff training practices.
- Establish a mechanism for tracking consent withdrawals across all partners.

Regulation 21 of the Data Protection (General) Regulations 2021 outlines the framework for data sharing, requiring that sharing be for clearly defined purposes with appropriate safeguards in place. Where there are no sufficient safeguards for the protection of personal data, explicit consent from data subjects is required. Data subjects must be informed about how their personal data will be used, who will have access, and the potential privacy implications.

Non-profits should therefore ensure that their consent forms clearly disclose all categories of partners with whom data may be shared, and should obtain separate, specific consent for any sharing that was not originally disclosed.

Statutory Reference: Section 36 DPA 2019 & Regulation 18, Data Protection (General) Regulations 2021
Processing by a data processor shall be governed by a binding contract. The absence of a written Data Processing Agreement is itself a breach of the DPA 2019. The data controller remains responsible for ensuring that the processor provides sufficient guarantees to implement appropriate technical and organizational measures.

Reflective Practice
Review a recent programme intake process in your organization. Identify: (a) Which method of consent was used? (b) Were the conditions for valid consent met? (c) Is there a documented withdrawal mechanism in place? Note any gaps and discuss corrective steps with your team.

7.5 Vital Interests

7.5.1 Legal Foundation: Vital Interests Under the DPA 2019

Vital interest is a separate and distinct lawful basis from consent. It applies specifically where processing personal data is necessary to protect an individual's life or prevent serious harm, and where obtaining consent is impossible or would cause unreasonable delay given the urgency of the situation.

Statutory Reference: Section 30(1)(b), DPA 2019
A data controller may process personal data where processing is necessary to protect the vital interests of the data subject or of another natural person. This is a narrow, residual basis. The word 'necessary' is operative, administrative convenience or a failure to design consent processes in advance does not qualify.

7.5.2 Life-Threatening vs. Serious Health Threshold

Non-profits must clearly distinguish between situations that justify invoking vital interests and those that do not.

Threshold Level	Characteristics	Non-Profit Examples	Vital Interests Applicable?
LIFE-THREATENING	Immediate risk of death or irreversible harm. Without processing, death or permanent incapacitation is the probable outcome.	Unconscious beneficiary at a health post; person struggling to breathe; active suicidal ideation; Gender-Based Violence survivor requiring emergency referral but unable to communicate.	YES: Presumptively applicable. Document and proceed, then regularize as soon as possible.
SERIOUS HEALTH EMERGENCY	Significant risk of severe, lasting harm to physical or mental health. Death is not immediately imminent, but failure to act may escalate the situation.	Person in acute mental health crisis; severe acute malnutrition requiring hospitalization where guardian is unreachable; notifiable infectious disease requiring immediate contact tracing.	LIKELY YES: Apply the four-step decision test (refer to 7.5.3). Document reasoning exhaustively.
CONVENIENCE OR ADMINISTRATIVE	Operational efficiency, programme reporting, donor compliance, or data quality purposes. No direct risk to individual wellbeing.	Sharing client data with a donor for reporting; updating a beneficiary database from secondary sources; merging datasets across project phases.	NO: Obtain consent or rely on another lawful basis. Applying vital interests here constitutes unlawful processing.

7.5.3 Decision-Making Under Emergency Conditions: The Four-Step Test

Four-step test provides a structured framework for compliant real-time decision-making. Each step should be documented as soon as circumstances allow.

Step 1 - Assess Urgency
Is there an immediate or imminent threat to life or serious harm to health? Use the threshold analysis in Section 7.5.2. If the situation falls below the serious health emergency threshold, do not invoke vital interests, seek consent or identify an alternative lawful basis.

Step 2 - Determine Necessity
Is processing the specific personal data strictly necessary to respond to the emergency? Access only the minimum data required. Ask: 'If I did not have this information, could I still provide the emergency response?' If yes, do not process it.

Step 3 - Limit Scope and Recipients
Is the scope of data sharing proportionate to the emergency? Share data only with those directly involved in managing the emergency, for instance, treating clinicians, emergency referral partner, or protection officer. Do not share broadly.

Step 4 - Document Actions
Record what data was accessed or shared, why, with whom, and when; this should be as close to the time of the decision as possible. This is both a legal obligation and primary evidence of good faith.

7.5.4 Emergency Data Processing Record

The Emergency Data Processing Record serves as the primary evidence that the organisation's invocation of vital interests was lawful, necessary, and proportionate. Under Section 25 of the DPA 2019, data controllers must be able to demonstrate compliance at any time. In the context of emergency processing, this means that the organisation must be able to produce a complete record of what data was processed, why, by whom, and with whom it was shared. A detailed breakdown is provided below.

Non-profits should ensure that the Emergency Data Processing Record is completed as close to the time of the emergency decision as possible, ideally within hours, not days. Where records are completed retrospectively, this must be noted explicitly, and the reasons for the delay should be documented. The record should be signed by the staff member(s) involved and reviewed by the Data Protection Officer or Program manager within a reasonable period.

Element	What to Record
Date, time, and location	As precisely as possible. Note, explicitly if recorded in retrospect.
Data subject identity	Full name and programme ID. If unknown, describe the individual (e.g. adult female, approximately 35 years, found at [location]).
Nature of the emergency	Brief factual description of what happened, the observed condition, and the immediate risk assessed.
Threshold assessment	State explicitly: 'Life-threatening' or 'Serious health emergency' and the factual basis for that assessment.
Four-step test outcome	Brief notes on each step: urgency, necessity, proportionality, and documentation.
Data accessed	Specific data elements accessed beyond 'health records.' State what was reviewed and why each element was necessary.

Recipients of data	Name, role, and organization of each person's data was shared with, and what specific information was shared.
Staff member(s) involved	Name, role, and signature or initials.
Outcome of the emergency	Resolution: stabilized, transferred to hospital, referred, deceased, ongoing care.
Follow-up actions required	Consent regularisation, partner notification, data deletion, ODPC notification, post-incident review date.

7.5.5 Three Accountability Tests

To ensure that decisions made under the vital interests' basis are justified and defensible, organizations should apply three accountability tests: necessity, proportionality, and accountability, as a structured framework for evaluating their actions.

The three accountability tests necessity, proportionality, and accountability provide a structured framework for evaluating whether the invocation of vital interests was lawful. Each test must be applied at the time of the emergency decision and documented in the Emergency Data Processing Record.

Test	Question to Ask	If the Answer is No
Necessity	Was this processing action required to save life or prevent serious harm? Would the emergency response have been materially compromised without it?	The processing was not justified under vital interests. Document this finding and assess whether a different lawful basis was applied.
Proportionality	Was only the relevant minimum data used? Were data recipients limited to those directly involved in the emergency response?	The scope of processing exceeded what was necessary. Review data minimization and implement stronger protocols.
Accountability	Can the organization defend its decision and actions if audited by the regulatory authority or if the data subject requests an explanation?	Documentation is insufficient. Strengthen the Emergency Data Processing Record and conduct staff training.

7.5.6 Transitioning Away from Vital Interests: Post-Incident Protocol

Transitioning away from vital interests is not optional, it is a legal obligation. Vital interest is an exceptional basis that applies only for as long as the emergency condition persists. Once the emergency has been resolved, continued processing of personal data without consent or another lawful basis constitutes unlawful processing under Section 30 of the DPA 2019.

The post-incident protocol should be triggered as soon as the emergency has stabilised and the immediate threat to life or serious harm has passed. The DPO or the designated person must formally assess whether the vital interests basis is no longer required and document this determination. Where the data subject is now capable of giving consent, the organisation must seek informed consent to continue processing, disclosing what data was processed during the emergency, why it was processed, and with whom it was shared. This transparency is essential to maintaining trust and ensuring that the data subject can make an informed decision about whether to consent to continued processing.

Where the data subject remains incapable of giving consent (for example, due to ongoing incapacity), the organisation must identify an alternative lawful basis for continued processing such as legitimate interests or contractual necessity or cease processing and delete the data. Consent cannot be presumed, and vital interests cannot be extended beyond the emergency period.
All partners who received data under vital interests must be notified that the emergency basis has ended and instructed to cease further processing. Data shared solely for the emergency purpose must be deleted or returned to the data controller. This is particularly important where partners were not covered by existing Data Processing Agreements. Therefore, continued processing by such partners would constitute unauthorised processing under the DPA 2019.

The internal post-incident review serves as a critical learning opportunity. The DPO and senior management should evaluate:

a) whether the vital interests basis was correctly invoked,
b) whether the four-step test was properly applied,
c) whether the Emergency Data Processing Record is complete and accurate,
d) whether any data breaches occurred during the emergency response,
e) whether protocols and training need to be updated.

Stage: Lessons learned should be documented and incorporated into future emergency preparedness planning. A breakdown of the key stages in the post incident protocol, actions to be taken and the associated timelines is as follows:	**Actions Required**	**Responsible**	**Timeline**
Stage 1 - Emergency Resolution Assessment	Formally determine that the vital interest basis is no longer required.	DPO or Designated Person	Immediately upon resolution
Stage 2 - Consent Regularisation	Where the data subject is now capable of giving consent, seek	Programme staff or case worker	Reasonable timeline Recommendation: After 5 to 7 days of resolution

Stage 3 - Partner Notification & Data Minimisation	Notify all partners who received data under vital interests. Instruct them to cease further processing and delete or return data shared solely for the emergency purpose.	DPO	Reasonable timeline Recommendation: After 5 to 7 days of resolution
Stage 4 - Internal Post-Incident Review	Evaluate whether the vital interests basis was correctly invoked. Assess documentation quality. Update protocols and training.	DPO + Senior Management	Reasonable timeline Recommendation: Within 30 days of resolution
Stage 5 - Record Update & Compliance Filing	Ensure all Emergency Data Processing Records are complete, filed, and retained for a minimum of 5 years. Confirm ODPC notification if a breach occurred.	DPO	Reasonable timeline Recommendation: Within 30 days of resolution

Note: The timelines provided are indicative recommendations only and do not constitute legally prescribed timeframes.

Unless otherwise expressly provided by applicable law, the timelines outlined herein are recommended operational benchmarks and should not be construed as mandatory legal requirements.

Statutory Reference: Section 43, DPA 2019 Breach Notification
If the emergency involves a data breach (unauthorized access, accidental disclosure, or loss of data), the DPO must notify the ODPC within 72 hours of becoming aware of the breach. Notification of the data subject is required where the breach is likely to result in high risk to their rights and freedoms.

7.6 Key Takeaways

- Consent must be freely given, specific, informed, and unambiguous.
- The burden of proof for consent lies with the data controller.
- Vulnerable populations require additional safeguards. Services must never be made conditional on consent that is not operationally necessary.
- The consent lifecycle extends beyond the point of collection. It must be actively managed through documentation, renewal, withdrawal, and expiry.

- Vital interest is a narrow, exceptional basis. It applies only to life-threatening or serious health emergencies where consent is impossible or impractical, and it must be documented immediately.
- Every action under vital interests must pass the necessity, proportionality, and accountability tests.
- Transitioning back to a consented or alternative lawful basis after an emergency is a legal obligation.

7.7 Assessment

Part A: Knowledge and Conceptual Understanding

1. What are the key characteristics of valid consent under the Data Protection Act, 2019, and why is each important in protecting data subjects?
2. How does valid consent differ from the vital interest's lawful basis in terms of control, purpose, and conditions of use?
3. In what types of situations is consent considered invalid, particularly where there is vulnerability, dependency, or power imbalance?

Part B: Applied Analysis

1. A beneficiary signs a consent form, but later states she only agreed because she feared losing access to food aid. Is this consent valid? What immediate steps should the organization take?
2. Your organization intends to share beneficiary data with a new partner not covered in the original consent. What are your lawful options, and what risks must you consider before proceeding?
3. A field officer encounters an unconscious individual requiring urgent medical care, with no way to obtain consent. Which lawful basis applies, and what key justification must be documented at the time of decision-making?

Part C: Organizational Reflection

1. After an emergency response, your organization continues to hold personal data collected under the vital interest's basis. What actions should be taken to ensure compliance and accountability post-incident?
2. How should your organization design systems and processes to ensure that consent is meaningful, ongoing, and not treated as a one-time formality?
3. What internal controls or documentation practices should be in place to justify the use of vital interests and prevent its misuse as a substitute for proper consent?

08.
Rights of Data Subjects

About This Module

This module equips learners to understand, explain, and operationalize the rights that every data subject holds over their personal data under the Kenyan law. It provides practical tools and procedures for handling Data Subject Requests (DSRs) lawfully, ethically, fairly, and within the statutory timelines required by the Data Protection Act, 2019 and its Regulations.

8.1 Introduction

This module explores the rights of data subjects under Kenyan law and provides practical guidance on handling Data Subject Requests (DSRs), meeting statutory timelines, and ensuring compliance with organizational obligations as non-profits.

The Data Protection Act, 2019 gives individuals important rights over their personal data and places corresponding responsibilities on organizations that collect, use, store, or share that information. These rights promote transparency, accountability, and respect for individual privacy.
Understanding and responding to data subject rights is a critical part of lawful and ethical data management. Individuals may request access to their data, seek corrections, object to processing, request deletion, or exercise other rights provided by law.

8.2 Objectives

By the end of this module, learners should be able;

1. To define the term 'data subject' under the DPA 2019 and explain who qualifies as one.
2. To identify, distinguish and describe all six rights of a data subject under Section 26 of the DPA 2019.
3. To explain the mandatory response timelines under the DPA 2019 and the subsidiary Regulations.
4. To apply a step-by-step procedure for receiving, verifying, and responding to Data Subject Requests.
5. To handle the rights of vulnerable data subjects, including minors and persons with disabilities.

8.3 Learning Outcomes

Outcome	Demonstrated Competence
Identify and explain rights of data subjects	Identify and explain the rights of data subjects and the corresponding organizational responsibilities.
Understand Data Subject Requests	Evaluate, process and respond to Data Subject Requests using the appropriate forms, procedures, and legal timelines.
Manage Data Subject Requests records	Maintain accurate Data Subject Requests records and assess requests for compliance, restriction, or lawful refusal.
Recognize legal obligations when dealing with data subjects and personal data	Understand the legal obligation they have as non-profits in handling personal data and the exercise of data subject rights within their programs.
Apply and manage data subject rights in third party environments	Apply and manage data subject rights issues involving representatives for vulnerable persons, third parties, and complaints to the Office of the Data Protection Commissioner.

8.4: WHO IS A DATA SUBJECT?

Legislation	Definition of Data Subject
DPA 2019, Section 2	An identified or identifiable natural person who is the subject of personal data.
Data Protection (General) Regulations, 2021	Reflects the same definition and extends its application to all data processing activities within Kenya.

In practical terms, a data subject is any natural individual whose personal data is collected, stored, shared, or otherwise processed. A natural person is a real human being who is recognized by the law to have legal rights, duties, and capacities.

Within the non-profit context, a data subject can refer to the following individuals who play different roles within its operations:

- Programme beneficiaries and clients/beneficiaries
- Donors and funders (where personal data is held)
- Staff, volunteers, consultants and interns
- Survey and research participants
- Third-party individuals who appear in case files, referral records, tendering or monitoring reports

Reflective Activity
Identify or think about your current programme and list three categories of people whose data you hold.

8.5: RIGHTS OF DATA SUBJECTS

Section 26 of the DPA 2019 provides every data subject with six legally enforceable rights over their personal data. The rights are as stated below:

Right	Section (DPA 2019) I Form (DPGR 2021)
(a) Right to be informed	Section 26(a), Section 29 — Duty to notify data subject
(b) Right to access personal data	Section 26(b), Section 30 I Form DPG2
(c) Right to object to processing	Section 26(c), Section 36 I Form DPG1
(d) Right to rectification (correction)	Section 26(d), Section 40 I Form DPG3
(e) Right to erasure of false or misleading data	Section 26(e), Section 38 I Form DPG5
(f) Right not to be subject to automated decision-making	Section 35 I No prescribed form - object in writing
(g) Right to data portability	Section 38 I Form DPG4

8.5.1 The Right to Be Informed

Before collecting any personal data, a non-profit must proactively inform the data subject of the following:

- The fact that personal data is being collected.
- The purpose(s) for which the personal data is being collected.
- The rights of the data subject under Section 26.
- Whether data collection is voluntary or mandatory, and the consequences of failing to provide it.
- The identity and contact details of the data controller or data processor.
- Any third parties to whom the data will be transferred, including details of safeguards in place.
- The technical and organizational security measures in place to ensure integrity and confidentiality.
- Whether the data is collected pursuant to a specific law.

Reflective Statement

How must information be provided? The DPA requires concise, transparent and easily accessible form using clear and plain language:

- A written privacy notice or data collection notice given before or at the point of data collection.
- Oral briefings for beneficiaries with low literacy, supplemented with written summaries.
- Digital privacy notices for online platforms, surveys, and digital case management systems.
- For children: age-appropriate explanations with guardian engagement.

Non-Profit Obligation

The right to be informed is not reactive, it is a proactive duty. A non-profit must not wait for a data subject to ask. The privacy notice must be provided before or at the moment personal data is collected. Failure to do so is an unlawful processing act under the DPA 2019.

8.5.2 The Right of Access

A data subject has the right to obtain confirmation of whether a non-profit holds personal data about them, and if so, to access that data. The scope of an access request includes:

- The purpose(s) of the processing.
- The categories of personal data held.
- Recipients or categories of recipients to whom data has been or will be disclosed.
- The expected retention period, or the criteria used to determine it.
- If data was not collected from the data subject directly, available information about its source.
- The existence of any automated decision-making, including profiling, and meaningful information about the logic involved.

Access requests are free of charge as a general rule. A reasonable fee covering administrative costs may be charged where a request is unfounded, excessive or repetitive. The non-profit must provide a copy of the personal data in a commonly used, structured, and machine-readable format where technically feasible.

8.5.3 The Right to Object to Processing

A data subject may object to the processing of all or part of their personal data for a specified purpose or in a specific manner. Where the objection is upheld, the non-profit must cease processing without undue delay.

Restriction of Processing: Under Section 34, a data subject may additionally request restriction of processing where the accuracy of the personal data is contested, processing is unlawful but the data subject requests restriction rather than erasure, the data is no longer needed but is required for a legal claim, or the data subject has objected and a determination on legitimate interests is pending.

Absolute Right for Direct Marketing: Where the objection concerns processing for direct marketing or fundraising purposes, this right is absolute. Non-profits must comply immediately and cannot override the objection by asserting a legitimate interest (Section 36(3), DPA 2019 and Regulation 8, General Regulations 2021).

Response Obligation: A non-profit must respond and comply within fourteen (14) days. If declining to comply, it must provide written reasons citing the specific legal jurisdiction or legitimate interest.

8.5.4 The Right to Rectification (Correction)

A data subject has the right to require a non-profit to correct personal data that is inaccurate, out of date, incomplete or misleading. Section 40 operationalizes the data accuracy principle in the DPA.

Third-Party Notifications: Where a non-profit has shared personal data with a third party and the data subject requests rectification, the non-profit must take all reasonable steps to inform those third parties of the correction, unless doing so is impossible or involves disproportionate effort.

Response Obligation: A non-profit must comply with rectification requests within fourteen (14) days, without charging any fee.

8.5.5 The Right to Erasure (Deletion)

In Regulation 12 of the Data Protection (General) Regulations 2021, a data subject may request erasure where:

- The personal data is no longer necessary for the purpose for which it was collected.
- The data subject withdraws consent that was the lawful basis for retention.
- The data subject objects to processing and there is no overriding legitimate interest to continue.
- The personal data was processed for direct marketing purposes and the individual objects.
- Processing is unlawful, including where it breaches the lawfulness requirements of the DPA.
- Erasure is necessary to comply with a legal obligation.

The right to erasure does NOT apply where continued processing is necessary to exercise the right of freedom of expression, to comply with a legal obligation, for the performance of a task in the public interest, for archiving in the public interest or scientific research, or for the establis hment or defence of a legal claim. Response Obligation: A non-profit must respond to erasure requests within fourteen (14) days at no cost to the data subject.

Critical Note
Non-profits conducting longitudinal research or supporting legal proceedings may rely on lawful grounds to refuse erasure. However, the refusal must be in writing, clearly reference the applicable lawful basis, and communicated to the data subject within 14 days. Silence is not a lawful refusal.

8.5.6 The Right Not to Be Subject to Automated Decision-Making

Every data subject has a right not to be subject to a decision based solely on an automated processing system, including profiling, which produces legal effects or significantly affects the data subject.
Examples in a non-profit context include automated eligibility scoring for programme entry, AI-based vulnerability assessments, or algorithmic targeting for service referrals.

Non-profit Obligations:

- Inform data subjects whenever automated tools are used to make or inform decisions about them.
- Integrate human oversight into all automated decision-making processes affecting individuals.
- Conduct a Data Protection Impact Assessment (DPIA) where automated profiling is used at scale.
- Ensure affected individuals can contest automated decisions and request human review.

Automated decision-making is permissible where the decision is necessary for the performance of a contract, the processing is authorized by law, or the data subject has given explicit, informed consent.

8.5.7 The Right to Data Portability

A data subject has the right to receive personal data concerning them in a structured, commonly used and machine-readable format without any hindrance, and may request that the data be transmitted directly to another data controller where technically feasible.
The right to portability does NOT apply where processing is necessary for a task carried out in the public interest or the exercise of official authority, or where it may adversely affect the rights and freedoms of others.

Response Obligation: A data controller or data processor must comply with data portability requests, at reasonable cost and within a period of 30 days. Where the portability request is complex or numerous, it may be extended in consultation with the regulatory authority.

8.6 Exercise their Own Rights

The Data Protection Act, 2019 (Section 27) provides situations where data subject rights may be exercised by another person, particularly where the individual is unable to act on their own behalf. This applies in cases involving minors or individuals whose capacity is limited due to disability or other conditions. In such instances, the law permits a legally authorized representative to act, but only where there is clear and verifiable authority to do so.

Organizations must therefore distinguish between when rights can be exercised directly by the data subject and when legal authorization is required to act on their behalf. The Data Protection Act, 2019 (Section 27) recognizes that not all data subjects can exercise their rights independently.

Non-profits working with children, refugees, persons with disabilities, or elderly beneficiaries must have clear internal procedures for verifying the authority of a representative before acting on any Data Subject Requests submitted on behalf of another person.

8.7 Procedures for Handling Data Subject Requests

Every non-profit must establish a clear internal procedure for receiving, processing and responding to Data Subject Requests (DSR). The following five-step procedure reflects the requirements of the DPA 2019 and the Data Protection (General) Regulations, 2021.

Step 1 - Receiving the Request

- Any member of staff who receives a DSR (in person, by phone, by email, or by post) must treat it as urgent and escalate it immediately to the designated DPO.
- Log the request immediately in the DSR Register with a receipt date and timestamp. The 14-day clock starts from the date of receipt.
- If a request is made verbally, confirm it in writing by email or letter to the data subject as soon as practicable.
- Do not require a data subject to use a specific form as a condition of acting on their request if an informal request is valid.

Step 2 - Identifying the Right Being Exercised

- Determine which right(s) are being exercised from the request.
- If the request concerns multiple rights (e.g., access + rectification), log and process each separately.
- Provide the data subject with the appropriate form(s) from the First Schedule of the Data Protection (General) Regulations, 2021 as a guide, but do not delay processing pending form completion.

Step 3 - Verifying the Identity of the Requester

- Before releasing any personal data or acting on a DSR, verify the identity of the requester to prevent unauthorized disclosure.
- Verification should be proportionate to the sensitivity of the data. Acceptable methods include matching request details against existing records or requesting a commonly used ID document.
- If the request is made by a representative (parent, guardian, authorized agent), verify their authority before acting.
- Do not request excessive documentation; this can be used as a barrier to suppress rights.

Step 4 - Assessing and Processing the Request

- Determine whether the non-profit holds the relevant personal data.
- Assess whether any exemptions or lawful grounds for refusal apply (e.g., legal obligation, public interest, legitimate overriding interest).
- If the request will be declined in whole or in part, prepare a written response setting out the specific legal basis for refusal.
- Where data must be retrieved from third-party processors, contact those processors immediately.

Step 5 - Responding to the Data Subject

- Respond within 14 days of receipt. If a brief extension is required (up to 30 days), notify the data subject in writing within the standard 14-day period and explain the reasons.
- Provide information in a concise, transparent and easily accessible form using clear and plain language.

- All responses must be in writing (letter, email, or formal printed notice).
- If the request is declined, the response must: (a) state the specific legal basis for refusal; (b) inform the data subject of their right to lodge a complaint with the regulatory body; and (c) inform them of their right to seek judicial review.

8.7.1 The Data Subject Request Register

Every non-profit must maintain a DSR Register to document all requests received as it is a key exercise to have the records in the instance a complaint is lodged by a data subject to the regulatory body. The Data Subject Request register has details of record, and the structure is detailed below;

Field	Detail to Record
Request ID	Unique identifier for tracking
Date received	Date and time the request was received (starts the 14-day clock)
Name of requester	Full name
Contact details	Email, phone, or postal address
Right being exercised	Access / Objection / Rectification / Erasure / Automated / Portability
Brief description	Summary of what is requested
Identity verified?	Yes / No / Method used
Assigned to	Name of staff member responsible
Date of response	Actual date response was sent
Outcome	Complied / Partially complied / Declined (with reason noted)
Extension notified?	Yes / No / Date notified
Escalated to ODPC?	Yes / No

8.8 THIRD-PARTY DATA SHARING AND DATA SUBJECT REQUESTS OBLIGATIONS

Non-profits frequently share beneficiary data with donors, implementing partners, or government agencies. When a data subject exercises a right, the non-profit's obligations extend to data shared with third parties.
8.8.1 Data Processing Agreements

Before sharing personal data with any third party, non-profits acting as data controller must have a written Data Processing Agreement (DPA) in place. This agreement must specify:

- The purpose and scope of the processing permitted.
- The processor's obligation to process only on the controller's written instruction.
- Security and confidentiality obligations.
- The processor's obligation to assist the controller in responding to DSRs.
- Data retention and deletion obligations.

8.8.2 What Happens When a DSR Involves Third-Party Data?

- The non-profit (data controller) remains responsible for responding to the data subject within 14 days.
- The non-profit must immediately notify the third-party processor of the DSR and request their cooperation.
- The third-party processor must assist the non-profit in fulfilling the request (this should be contractually required in the Data Processing Agreement).
- If a third-party refuses to cooperate with a rectification or erasure instruction, the non-profit must document this, inform the data subject, and report the non-compliance to the regulatory body where applicable.

8.9 The Office of the Data Protection Commissioner and Enforcement

8.9.1 When Can a Data Subject Complain to the ODPC?

Under Section 56 of the DPA 2019, a data subject may lodge a complaint with the Office of the Data Protection Commissioner (ODPC) where a data controller or data processor:

- Fails or refuses to respond to a DSR within the prescribed timeline.
- Provides an inadequate or unlawful response to a DSR.
- Refuses to correct, delete, or provide access to personal data without a lawful basis.
- Otherwise breaches the provisions of the DPA 2019 or its regulations.

8.9.2 ODPC Complaint Process

A complaint to the ODPC may be lodged online via the ODPC portal (www.odpc.go.ke) or in writing. The complaint must include a description, the data controller involved, and evidence of the DSR and the response (or non-response) received. Facilitators should ensure participants understand that data subjects do not need a lawyer to lodge a complaint.

8.9.3 Non-Profit Obligations When a Complaint Is Lodged

When a non-profit experiences a complaint lodged against them by a data subject, the following are the necessary steps to take:

- Respond to the Office of the Data Protection Commissioner enquiries within the timelines specified.
- Retrieve and preserve all records related to the DSR in question.
- Do not destroy, alter or conceal records relevant to the complaint.
- Cooperate with any ODPC investigation or audit.
- Take note of the checklist below to ensure continuous compliance even after the process is adjourned and amicably solved with the data subject.

Data Subject Rights Compliance Checklist

Ref	Checklist Item	Status / Notes
1	A Privacy Notice is in place and provided to data subjects before collection.	Done Pending
2	The lawful basis for each processing activity is documented.	Done Pending
3	A procedure exists to receive, log and track DSRs.	Done Pending
4	Identity verification is conducted before responding to DSRs.	Done Pending
5	All DSRs are responded to within the stipulated timelines.	Done Pending
6	Data subject rights are communicated in plain language in the Privacy Notice.	Done Pending
7	A data retention schedule is documented and enforced.	Done Pending
8	Data Sharing Agreements (DSAs) are in place with all third parties.	Done Pending
9	A DPIA process is integrated into project design for high-risk processing activities.	Done Pending
10	Automated decision-making tools have documented human oversight mechanisms.	Done Pending
11	Proxy request procedures are in place (for minors and incapacitated individuals).	Done Pending
12	Staff are trained on data subject rights and DSR handling.	Done Pending
13	A DPO or designated data protection responsible person is appointed.	Done Pending
14	The ODPC complaint pathway is communicated to data subjects in refusal letters.	Done Pending
15	Refused DSRs are documented with written legal reasons on file.	Done Pending

8.10 Key Takeaways

- Data subject rights are the operational expression of control and give individuals authority over how their personal data is used.
- Rights apply throughout the data lifecycle (collection, use, sharing, storage, deletion), not just at the point of consent.
- Timely response is non-negotiable and requests must be handled within legally defined timelines and documented. Every request should leave an audit trail—what was requested, how it was handled, and the final outcome.
- Where a data subject cannot act independently (e.g., minors, persons with limited capacity), rights may be exercised by authorized representatives but only after proper validation of authority.

- Rights are not absolute; organizations may lawfully limit them under specific conditions (e.g., legal obligations, public interest) but must justify and document this.
- Consent withdrawal must be as easy as giving consent, and systems should support this without friction.

8.11 Case Scenarios and Discussion Exercises

Case Scenario 1: Umoja Non-Profit (Multiple Simultaneous Rights)
Umoja non-profit runs a food distribution programme. They collect names, national ID numbers, phone numbers, and family sizes from beneficiaries. Within one week, a beneficiary named Mary submits four separate requests: (1) Access to all personal data Umoja holds about her. (2) Her family size is recorded as 3 but should be 5 demands correction. (3) Objects her phone number being shared with a donor for unsolicited marketing calls. (4) Demands her entire record to be deleted because she no longer wants services.

Discussion Questions: (a) Which form does each request correspond to? What is the deadline for each request? (b) For Request 3 (phone number for marketing): what makes this an absolute right? Can Umoja refuse? (c) For Request 4 (erasure): does Umoja have a lawful basis to retain any of Mary's data for donor reporting? What entries should appear in Umoja's DSR Register?

Case Scenario 2: Balancing Access and Erasure Against Research Interests
A non-profit runs a child protection programme. A former beneficiary (now an adult) requests: (a) Access to their case file. (b) Deletion of certain counselling records because they are pursuing a public career. The non-profit still uses the data for donor reporting and longitudinal research.

Discussion Questions: (a) What is the non-profit's obligation regarding the access request, and can any parts of the case file be withheld? (b) On what grounds, if any, can the non-profit refuse the erasure request? (c) How should the non-profit communicate a partial refusal to the data subject?

09.

Obligations of Data Handlers and Consequences of non-compliance

About This Module

This module is designed to help learners understand their specific legal responsibilities as data handlers, translate legal provisions into operational practices, recognize legal risks and liabilities, and build a culture of responsible data use within their organizations.

9.1 Introduction

Non-profit organizations frequently work with donors, implementing partners, service providers, consultants, and technology platforms that require access to personal data. While data sharing may be necessary for programme delivery and operational effectiveness, it also creates additional data protection responsibilities.

The Data Protection Act, 2019 requires organizations to ensure that personal data remains protected when shared with third parties. Accountability does not end when data leaves the organization that originally collected it.

This module examines the roles and responsibilities of data controllers, data processors, and third parties, and provides practical guidance on lawful data sharing, contractual safeguards, and accountability measures necessary to protect personal data throughout its lifecycle.

9.2 Objectives

By the end of this module, participants should be able:

1. To explain the legal obligations of data controllers, data processors, and third-party data handlers under the Data Protection Act, 2019 and related Regulations.
2. To understand and apply registration, governance, security, and accountability requirements to organizational data processing activities.
3. Implement compliance measures for lawful processing, data protection impact assessments, and personal data breach management.
4. Assess the legal, financial, and operational consequences of non-compliance and develop appropriate compliance improvement strategies.

9.3 Learning Outcomes

By the end of this module, learners will be able to demonstrate that following:

Outcome	Demonstrated Competence
Understand the roles and responsibilities of data handlers	Distinguish the roles, responsibilities, and accountability of data controllers and data processors within their organizations.
Determine and apply legal obligations	Determine and apply applicable registration, lawful processing, security, and governance requirements under Kenyan data protection law.
Understand and apply compliance	Conduct basic compliance activities, including DPIAs, breach response procedures, and data protection risk assessments.
Identify and apply corrections to violations	Identify potential violations, applicable penalties, and corrective actions required to achieve and maintain compliance.

9.4 UNDERSTANDING DATA HANDLERS

Before examining obligations, participants must understand who the DPA 2019 applies to.

9.4.1 Data Controller (Section 2, DPA 2019)

A data controller is any person or entity that, alone or jointly with others, determines the purpose and means of processing personal data. The data controller:

- Determines why data is collected and how it will be used.
- Bears primary legal responsibility for compliance with the DPA 2019.
- Must ensure that any data processor they engage operates under a written contract.

9.4.2 Data Processor (Section 2, DPA 2019)

A data processor is any person or entity that processes personal data on behalf of a data controller. The processor:

- May only process data on the documented instructions of the controller.
- May not process data for its own separate purposes.
- Must enter into a written data processing agreement with the controller (Section 41(2), DPA 2019).

Practical Example
A nonprofit collecting beneficiary details → Data Controller. A cloud storage provider storing that data on behalf of the nonprofit → Data Processor. In many real-world cases, organisations act simultaneously as both a controller (for their own staff data) and a processor (for client data).

9.4.3 Distinctions Between Data Controller and Processor

DATA CONTROLLER	DATA PROCESSOR
Determines the purpose of processing, the why and for whom.	Carries out processing operations on the controller's behalf, the how.
Determines the means of processing: what systems, methods, and categories of data to use.	Must follow the controller's documented instructions. Cannot depart from them without the controller's authorisation.
Bears primary legal accountability under the DPA 2019. Obligations run directly to data subjects and the ODPC.	Bears direct obligations under the DPA 2019 but is primarily accountable to the controller and through the controller to data subjects.
Must register with the ODPC where registration thresholds are met (Section 18, DPA 2019).	Must also register with the ODPC where registration thresholds are met (Section 18, DPA 2019).
Must enter into a written data processing agreement with each processor (Section 41(2), DPA 2019).	Must only process data under a written contract with the controller (Section 41(2), DPA 2019).
Receives breach notifications from processors. Has 72 hours to notify the ODPC after becoming aware (Section 43, DPA 2019).	Must notify the controller of a breach within 48 hours of becoming aware (Regulation 38, General Regulations 2021).
Must conduct or commission a DPIA before high-risk processing begins.	Must assist the controller in conducting DPIAs and provide all information necessary to demonstrate compliance.
Remains liable to data subjects for damages caused by processor non-compliance where the controller failed to adequately verify the processor's guarantees.	Directly liable to data subjects for damages caused by its own processing failures (Section 65, DPA 2019).

9.5 REGISTRATION REQUIREMENTS

9.5.1 Mandatory Registration Obligation

According to section 18 of the DPA 2019 provides that no person shall act as a data controller or data processor without being registered with the Data Commissioner. Handling personal data is therefore a regulated function, not an operational activity.

What Determines Whether You Must Register?

The Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021 set the thresholds for mandatory registration. The Data Commissioner considers:

- The nature of the industry (e.g., health and finance are higher-risk sectors).
- The volume of personal data being processed.
- Whether sensitive personal data is involved.
- Whether personal data is being transferred outside Kenya.

9.5.2 The Registration Process (Section 19, DPA 2019)

Registration is a compliance disclosure exercise, not a formality. Organisations must provide:

- The categories of personal data collected and processed.
- The purposes for which data is collected.
- The categories of data subjects.
- The security safeguards in place.
- The risks involved in the processing.

> Providing false or misleading information in a registration application is a criminal offence under Section 19(3) of the DPA 2019.

After registration, data controllers and processors must notify the Data Commissioner of any material changes to their registration details. Failure to do so constitutes an offence. Registration is subject to renewal after 2 years.

The register of data controllers and data processors is publicly accessible. This is done to introduce transparency and public accountability to customers, partners, and regulators to allow verifying whether an organization is registered and compliant.

Registration may be cancelled by the Data Commissioner where false or misleading information was submitted in the registration application, or where the registered entity fails to comply with the requirements of the Act.

9.6 CONTINUOUS COMPLIANCE: AUDITS AND GOVERNANCE

The Data Commissioner has authority to conduct periodic audits of data controllers and processors to assess compliance with the DPA 2019 and its Regulations. Compliance is not a one-time activity; it is an ongoing obligation. Organisations must therefore maintain documentation that demonstrates continuous compliance.

Organizations are required to designate a Data Protection Officer (DPO) where they process personal data, their core activities require regular and systematic monitoring of data subjects on a large scale, or their core activities involve large-scale processing of sensitive personal data. The DPO should have expert knowledge of data protection law and practice. The DPOs' responsibilities include advising the organisation, undertaking training for staff, supporting and overseeing assessments. Above all, the DPO acts as the primary point of contact with the regulatory authority.

The DPO must avoid conflicts of interest. They should not simultaneously hold a position that requires determining the purposes and means of processing personal data.

Within the General Regulations 2021, Regulations 41–45. A Data Protection Impact Assessment (DPIA) is a structured process for identifying and mitigating privacy risks before commencing processing activities that are likely to pose a high risk to the rights and freedoms of data subjects.

DPIAs must be submitted to the Data Commissioner at least 60 days before processing begins. Where the DPIA reveals unmitigable high risk, the data controller must consult the Data Commissioner before proceeding; this is known as prior consultation.

9.7 SECURITY AND ORGANISATIONAL MEASURES

Data controllers are required to implement appropriate technical and organizational measures to ensure the security of personal data. These measures must safeguard personal data against unauthorized or unlawful processing, as well as protect it from accidental loss, destruction, or damage.

When determining appropriate data protection measures, a data controller must consider several factors. These include the current state of the art and available technology, as well as the cost of implementing such measures relative to the risks involved. Consideration must also be given to the nature, scope, context, and purpose of the data processing activities, alongside the potential risks posed to the rights and freedoms of data subjects.

Where a data controller engages a data processor, the processing must be governed by a written contract. This contract should clearly require the processor to act only on the documented instructions of the controller. It must also impose confidentiality obligations on all individuals authorized to process the data and require the processor to support the controller in meeting its obligations toward data subject rights. Additionally, the contract must provide for the deletion or return of all personal data to the controller upon termination of the agreement.

Lastly, data controllers are required to integrate data protection mechanisms into the design of processing activities from the outset. This implies that privacy and data protection considerations must be built into both systems and processes before any data is collected or processed.

9.8 DATA BREACH MANAGEMENT

Data breach refers to a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data. Organisations are required to have clear procedures for identifying, reporting, and investigating data breaches promptly. Additionally, organisations must maintain internal records of breaches, regardless of whether they are reportable, and implement corrective actions to prevent recurrent.

A data breach is notifiable where personal data has been accessed or acquired by an unauthorized person and there is a real risk of harm to the data subject. Under the DPA 2019, high risk data breaches are those incidences that are likely to result in significant risk to the rights and freedoms of individuals. These include breaches such as identity theft, financial loss, reputational damage, or discrimination. The General Regulations 2021 (Second Schedule) further specifies categories of personal data whose breach automatically constitutes a notifiable breach.

9.8.1 Breach Notification Timelines

Notification Direction	Timeline & Basis
Data Controller → Data Commissioner	Within 72 hours of becoming aware of the breach (Section 43, DPA 2019).
Data Processor → Data Controller	Within 48 hours of becoming aware of the breach (Regulation 38, General Regulations 2021). This gives the controller time to assess and meet the 72-hour deadline.
Data Controller → Affected Data Subjects	Without undue delay, where the breach is likely to result in high risk to their rights and freedoms (Section 43(1)(b), DPA 2019; Regulation 38(2), General Regulations 2021).

9.8.2 Required Content of Breach Notification (Regulation 38)

Notification to the Data Commissioner must include:

- The date and circumstances in which the controller first became aware of the breach.
- A chronological account of steps taken after becoming aware.
- Details of how the breach occurred, where applicable.
- The number of data subjects affected.
- The categories and types of personal data affected.
- The potential harm to affected data subjects.
- Remediation measures taken or planned.

Organizational Reflection
Organizations must have incident response plans, breach registers, and internal escalation procedures in place before a breach occurs. The 72-hour controller notification timeline allows very little investigation time; prior preparation is essential.

9.10 CONSEQUENCES OF NON-COMPLIANCE

Enforcement Notices (Section 58, DPA 2019)

Enforcement notices are regulatory tool under the Data Protection Act 2019, designed to ensure that organisations and individuals comply with their data protection obligations. Issued by the Data Commissioner, these notices serve as formal directives requiring corrective action where a breach of the law has been identified.

Under Section 58, an enforcement notice not only highlights instances of non-compliance but also provides clear instructions on how the issue must be remedied within a specified timeframe. This mechanism plays a crucial role in promoting accountability, safeguarding personal data, and reinforcing adherence to the principles of data protection.

Where the Data Commissioner is satisfied that a person has failed to comply with the DPA 2019, the Commissioner may issue an enforcement notice specifying:

- The provisions that have been contravened.
- The measures required to eliminate the breach.
- The period within which corrective action must be taken.

Penalty Structure

Category	Legal Basis	Consequence
General Criminal Penalty	S.72, DPA 2019	Fine not exceeding KES 3,000,000 OR imprisonment not exceeding 10 years, or both.
Administrative Fine	S.58(4) & S.62, DPA 2019	Fine not exceeding KES 5,000,000 or 1% of annual turnover of the preceding financial year, whichever is lower.
Compounded Offences	S.58(8) & S.74, DPA 2019; General Regulations 2021	The Data Commissioner may compound offences for payment of up to two-thirds of the maximum applicable fine.
Civil Liability	S.65, DPA 2019	Damages recoverable for both financial loss and distress suffered as a result of a contravention of the Act.
Enforcement Notice	S.58, DPA 2019	The Commissioner specifies contraventions, corrective measures required and the period within which they must be taken.
Deregistration	S.22, DPA 2019	Registration cancelled where false information was submitted or the entity fails to comply with the Act.
Individual Liability	DPA 2019	Fine of KES 10,000 per day.

9.11 KEY TAKEAWAYS

- Data handlers must comply with the principles and requirements set out in the Data Protection Act 2019 when collecting, processing, and storing personal data. Appropriate technical and organisational measures must be implemented to safeguard data and prevent breaches.
- Data handlers must be able to demonstrate accountability and maintain records of their data processing activities. In the event of non-compliance, the Data Commissioner has the authority to investigate and take corrective action.

- One key consequence of non-compliance is the issuance of enforcement notices, which specify the breach, required corrective measures, and a deadline for compliance.
- Failure to comply with enforcement notices may lead to more severe actions, including financial penalties or legal proceedings.
- Non-compliance can also result in reputational damage, loss of trust, and potential harm to affected individuals.
- Adherence to obligations is essential to avoid regulatory consequences and to uphold the rights and freedoms of data subjects.

Case Scenario: Compliance Review

Scenario: A CBO collects user data through a mobile application, shares it with marketing partners, has no privacy notice, and has not registered with the ODPC.

- Identify all legal violations with specific section references from the DPA 2019 and General Regulations 2021.
- Assess the applicable penalties under Sections 58, 62 and 72 of the DPA 2019.
- Draft a prioritized compliance remediation plan with timelines.

9.12 Assessment

Part A: Knowledge and Conceptual Understanding

1. What are the primary obligations of data controllers and data processors under the Data Protection Act 2019?
2. What is the purpose of implementing technical and organizational security measures under Section 41?
3. What must be included in a data processing agreement between a controller and a processor?
4. What factors must be considered when determining "appropriate measures" for data protection under Section 42?
5. What is an enforcement notice, and under what circumstances can the Office of the Data Protection Commissioner issue one?

Part B: Applied Analysis

1. An organization collects and processes personal data but has no formal contracts with third-party processors. Identify the compliance gaps and legal risks.
2. A data breach occurs due to weak security controls. Assess how the organization failed to meet its obligations and outline the immediate corrective actions required.
3. An enforcement notice is issued requiring corrective measures within 30 days. Analyse the operational and legal implications of failing to comply within the given timeline.
4. A controller implements minimal security measures due to budget constraints. Evaluate whether this meets the "appropriate measures" threshold under the law.
5. A processor continues to use personal data after termination of a contract. Identify the violations and potential consequences.

Part C: Organizational Reflection

1. How does your organization ensure ongoing compliance with enforcement notices or regulatory directives?
2. What internal accountability mechanisms are in place to detect and respond to non-compliance early?
3. What are the potential reputational and operational impacts your organization would face in the event of regulatory enforcement or penalties?

10.
Cross-Border Data Transfer

About This Module

This module examines the legal, technical, and operational requirements governing cross-border transfers of personal data. Learners will learn how to assess transfer risks, select & apply lawful transfer mechanisms, evaluate adequacy decisions, manage international partnerships, and establish safeguards for cloud services, remote access, and critical data infrastructure. Learners should be able to establish transfer governance programs that effectively demonstrate compliance with the Office of the Data Protection Commissioner.
The module also explores practical scenarios common in the non-profit sector, including donor reporting, consortium arrangements, cloud-based programme management systems, humanitarian response coordination, and regional data sharing initiatives.

10.1 Introduction

Non-profit organisations increasingly rely on cloud platforms, donor reporting systems, regional databases, international consultants, and global partnerships to deliver programmes and services. As a result, personal data is often transferred, accessed, or processed outside Kenya, sometimes without organisations fully recognising that a cross-border transfer has occurred.

While international data sharing can improve collaboration, efficiency, and service delivery, it also introduces privacy, security, and compliance risks. The Data Protection Act, 2019 (DPA) and the Data Protection (General) Regulations, 2021 require organisations to ensure that personal data remains protected when transferred across borders and that appropriate safeguards are in place.
This module examines the legal and operational requirements governing cross-border data transfers. Learners will learn about adequacy decisions, transfer safeguards, transfer impact assessments, cloud services, remote access, data localisation requirements, and accountability measures necessary

for lawful international data sharing. Attention is given to the realities faced by non-profit organisations working with vulnerable populations, sensitive personal data, and international partners.

Reflective Practice
Identify one system, platform, programme activity, or partnership within your organisation that involves personal data being accessed, stored, or shared outside Kenya.

Keep this example in mind as you work through the module. You will use it to assess whether a cross-border transfer is taking place, what safeguards may be required, and how your organisation can demonstrate compliance.

Examples: *cloud-hosted beneficiary databases, donor reporting platforms, international research partnerships, global safeguarding systems, remote access by consultants, or regional programme management platforms.*

10.2 Objectives

By the end of this module learners should be able to:

- Explain the legal requirements governing cross-border transfers under the DPA 2019 and General Regulations.
- Distinguish between adequacy decisions and appropriate transfer safeguards.
- Evaluate transfer mechanisms including Standard Contractual Clauses, Binding Corporate Rules, and Cross Border Privacy Rules certifications.
- Assess risks associated with cloud hosting and remote access arrangements.
- Identify when critical data infrastructure considerations affect transfer decisions.
- Apply transfer impact assessments before international transfers.
- Develop organisational controls for lawful international data sharing.

10.3 Learning Outcomes

Outcome	Demonstrated Competence
Define Cross-border Transfer	Determine whether a transfer qualifies as a cross-border transfer.
Evaluate transfer mechanisms	Select appropriate transfer mechanisms.
Understand & manage transfer risks	Conduct transfer risk assessments. Manage transfers involving critical and sensitive personal data.
Understand cloud and remote access	Evaluate cloud and remote-access arrangements.
Apply transfer protocols	Implement transfer governance controls.

10.4 Understanding Cross-Border Data Transfers

10.4.1 Legal Foundation

Article 46 of the DPA 2019 and Regulation 26 of the General Regulations provide conditions under which personal data may be transferred outside Kenya.

A transfer occurs whenever personal data becomes accessible from another jurisdiction, regardless of where servers are physically located.

For non-profits, cross-border transfers commonly occur through:

1. International donor reporting
2. Regional programme databases
3. Foreign cloud hosting
4. Global HR/Financial systems
5. International consultants
6. International case management systems
7. Cross-border referral systems
8. Shared humanitarian response platforms

10.4.2 What Constitutes a Cross-Border Transfer?

Transfer Type	Example
Physical transfer	Sending beneficiary records to Uganda office from Kenya (a foreign country)
Cloud hosting	Hosting data on servers in Europe from Kenya (a foreign country)
Remote access	Consultant in Germany accessing Kenyan database
International support desk	Foreign IT vendor accessing records
Regional consortium	Shared East African beneficiary platform

Important principle:
Remote access itself may constitute a cross-border transfer even where the data never physically leaves Kenya.

10.4.3 Four Legal Bases for Cross-Border Transfers

Under Regulation 40, transfers may rely on:

- Adequacy Decisions
- Appropriate Safeguards
- Necessity
- Consent

Participants should understand that not every transfer requires consent. Consent is generally the last option where other transfer mechanisms are unavailable.

10.5 Adequacy Decisions

10.5.1 What is an Adequacy Decision?

An adequacy decision is a determination that another country provides a level of personal data protection substantially equivalent to Kenya's framework.

When adequacy exists:

- Transfers become lower risk.
- Fewer contractual safeguards are required.
- Compliance obligations remain.

10.5.2 Factors Considered During Adequacy Assessments

The assessment generally considers:

- **Data protection legislation:** The assessment looks at whether the country has a comprehensive legal framework governing how personal data is collected, used, stored, shared, and deleted.

- **Independence of supervisory authority:** A supervisory authority is the regulator responsible for overseeing data protection. For example, in Kenya, the Office of the Data Protection Commissioner (ODPC) performs this regulatory role. Adequacy assessments look at whether the regulator is genuinely capable of acting independently, not merely whether a regulator exists.

- **Enforcement mechanisms:** What happens when someone breaks the data protection rules? A country may have excellent legislation, but if nobody enforces it, the protection may exist only on paper.

- **Judicial remedies:** This concerns the ability of individuals to obtain justice through courts or other legally recognised mechanisms when their data protection rights have been violated.

- **Security standards:** Data protection is not only about legal rights; it is also about protecting the data from being compromised. Adequacy assessments therefore consider whether organisations are required to implement appropriate technical and organisational security measures.

- **Rule of law:** Does the country's legal system operate according to predictable, transparent, and enforceable laws? For data protection to work, people need confidence that the law applies not only to ordinary citizens and private companies but also to public authorities.

- **Data Subject Rights:** A data subject is the individual to whom personal data relates. Adequacy assessments therefore ask: what rights do individuals have over their personal data, and can they exercise those rights?

- **Human rights protections:** This demonstrates why data protection cannot be separated completely from broader human rights protections. This is the foundation protecting the dignity and safety of everyone.

Case Study

Rwanda provides a useful regional example of how a country can establish a national framework for protecting personal data and regulating privacy. The framework is anchored in Law No. 058/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy, which was officially gazetted in October 2021. The law establishes rules for the collection, use, storage, sharing, transfer and other forms of processing of personal data. It applies not only to organisations established in Rwanda but, in certain circumstances, also to organisations outside Rwanda that process the personal data of individuals located in Rwanda.

Rwanda presents an important regional example because it has established:

- Comprehensive data protection legislation.
- A supervisory authority.
- Cross-border transfer provisions.
- Security obligations.

Adequacy is not assumed simply because a country is within East Africa. Membership in a regional bloc alone does not automatically create adequacy. A formal assessment must still be conducted. Each transfer requires an assessment of safeguards and applicable legal obligations.

10.6 TRANSFERS BASED ON APPROPRIATE SAFEGUARDS

10.6.1 Appropriate Safeguards Overview

Transfers may proceed where appropriate safeguards ensure a level of protection equivalent to Kenyan law. Appropriate safeguards are legal, technical and organisational measures used to ensure that personal data transferred outside Kenya continues to receive a level of protection that is substantially equivalent to the protection provided under Kenyan data protection law.

Under Kenya's data protection framework, international transfers of personal data should not result in individuals losing the protections they would have enjoyed if their data remained in Kenya. Safeguards therefore help manage the risks that may arise when personal data is transferred to another country or international organisation.

10.6.2 The Malabo Convention

The Malabo Convention seeks to, among other objectives, harmonize the laws of member states on data protection and encourage member states to create frameworks to protect personal data within the continent

(refer to module 3). Participants should understand:

- Purpose of the Convention
- Ratification requirements
- Relationship to Kenyan law
- Limitations of relying solely on ratification

Ratification strengthens adequacy prospects but does not automatically authorise transfers.

10.6.3 Transfer Mechanisms used to demonstrate Appropriate Safeguards

10.6.3 A. Reciprocal Data Protection Agreements (RDPAs)

An RDPA is typically a bilateral or multilateral arrangement between countries that agree to recognize and uphold comparable data protection standards. It establishes mutual recognition of data protection standards between countries. The ODPC guidance identifies RDPAs as one of the mechanisms that may constitute appropriate safeguards for transfers.

Organisational Reflection

Suppose Kenya and Rwanda enter into a Reciprocal Data Protection Agreement.
A Kenyan NGO transferring beneficiary data to a partner organisation in Rwanda may rely on the fact that both jurisdictions have mutually recognised data protection standards.
The agreement operates at the country level.

10.6.3 B. Standard Contractual Clauses (SCCs)

Standard Contractual Clauses (SCCs) are legally binding contractual provisions requiring recipients to protect personal data to prescribed standards. These legally binding clauses are inserted into contracts between the transferring organisation and the receiving organisation. It establishes contractual safeguards between the transferring organisation and the receiving organisation.

Reflective Practice
Non-profits use: International donors, foreign cloud providers, international research partners, and Global technology vendors.

Example

A Kenyan NGO uses a cloud service provider in Germany.

Even if no RDPA exists between Kenya and Germany, non-profits can use SCCs to contractually require the provider to:

- Protect personal data.
- Limit the use of the data.
- Notify breaches.
- Restrict onward transfers.
- Submit to audits.

SCCs operate at the organization level.

Risks of SCCs

- *Not sufficient alone if recipient country laws undermine protections.*

10.6.3 C. Binding Corporate Rules (BCRs)

BCRs are internal privacy rules governing transfers within multinational organisations. BCRs are legally enforceable internal privacy rules adopted by a multinational group of organisations to govern transfers of personal data within the group across different countries. BCRs are intra-group safeguards. BCRs are typically used by organizations such as: International NGOs with country offices; Multinational companies; Federated organisations; and Global humanitarian agencies.

Elements of Valid BCRs

Requirement	Description
Scope	Categories of transfers covered
Binding Nature	Legally enforceable; approved by regulators
Accountability	Monitoring and audits; consistent protection across entities
Complaint Handling	Data subject remedies
Third Country Laws	Conflict reporting
Updates	Change management
Audits	Compliance verification

Example

A global NGO operates offices in: Kenya, Uganda, Rwanda, Germany, and the United States. Programme data collected in Kenya may need to be accessed by regional and global offices.

Instead of signing separate SCCs between every office, the NGO develops BCRs that apply across the entire organisation.

BCRs are based on the internal governance structure of the organisation.

10.6.3 D. Cross Border Privacy Rules (CBPR)

The CBPR framework promotes accountability-based international transfers. CBPRs are an accountability-based framework under which organisations voluntarily demonstrate compliance with recognised privacy standards through certification and ongoing monitoring.
Unlike SCCs and BCRs, CBPRs do not primarily rely on contracts or organisational hierarchy. Instead, they rely on:

- Demonstrated privacy practices
- External verification
- Accountability mechanisms
- Continuous compliance

CBPR is based on certified privacy governance and accountability practices rather than a specific contract or corporate structure.

CBPR does not replace Kenyan legal requirements. Instead, it can provide additional assurance that an organisation follows internationally recognised privacy practices.

Summary of Transfer Mechanisms used to demonstrate Appropriate Safeguards

Mechanism	Primary Purpose	Typical User	Safeguard Type
Reciprocal Data Protection Agreement (RDPA)	Mutual recognition between jurisdictions	Governments	Jurisdiction-level safeguard
Standard Contractual Clauses (SCCs)	Contractual protection between organisations	NGOs, vendors, donors	Contractual (organization-level) safeguard
Binding Corporate Rules (BCRs)	Internal transfers within a group	International NGOs, multinationals with regional and global offices	Intra-group safeguard
Cross-Border Privacy Rules (CBPRs)	Demonstrate recognised privacy governance	Technology providers, multinationals	Certification and accountability safeguard

10.7 TRANSFERS BASED ON NECESSITY

10.7.1 Transfer as Necessity

The Data Protection Act, 2019 and the Data Protection (General) Regulations recognise that certain cross-border transfers may be necessary to enable organisations to perform essential functions, protect individuals, comply with legal obligations, or serve important public interests.

Transfer as necessity is a distinct lawful basis from adequacy decisions, appropriate safeguards, and consent. It applies only where the transfer is objectively required for a specific lawful purpose and where that purpose cannot reasonably be achieved without the transfer.

The burden rests on the data controller or processor to demonstrate and document why the transfer was necessary and proportionate in the circumstances.

A cross-border transfer may be lawful where necessary for:

Lawful Basis	Example
Contract Performance	The transfer is necessary to perform a contract with the data subject or to take steps requested by the data subject before entering into a contract e.g. international payroll platform.
Legal Claims	The transfer is necessary for the establishment, exercise, or defence of a legal claim e.g. Cross-border litigation involving beneficiaries.
Vital Interests	The transfer is necessary to protect the life, health, or physical integrity of a person who is incapable of giving consent e.g. Emergency referral during humanitarian crises.
Legitimate Interests	The transfer is necessary to pursue compelling legitimate interests that do not override the rights and freedoms of the data subject e.g. Hosting programme systems on foreign cloud infrastructure.
Public Interest	The transfer is necessary for an important public interest recognised by law e.g. Disease surveillance and epidemic response.
Updates	Change management
Audits	Compliance verification

10.7.2 Necessity Decision Test

Before relying on necessity, organisations should ask:

Step 1 - Identify the Purpose
What objective is the transfer intended to achieve?

Step 2 - Assess Necessity
Is the transfer genuinely needed to achieve that objective?

Step 3 - Consider Alternatives
Can the objective be achieved without transferring personal data or by transferring less data?

Step 4 - Apply Data Minimisation
Is only the minimum necessary personal data being transferred?

Step 5 - Document the Decision
Can the organisation demonstrate why reliance on necessity was appropriate?

Key Principle
Transfer as a necessity is not a blanket exemption from data protection obligations. Even where necessity applies, organisations must continue to comply with the principles of lawfulness, purpose limitation, data minimisation, security, transparency, and accountability.

10.8 TRANSFERS BASED ON CONSENT

10.8.1 Consent as a Transfer Basis

Cross-border transfers may be conducted on the basis of consent where no adequacy decision exists, no appropriate safeguards are available, and no other lawful basis justifies the transfer.

Consent serves as a residual transfer mechanism and should not be treated as the default basis for international data sharing. Organisations should first consider whether the transfer can be justified through adequacy, appropriate safeguards, or necessity before relying on consent.

When consent is used, the organisation must be able to demonstrate that the data subject was fully informed about the proposed transfer, understood the associated risks, and freely agreed to the transfer. Where consent is relied upon for a cross-border data transfer, it must satisfy all requirements for valid consent under the Data Protection Act, 2019 and the Data Protection (General) Regulations, 2021.

Consent should generally be used where:

- No adequacy decision exists.
- No safeguard exists.
- No necessity ground exists.

Before obtaining consent for a cross-border transfer, organisations should inform the data subject of:

- The purpose of the transfer.
- The categories of personal data being transferred.
- The country or countries where the data will be transferred.
- The identity of the receiving organisation.
- The intended use of the personal data.
- Whether additional recipients may access the data.
- The risks associated with transferring the data.
- The right to withdraw consent.

The information should be communicated in clear and understandable language appropriate to the context and data subjects.

10.8.2 Additional Requirements for Sensitive Data

The ODPC Guidance Note emphasises that cross-border transfers involving sensitive personal data require enhanced protection and explicit consent from the data subject together with confirmation that appropriate safeguards exist.

Examples of sensitive personal data include:

- Health information
- Biometric data
- Genetic information
- Ethnic origin
- Religious beliefs
- Sexual orientation
- Children's information
- Family information

10.8.3 Consent Withdrawal

Data subjects retain the right to withdraw consent at any time. Organisations relying on consent should establish mechanisms to:

- Receive withdrawal requests.
- Cease future transfers where feasible.
- Inform recipients where appropriate.
- Document actions taken following withdrawal.

Withdrawal does not affect the lawfulness of transfers conducted before consent was withdrawn.

Organisational Reflection
A Kenyan Non-Profit is conducting a nutrition study with a university located outside Kenya. The university intends to receive participant-level data for analysis.

Before transferring the data, the non-profit:

1. Explains the purpose of the research.
2. Identifies the recipient institution.
3. Explains where the data will be processed.
4. Describes potential risks associated with the transfer.
5. Obtains explicit written consent from participants.
6. Maintains records demonstrating consent was obtained.

Where sensitive health information is involved, additional safeguards should also be implemented.

10.8.4 Consent Assessment Framework

Before relying on consent for a cross-border transfer, ask:

Step 1 – Is another transfer basis available?

Consider adequacy, appropriate safeguards, or necessity first.

Step 2 – Can consent be freely given?

Assess any dependency or vulnerability concerns.

Step 3 – Have transfer risks been explained?

Ensure the data subject understands potential consequences.

Step 4 – Has consent been documented?

Maintain evidence of consent.

Step 5 – Can withdrawal be operationalised?

Ensure procedures exist to manage withdrawal requests.

Key Principle

Consent should not be used as a substitute for appropriate safeguards or transfer governance measures. Even where consent is relied upon, organisations remain responsible for ensuring that personal data transferred outside Kenya is protected through appropriate technical, organisational, and contractual safeguards.

10.9 Cloud Services and Remote Access

10.9.1 Cloud Services as Cross-Border Transfers

Non-profit organisations increasingly rely on cloud-based technologies to support programme implementation, beneficiary management, donor reporting, collaboration, and data storage. While cloud services provide flexibility, scalability, and cost efficiencies, they also create significant data protection obligations

where personal data is stored, processed, or accessed outside Kenya.
According to the ODPC Guidance Note, processing personal data in cloud environments hosted outside Kenya constitutes a cross-border transfer of personal data. Organisations remain responsible for ensuring that personal data is protected regardless of where it is stored or processed.

Examples of commonly used cloud services include:

- Microsoft 365
- Google Workspace
- Salesforce
- Kobo Toolbox
- District Health Information System 2
- Amazon Web Services
- Microsoft Azure
- Dropbox
- SharePoint
- International safeguarding platforms

10.9.2 Shared Accountability in Cloud Environments

The use of a cloud service provider does not transfer legal responsibility for data protection to the provider. The ODPC Guidance Note emphasises that data controllers and cloud service providers share responsibility for protecting personal data. This includes conducting due diligence before engagement and continuously monitoring compliance throughout the relationship.

Non-profit organisations remain accountable for:

- Selecting compliant providers.
- Establishing lawful transfer mechanisms.
- Conducting risk assessments.
- Implementing security controls.
- Monitoring service providers.
- Protecting data subject rights.

10.9.3 Cloud Service Models

ODPC identifies three common cloud service models (these are listed below). The level of organisational control decreases as responsibility shifts from Infrastructure as a Service (IaaS) to Software as a Service (SaaS) environment. SaaS solutions generally require enhanced vendor due diligence because organisations have less direct control over data handling practices.

Model	Description	NGO Example
Infrastructure as a Service (IaaS)	Provider supplies computing infrastructure while the organisation manages applications and data.	AWS Virtual Servers

Platform as a Service (PaaS)	Provider supplies infrastructure and development environment.	Microsoft Azure Platform Services
Software as a Service (SaaS)	Provider supplies complete software solution.	Microsoft 365, Salesforce, Google Workspace

10.9.4 Cloud Deployment Models

Cloud environments may be deployed through different models:

Model	Characteristics
Private Cloud	Dedicated infrastructure for a single organisation, offering greater control and privacy protections.
Public Cloud	Shared infrastructure used by multiple organisations, potentially introducing additional privacy and security risks.

The ODPC recommends that organisations conduct thorough privacy and security assessments before adopting public cloud solutions.

10.9.5 Remote Access as a Transfer Event

A cross-border transfer may occur even where personal data remains physically stored in Kenya.
Where an individual located outside Kenya remotely accesses, views, downloads, or processes personal data held within Kenya, personal data has effectively become accessible across borders.

Scenario:
A programme database remains hosted in Nairobi.
A consultant in Brussels logs in remotely.
This may constitute a cross-border transfer because personal data becomes accessible outside Kenya.
Required safeguards include:

- Access controls.
- Encryption.
- Transfer agreements.
- Logging and monitoring.

10.10 Critical Data Infrastructure and Sensitive Data

10.10.1 Understanding Critical Information Infrastructure and High-Risk Data

Not all personal data presents the same level of risk when transferred across borders. Certain categories of data and systems are considered particularly sensitive because unauthorised access, loss, disclosure,

or disruption could result in significant harm to individuals, communities, or the public interest.
The Data Protection Act, 2019 and the Data Protection (General) Regulations, 2021 impose additional obligations where personal data relates to strategic interests of the State, critical information infrastructure, or sensitive personal data.
For non-profit organisations, this is particularly important when operating health programmes, education initiatives, child protection systems, safeguarding mechanisms, refugee support programmes, and humanitarian response activities.

10.10.2 Strategic Interests of the State and Data Localisation

Section 50 of the Data Protection Act requires certain categories of personal data connected to the strategic interests of the State to be domiciled within Kenya. Where applicable, organisations may be required to process the data through infrastructure located in Kenya or maintain a serving copy within the country.

Under Regulation 26, activities considered to involve strategic interests include:

- Civil registration and legal identity systems.
- Electoral systems.
- Public finance management systems.
- Protected computer systems.
- Early childhood and basic education systems.
- Primary and secondary healthcare systems.

10.10.3 Critical Information Infrastructure

Critical Information Infrastructure (CII) refers to information systems, networks, databases, and services whose disruption, compromise, or loss could negatively affect essential services, public welfare, national security, or economic stability.

Examples that may affect non-profit organisations include:

Sector	Example System
Health	Electronic Medical Records (EMRs)
Education	Learner Management Systems
Child Protection	National child welfare databases
Humanitarian Response	Refugee registration and protection systems
Public Health	Disease surveillance platforms
Social Protection	Cash transfer and beneficiary management systems

Where these systems involve cross-border processing, additional scrutiny and safeguards should be applied.

10.10.4 Accountability Tests for High-Risk Transfers

Every transfer involving critical systems or sensitive personal data should pass the following tests:

Test	Question
Necessity	Is the transfer genuinely required?
Proportionality	Is only the minimum necessary data being transferred?
Accountability	Can the organisation demonstrate compliance if audited by the ODPC?

Example:

1. A health NGO uses a cloud-based Electronic Medical Records system hosted outside Kenya. Before transferring patient information, the organisation should:

- Assess localisation requirements.
- Conduct a Transfer Impact Assessment.
- Verify provider safeguards.
- Implement encryption and access controls.
- Ensure a serving copy is maintained where required.

2. A humanitarian organisation transfers refugee case management information to a regional protection coordination platform.

The organisation should:

- Assess transfer risks.
- Evaluate recipient safeguards.
- Ensure compliance with transfer agreements.
- Monitor access to the data.
- Maintain accountability records.

Key Principle

The more sensitive the personal data and the more critical the underlying system, the greater the responsibility on the organisation to justify the transfer, implement enhanced safeguards, and demonstrate accountability. Cross-border transfers involving health, education, child protection, refugee, and safeguarding data require particularly careful assessment and governance.

10.11 Transfer Impact Assessment (TIA)

10.11.1 Understanding Transfer Impact Assessments

Before transferring personal data outside Kenya, organisations must understand and evaluate the risks associated with the transfer. A Transfer Impact Assessment (TIA) is a structured process used to determine whether personal data will remain adequately protected once it leaves Kenya and whether the proposed safeguards are sufficient to protect the rights and freedoms of data subjects.

A TIA helps organisations identify legal, technical, operational, and security risks associated with cross-border transfers and provides evidence that appropriate due diligence was conducted before the transfer took place.

For non-profit organisations, TIAs are particularly important where personal data is transferred to cloud service providers, international donors, regional programme partners, research institutions, safeguarding platforms, or service providers located outside Kenya.

10.11.2 Purpose of a Transfer Impact Assessment

A Transfer Impact Assessment helps an organisation:

- Understand where personal data is being transferred.
- Identify risks associated with the receiving jurisdiction.
- Evaluate the adequacy of transfer safeguards.
- Determine whether additional protection is required.
- Demonstrate accountability and compliance.
- Support decision-making before the transfer occurs.

A properly documented TIA may also assist the organisation in demonstrating compliance during audits, investigations, or regulatory reviews.

10.11.3 When should a TIA Be Conducted?

A TIA should be considered where:

- Personal data is transferred outside Kenya.
- Cloud services are hosted outside Kenya.
- International organisations access programme data.
- A new international partner receives personal data.
- Sensitive personal data is involved.
- There are concerns about the legal environment in the receiving country.
- Remote access to personal data is provided to persons located outside Kenya.
- Significant changes occur to existing transfer arrangements.

10.11.4 Five-step Transfer Impact Assessment Framework

Steps	Action	Questions to Ask
Step 1	Map the Transfer Clearly identify: • What data is being transferred. • Who is transferring the data. • Who will receive the data. • Where the data will be transferred. • The purpose of the transfer.	What categories of personal data are involved? Does the transfer include sensitive personal data? Is the transfer a one-time activity or ongoing?
Step 2	Assess the Receiving Country or Jurisdiction Evaluate the destination country's data protection environment. Consider: • Existence of data protection legislation. • Regulatory oversight. • Enforcement mechanisms. • Privacy protections. • Cybersecurity maturity. • Human rights protections.	Does the country have a data protection authority? Are there effective legal remedies for data subjects? Are there known concerns regarding government access to data?
Step 3	Assess the Receiving Organisation Evaluate whether the recipient can adequately protect personal data. Review: • Information security controls. • Data protection policies. • Incident response procedures. • Vendor management practices. • Previous compliance history.	Has the recipient experienced recent data breaches? Does the organisation have a Data Protection Officer? Are staff trained in data protection and cybersecurity?
Step 4	Evaluate Transfer Safeguards Assess the safeguards that will protect the data during and after transfer. Possible safeguards include: • Standard Contractual Clauses (SCCs) • Binding Corporate Rules (BCRs) • Reciprocal Data Protection Agreements • Encryption • Access controls	Are the safeguards legally enforceable? Are they sufficient for the sensitivity of the data? Can compliance be independently verified?

	• Data minimisation • Transfer agreements • Audit rights	
	Determine Residual Risk and Decide After considering all safeguards, determine whether any remaining risks are acceptable. The final decision and supporting rationale should be documented.	Possible outcomes include: Outcome and Action **Low Risk** Proceed with transfer **Medium Risk** Proceed with additional safeguards **High Risk** Escalate for management or DPO review **Unacceptable Risk** Do not proceed with transfer

10.11.5 TIA Documentation Requirements

The following information should be retained:

- Date of assessment.
- Assessor's name and role.
- Description of transfer.
- Countries involved.
- Recipient details.
- Risks identified.
- Safeguards evaluated.
- Final decision.
- Approval authority.

The TIA should be reviewed periodically, particularly where:

- The transfer changes.
- New recipients are added.
- The legal environment changes.
- New risks emerge.

Key Principle
A Transfer Impact Assessment is not a one-time compliance exercise. It is an ongoing risk management tool that helps organisations determine whether personal data can be transferred outside Kenya safely, lawfully, and in a manner that protects the rights and freedoms of data subjects.

10.12 Key Takeaways

- Cross-border transfers include both physical transfers and remote access.
- Adequacy decisions reduce transfer risks but do not eliminate compliance obligations.
- SCCs, BCRs, and CBPRs are important transfer mechanisms but must be supported by accountability measures.
- Cloud hosting and international vendor access require transfer assessments.
- Sensitive and critical infrastructure data requires enhanced safeguards.
- Every non-profit should maintain a documented cross-border transfer programme.
- Accountability, transparency, and risk assessment remain central to lawful international data sharing.

10.13 Assessment Questions

Part A: Knowledge and Conceptual Understanding

- What makes a data transfer "cross-border"?
- Does remote access to personal data from another country constitute a cross-border transfer? Explain.
- Does remote access from another country constitute a cross-border transfer? Explain.
- What is the difference between adequacy and Standard Contractual Clauses (SCCs)?
- What are Standard Contractual Clauses (SCCs) and when are they used?
- What are Binding Corporate Rules (BCRs)?
- What rights should data subjects retain when their personal data is transferred internationally?

Part B: Applied Analysis

1. An employee in Kenya accesses beneficiary data while travelling abroad. Does this constitute a cross-border transfer? Explain.
2. A donor requests access to beneficiary-level data hosted in Europe. What transfer assessment should be performed first?
3. What safeguards should be implemented when using a global cloud service provider?
4. An NGO wants to transfer personal data to a country without an adequacy decision. What options are available?
5. What factors should be considered before transferring sensitive or vulnerable persons' data internationally?
6. What should an organisation do if the risks of an international transfer cannot be adequately mitigated?

Part C: Organizational Reflection

1. Your organisation uses a cloud service provider with support staff located globally. What safeguards should be implemented?
2. Are international transfer requirements included in your organisation's contracts with third parties?
3. How does your organisation assess the risks of transferring sensitive or vulnerable persons' data internationally?

11.

Setting Up a Privacy Program

About This Module

This module forms part of the Data Protection Toolkit for Nonprofit Organisations. It builds directly on the foundation laid in the previous ten modules: privacy and personal data (Modules 1–2), the legal and regulatory framework and the Data Protection Act, 2019 (Modules 3–4), the principles of data protection (Module 5), lawful bases and consent (Modules 6–7), the rights of data subjects (Module 8), the obligations of data handlers (Module 9), and cross-border data transfers (Module 10). Having established what the law requires, this module moves from understanding to implementation. It is a practical, operational guide to establishing, running, and monitoring a privacy programme within a nonprofit organisation, covering the structures, tools, processes, and documentation that responsible data governance requires.

The module addresses thirteen interconnected components of a functional privacy programme, from data mapping and the Record of Processing Activities through to Data Protection Impact Assessments, ODPC registration, data sharing, classification, incident management, cross-border transfers, technical and organisational measures, policies and notices, audit readiness, the role of the Data Protection Officer, and programme monitoring.

11.1 What is a programme?

Ask a programme officer at any nonprofit to describe their livelihoods programme, their WASH programme, or their child protection programme, and they will not hesitate. They will tell you its name, who it serves, what it is trying to achieve, what activities it runs, who is responsible for it, how it is funded, and how its results are tracked. They understand, instinctively, that a programme is not a single activity or a single document. It is a coordinated, ongoing body of work, organised around a clear purpose, sustained over time, and accountable to somebody.

A privacy programme is no different. It is simply a programme whose "beneficiaries" are the data subjects whose personal data the organisation holds, whose "outcome" is the lawful, fair, and secure handling of that data, and whose "activities" are the thirteen components this module goes on to describe. Organisations that already run structured, well-governed programmes in other areas of their work are, in truth, halfway to running a good privacy programme. What is missing is usually not capacity. It is the recognition that privacy deserves the same programmatic treatment as any other area of organisational work.

11.2 Elements of a good programme?

Whether it delivers clean water, protects children, or protects personal data, a genuine programme, as opposed to a loose collection of good intentions, tends to share the following elements. Each is worth pausing on, because each is also a diagnostic: an organisation can test the health of its own privacy programme, or the absence of one, against every item on this list.

- **A name.** A programme that people can name is a programme people can find, fund, staff, report on, and hold accountable. "The stuff we do about data" is not a programme; it is an unassigned worry that circulates informally among whichever staff members happen to notice a problem. "The [Organisation Name] Privacy Programme" is a programme: it can appear on an organogram, in a budget line, in a donor report, and in a staff member's job description. Naming it is a small act with disproportionate consequences. It is the first act of taking the work seriously, and the first step toward giving privacy a visible place in the organisation's structure alongside its other named programmes.

- **A defined purpose and scope.** What is this programme trying to achieve, and what does it cover? A privacy programme exists to protect the personal data the organisation processes, in service delivery, in fundraising, in human resources, in research, and in partnership and donor reporting, across every department, project, field office, and system where that processing happens. A scope that quietly stops at head office or covers only the flagship programme while leaving field offices, volunteers, and partner organisations untouched, is not a real scope. It is a description of wherever the organisation happened to find it convenient to look.

- **An owner.** Every credible programme has someone who is accountable for it, even where many people contribute to it. A livelihoods programme has a programme manager even though field officers, finance staff, and partners all play a role. A privacy programme is no different: it needs a named owner, ordinarily the Data Protection Officer, discussed later in this module, who can

answer for the programme's performance even while day-to-day privacy responsibilities are distributed across many roles. Without an owner, a privacy programme becomes everybody's shared concern and, in practice, nobody's specific job.

- **A defined set of activities or components.** A programme is made up of identifiable, describable parts, not a single undifferentiated effort. This module's thirteen components (data mapping, ROPA, DPIA, ODPC registration, data sharing, classification, incident management, cross-border transfers, technical and organisational measures, policies and notices, audit readiness, and the DPO role) are the working parts of the privacy programme, in the same way that "borehole rehabilitation" or "hygiene promotion" might be the working parts of a WASH programme. Naming the components is what turns "we take data protection seriously" from a sentiment into a workplan.

- **Resources.** A programme without a budget, time, or people attached to it is an aspiration, not a programme. Even a modest privacy programme requires designated staff time, however small a percentage of a role; some budget for tools, storage, or training; and visible support from leadership when trade-offs arise, for instance between speed of data collection and the rigour of consent procedures. Organisations that assign privacy responsibilities without any of the resources needed to carry them out are, in effect, setting the programme up to fail while appearing, on paper, to have addressed the requirement.

- **Governance and oversight.** Someone, or somebody, such as senior management, an executive committee, or a board, must be able to ask how the programme is doing and receive a credible, evidenced answer, not a reassurance. This means privacy has a reporting line: a point at which programme performance, incidents, and risks are escalated upward and reviewed, rather than absorbed silently by whoever happens to be closest to the problem.

- **Documentation**. Programmes leave a paper trail: plans, policies, records, reports. A privacy programme that exists only in the heads, and good intentions, of a few experienced staff members is not resilient. It cannot survive staff turnover, it cannot be audited, and it cannot be demonstrated to a regulator, a donor, or an affected individual who asks, reasonably, how their information is being protected. If it is not written down, it is not yet a programme.

- **Monitoring and evaluation.** A programme without a way of measuring its own performance cannot improve, and cannot demonstrate, to itself or to anyone else, that it is working. This might be as simple as an annual self-assessment against the thirteen components, or as structured as a dashboard tracking indicators such as outstanding data subject requests, overdue DPIAs, or unresolved incidents. The final component of this module addresses exactly this for the privacy programme.

- **Continuity.** Unlike a single project with a start and an end date, a genuine programme is not a one-off exercise that concludes when a policy is signed or a training is delivered. It runs, adapts, and renews itself over time, in the same way an education programme continues from one cohort to the next regardless of which teacher is currently assigned to it. A privacy programme that depends entirely on one committed individual, and quietly lapses the day that person leaves, was never a programme. It was a personal habit that happened to benefit the organisation while it lasted.

Understood this way, setting up a privacy programme is not an unfamiliar or purely legal exercise. It is the application of programme management discipline that most nonprofits already possess, in their other areas of work, to a subject matter, personal data, that has, until now, too often been left without one. What remains is to see why that discipline is not optional.

11.2 Objectives

1. To equip learners with the knowledge and practical tools required to design, establish, and operate a functional privacy programme within their organisation.
2. To explain how to map personal data processing, maintain a Record of Processing Activities (ROPA), and apply data classification as a proportionate, risk-based tool for handling different categories of personal data.
3. To introduce Data Protection Impact Assessments and the technical and organisational measures that together form an adequate baseline of safeguards, establishing when, why, and how each must be applied.
4. To address the requirements for responsible data sharing, both within the organisation and with external partners, and the conditions and safeguards applicable to transferring personal data outside Kenya.
5. To establish the legal and practical requirements for incident management and breach reporting, including the applicable regulatory thresholds, and to define the role of the Data Protection Officer as an institutional function responsible for this and other aspects of the programme.
6. To provide practical guidance on ODPC registration, the policies and notices required for transparency and accountability, and audit readiness, and to introduce a monitoring framework and dashboard for tracking the ongoing health of the privacy programme against ODPC oversight expectations.

11.3 Learning Outcomes

Outcome	Demonstrated Competence
Conduct data mapping	Produce a data map for a significant organizational processing activity, identifying data categories, purposes, access, sharing, and risk levels.
Maintain a ROPA	Explain what a Record of Processing Activities is, what it must contain, and how it connects to lawful basis and the data lifecycle.
Conduct or commission a DPIA	Explain when a DPIA is required, describe its key stages, and identify the criteria used to assess high-risk processing.
Establish and maintain compliance with ODPC regulatory requirements.	Evaluate the organisation's status as a data controller or data processor under Kenyan law, to complete the ODPC registration process where applicable, and to implement measures that keep the organisation prepared for ODPC compliance reviews or audits.
Establish data sharing arrangements	Explain the conditions for lawful data sharing and the requirements of a data sharing agreement.

Apply data classification	Assign classification levels to categories of personal data held by the organization and describe the handling requirements for each level.
Manage data incidents and breaches	Describe the organization's incident response obligations, including the regulatory reporting threshold and timelines under the Regulations.
Incorporate cross-border personal data transfer controls into the organisation's privacy programme	Assess whether a processing activity involves the transfer of personal data outside Kenya, determine the applicable transfer safeguard, and embed a review step so that any new or changed cross-border transfer is assessed before it takes place.
Implement technical and organizational measures	Identify the baseline technical and organizational measures applicable to Not-for-Profit organizations and assess current gaps.
Produce required policies and notices	Identify which policies and notices the organization must have, explain what each must contain, and assess current gaps.
Prepare for regulatory audit	Describe the key areas of ODPC audit focus and identify the documentation and processes that must be in place to demonstrate compliance.
Define and operationalize the DPO role	Explain the DPO as an institutional function, describe the qualifications and independence requirements, and identify how the role applies to Nonprofit organizations.
Monitor the privacy programme	Use the privacy programme monitoring dashboard to track programme health, identify gaps, and cross-reference against ODPC oversight expectations.

11.3 Introduction

Understanding data protection law is necessary, but it is not sufficient. An organisation that can explain what a lawful basis is, or list the categories of sensitive personal data, has acquired important knowledge. Knowledge alone, however, does not protect individuals whose information the organisation holds. What protects them, and what satisfies the requirements of the Data Protection Act, 2019, is operational implementation: the processes, structures, tools, documentation, roles, and oversight mechanisms that together constitute a functioning privacy programme.

This module addresses the practical question that follows naturally from Modules 1 to 10: given what we now know about privacy, personal data, and the legal framework, what does our organisation need to do? The answer is the design and operation of a privacy programme, a structured, systematic, and accountable approach to managing all personal data within the organisation, from the moment it is collected to the moment it is securely disposed.

A privacy programme is not a single document, and it is not a one-time compliance exercise. It is an ongoing operational commitment. It encompasses the organisation's understanding of what data it holds and why; the legal grounds on which it processes that data; the agreements it has with partners and service providers; the technical safeguards it maintains; the policies and notices it publishes; the processes it follows when things go wrong; the registration and oversight obligations it meets in relation to the Office of the Data Protection Commissioner; and the monitoring mechanisms it uses to verify that the programme remains effective over time.

For nonprofit organisations, building a privacy programme is not a bureaucratic exercise. It is an expression of commitment to the dignity, safety, and rights of the individuals and communities the organisation serves. The communities most nonprofits work with, including displaced persons, survivors of violence, people living in poverty, persons with disabilities, children, and members of marginalised groups, are precisely those for whom privacy failures carry the most serious consequences. A functioning privacy programme is therefore not only a legal obligation; it is a professional and ethical responsibility.

This module is structured around thirteen programme components. Each is examined in turn, with its legal foundation, operational requirements, practical tools, and common implementation challenges. Taken together, the thirteen components provide a complete operational framework for any nonprofit organisation seeking to manage personal data responsibly and in compliance with Kenyan law.

Reflective Practice

Using the nine elements of a programme, take stock of how your organisation currently handles personal data, not as a compliance checklist, but as an honest programmatic self-assessment.

1. Does your organisation's data protection work have a name, or is it currently an informal, unassigned responsibility?
2. Can you describe its scope in one sentence? Does that scope genuinely cover every department, field office, project, and partner, or only the parts that are easiest to see?
3. Who, by name or by role, is currently accountable for privacy in your organisation? If a donor or the ODPC asked tomorrow, who would answer?
4. What staff time, budget, or tools are currently allocated to privacy work? Is this enough to do the work that is being asked, or expected?
5. If something went seriously wrong, a data breach, a misdirected dataset, an unlawful disclosure, who above the immediate team would find out, and how quickly?
6. Where does your organisation's privacy-related knowledge currently live: in written policies and records, or mainly in the memory of one or two experienced staff?
7. Does anyone currently track how well your data protection efforts are working, or would you only find out they had failed after something went wrong?
8. If the staff member most responsible for data protection in your organisation left tomorrow, would the work continue, or would it stop with them?

11.3 The Thirteen Components at a glance

The components in this module are sequenced to follow the order a nonprofit would sensibly build them in practice, not an arbitrary list. You start by finding out what data you hold and how sensitive it is, formalise that into a living record, and appoint someone to own it. Only then does it make sense to assess risk, put safeguards and policies in place, govern how data moves in and out of the organisation, prepare to respond when something goes wrong, and finally, once all of that is genuinely in place, declare it to the regulator through registration.

FOUNDATIONS	01 Data Mapping 02 Data Classification 03 Record of Processing Activities
GOVERNANCE	04 The Data Protection Officer
RISK & SAFEGUARDS	05 Data Protection Impact Assessments 06 Technical & Organisational Measures 07 Policies & Notices
DATA IN MOTION	08 Data Sharing Arrangements 09 Cross-Border Data Transfers
RESPONSE & ASSURANCE	10 Incident Management & Breach Reporting 11 Audit Readiness 12 Monitoring the Programme
REGULATORY STANDING	13 ODPC Registration & Self-Audit

1. COMPONENT 01 · FOUNDATIONS

Data Mapping

Data mapping is the foundation on which every other component of the privacy programme rests. It is the exercise of tracing what personal data an organisation holds, where it comes from, how it moves, who touches it, where it is stored, and when and how it is eventually disposed of. Module 2 introduced the data lifecycle and the Basic Data Mapping Template as conceptual tools; this section turns that concept into an ongoing organisational practice, not a one-off classroom exercise.

An organisation cannot protect data it cannot describe. Many nonprofits discover, the first time they attempt a proper data mapping exercise, that personal data is being held in places nobody had previously accounted for: a programme officer's personal WhatsApp, a volunteer's personal laptop, a paper register in a field office cabinet, or a spreadsheet emailed to a donor two years ago and never deleted from anyone's inbox. Mapping surfaces these blind spots before they become incidents.

How to Conduct a Data Mapping Exercise

- **Identify processing activities.** List every activity, by department and by programme, that involves personal data: beneficiary registration, staff payroll, volunteer management, donor CRM, M&E surveys, case management, and so on.
- **Interview process owners.** Speak to the staff who run each activity, not only their managers. The person entering data daily usually knows more about where it really goes than the policy says it should.
- **Trace the full flow.** For each activity, follow the data from collection, through use and storage, to sharing and eventual disposal, noting every system, device, and person it passes through.
- **Document systematically.** Record data categories, purpose, legal basis, retention period, who has access, who it is shared with, and an initial risk rating for each processing activity.
- **Visualise the flow**. A simple flow diagram, even hand-drawn, often reveals unnecessary duplication or unsafe hand-offs that a written list does not.

Practical Tool: Data Mapping Register

Build on the Basic Data Mapping Template introduced in Module 2 by turning it into a living register with, at minimum, the following columns:

- Processing activity and responsible department
- Data categories collected (and whether any are sensitive personal data)
- Source of the data and method of collection
- Purpose and lawful basis
- Storage location(s) and format (paper, local device, cloud)
- Recipients or third parties the data is shared with, including cross-border recipients
- Retention period and disposal method
- Risk rating and date last reviewed

Common challenges include data held outside official systems ("shadow data" on personal devices or messaging apps), data inherited from predecessor projects with no institutional memory of its purpose, and decentralised field offices that maintain their own informal records. A realistic mapping exercise treats these as expected findings to be brought into the register, not as embarrassment to be hidden.

Getting Started This Week

- Pick one programme or department and list every activity this week that touches personal data.
- Assign one staff member per activity to walk you through what happens to the data, not what the policy assumes happens.
- Open a shared spreadsheet and start the Data Mapping Register with just those first few activities.

2. COMPONENT 02 · FOUNDATIONS

Data Classification

Not all personal data carries the same level of risk, and treating all of it identically is neither efficient nor protective. Data classification is the operational tool that allows an organisation to apply proportionate handling rules: light-touch controls for low-risk information, and strict controls for the data whose exposure could cause the most serious harm.

A Simple Classification Scheme

Level	Handling Requirements
Public	Information intended for public release (e.g., published annual reports). No special handling required.
Internal	Ordinary organisational information not intended for external release, but low risk if seen internally (e.g., internal staff directories). Access limited to staff; no special encryption required.
Confidential	Personal data such as standard beneficiary or staff records. Access restricted to authorised personnel on a need-to-know basis; password protection and controlled sharing required.
Restricted/ Sensitive	Sensitive personal data as defined under Section 46 of the DPA 2019 (health status, biometric data, data on children, data revealing ethnicity or religion, and similar categories), and any data whose exposure could endanger a data subject, such as case files for survivors of violence. Strict access controls, encryption, logging of access, and heightened approval requirements for any sharing.

The classification level assigned to a category of data should flow directly from the data mapping exercise and be recorded in the ROPA, so that classification is not a separate, disconnected exercise but a natural extension of already knowing what data the organisation holds. A common failure mode runs in both directions. Some organisations classify everything as confidential, which is easier in the short term but paralyses ordinary operations and, over time, trains staff to ignore the classification altogether. Others under-classify genuinely sensitive information, such as a survivor's location data, simply because it sits in the same spreadsheet as routine attendance records. Proportionate classification requires deliberate, category-by-category judgment, not a blanket default in either direction.

Getting Started This Week

- Take the data mapping register you started and add one column: classification level.
- Classify your three most sensitive data categories first; do not attempt to classify everything on day one.
- Share the classification scheme with programme leads so they understand what 'Restricted/ Sensitive' means in day-to-day practice.

3. COMPONENT 03 · FOUNDATIONS

Record of Processing Activities (ROPA)

Legal Foundation
The accountability principle under Section 25(h) of the Data Protection Act, 2019, read together with Regulations 39–48 of the Data Protection (General) Regulations, 2021, requires data controllers and processors to be able to demonstrate compliance with the Act. A Record of Processing Activities is the primary evidentiary tool for meeting that obligation.

Where data mapping is the investigative exercise, the ROPA is its formal, ongoing output: a structured, continuously maintained register of every processing activity the organisation carries out. It is not produced once and filed away. It is a living document that is updated whenever a new processing activity begins, an existing one changes, or a periodic review takes place.

A ROPA should be organised so that any single processing activity can be understood at a glance: what data is processed, why, on what legal basis, for how long, by whom, and with what safeguards. This is the document an organisation should be able to produce, with confidence and without a scramble, if the Office of the Data Protection Commissioner requests it during registration, a self-audit, or an inspection.

What a ROPA Must Contain

- The name and contact details of the data controller (and DPO, where designated).
- The purposes of processing for each activity.
- Categories of data subjects and categories of personal data, flagging any sensitive personal data.
- The lawful basis relied on for each activity (see Modules 6 and 7).
- Categories of recipients, including processors and any recipients outside Kenya.
- Retention periods, or the criteria used to determine them.
- A general description of the technical and organisational security measures in place.

A ROPA that is created for the sole purpose of registration, and never revisited, quickly becomes fiction: it describes an organisation that no longer exists, because programmes end, systems change, and new donor requirements introduce new data flows. Ownership of keeping the ROPA current should sit clearly with the DPO, with a defined review cycle (at minimum annually, and whenever a significant new processing activity is introduced).

Getting Started This Week

- Convert your data mapping register into ROPA format by adding lawful basis and retention columns.
- Assign a named owner, ideally the DPO, responsible for keeping the ROPA current.
- Set a recurring calendar reminder for at least an annual ROPA review.

Ref	Process / Activity Name	Department	Categories of Data Subjects	Categories of Personal Data	Storage Medium	Transferred Into or Out of the Organisation?	Where Is the Data Received From?	Transferred Outside Kenya?	Protection Measures If Transferred Outside Kenya	How Is the Data Transferred?
DR-01	Recruitment	Human Resources	Prospective employees	Name, National ID, academic certificates, referee details, employment history	Digital	Internal Only	Direct from applicant	No	Standard contractual clauses executed with the payroll vendor	Electronically, via vendor platform
DR-02	Employee Payroll Processing	Human Resources	Employees	Name, National ID and passport number, KRA PIN, bank account details, salary, next of kin, statutory deduction numbers	Digital	Out	Not applicable, generated internally	Yes	Not applicable	Not applicable, internal
DR-03	Digital Security Helpdesk and Incident Response for At-Risk Users	Digital Security Helpdesk	Human rights defenders, journalists, activists and other at-risk individuals requesting support	Name or pseudonym, contact details, device and account information, nature of the digital threat (account compromise, surveillance, doxxing), political opinion or affiliation where relevant to the threat, location data	Digital, encrypted case management system	Internal Only	Direct from the individual, via secure intake channel	No	Confidentiality undertakings with co-counsel; encrypted file transfer	Secure email or in-person exchange
DR-04	Legal Aid and Strategic Litigation Case Management	Legal & Policy	Clients and litigants facing arrest, prosecution or harassment over online speech, internet shutdowns, or unlawful surveillance	Name, national ID, contact details, case facts, court records, criminal record extracts, political opinion, correspondence with counsel	Digital and physical case files	Out	Direct from client and from courts or law enforcement	Unconfirmed, where co-counsel or regional courts are involved	Not applicable for identifiable data; aggregation and anonymisation protocol for shared datasets	Not applicable, internal
DR-05	Human Rights Violations Documentation and Incident Database	Research & Investigations	Victims and witnesses of online censorship, surveillance, harassment or internet-shutdown-related harm	Name or identifier, contact details, incident description, location, evidence (screenshots, correspondence), in some cases health or trauma-related information	Digital, restricted-access database	Internal Only, with anonymised aggregate data shared externally for reporting	Direct from victims, witnesses, and partner organisations	No, for identifiable records; anonymised datasets may be shared with international partners	Not applicable	Not applicable, internal
DR-06	Secure Whistleblower and Tip Line	Research & Investigations	Whistleblowers and confidential sources	Contact details where voluntarily provided, tip content, supporting evidence; may be submitted anonymously	Digital, encrypted secure-drop platform	Internal Only	Direct from the source, anonymous or named	No	Standard contractual clauses with campaign platform vendor	Electronically, via vendor API
DR-07	Advocacy Campaign and Petition Management	Communications & Campaigns	Campaign supporters and petition signatories	Name, email address, country or region, campaign preferences	Digital, campaign management platform	Out	Direct from supporters via online forms	Yes	Not applicable	Not applicable, internal
DR-08	Digital Security and Rights Training Management	Programmes	Training participants (journalists, activists, civil society staff)	Name, organisation, contact details, dietary or accessibility needs, attendance records, pre/post assessment scores	Digital	Internal Only	Direct from participant via registration form	No	Standard contractual clauses with CRM and payment processing vendors	Electronically, via vendor platform
DR-09	Donor and Grant Management	Grants & Fundraising	Individual donors and institutional funder contacts	Name, contact details, donation history, payment details, correspondence	Digital, CRM and finance systems	Out	Direct from donor, or from payment processor	Yes	Not applicable, see recommended action to document transfer safeguards	Secure file share
DR-10	Sub-Grantee and Partner Organisation Due Diligence	Grants & Fundraising	Sub-grantee and partner organisation staff	Names, roles, contact details, organisational registration details, financial and safeguarding due diligence records	Digital	Internal Only, with disclosure to funders on request	Direct from partner organisations during onboarding	Unconfirmed, where regional partners are onboarded	Standard contractual clauses with analytics and mailing list vendors	Electronically, via vendor scripts and API
DR-11	Website Analytics and Newsletter Subscription	Communications & Campaigns	Website visitors and newsletter subscribers	Email address, IP address, browsing behaviour, device and location data	Digital	Out	Direct from website visitor	Yes	Not applicable	Formal correspondence or agency portal
DR-12	Freedom of Information and Public Records Requests	Legal & Policy	Government officials and third parties named in records requested or received	Names, job titles, correspondence, and personal data incidentally contained in disclosed public records	Digital and physical	Internal Only, with onward disclosure in published research where appropriate	Government agencies, in response to formal requests	No	Data-sharing agreement with the partner monitoring network; aggregation before external sharing	Electronically, via API
DR-13	Monitoring of Internet Shutdowns and Online Censorship	Research & Investigations	Affected internet users, reported via crowdsourced and network measurement tools	IP address, network measurement data, incident reports, and where volunteered, contact details of reporters	Digital	Out, to international monitoring networks and partner coalitions	Automated network probes and direct submissions	Yes	Not applicable	Not applicable, internal
DR-14	Volunteer and Independent Consultant Management	Human Resources	Volunteers and independent consultants	Name, contact details, areas of expertise, contracts, bank details for consultant payments	Digital	Internal Only	Direct from the individual	No	Not applicable	Not applicable, internal
DR-15	Identity and Access Management for Organisational Systems	IT & Security	Employees, volunteers, and consultants with system access	Usernames, access logs, system permissions, device information	Digital	Internal Only	HR onboarding records	No	Not applicable	Not applicable, internal
DR-16	Board Governance and Minute-Taking	Governance	Board members	Names, contact details, declarations of interest, meeting minutes	Digital and physical	Internal Only	Direct from board members	No	Not applicable	Not applicable, internal

Processing Activity	Description of Why the Data Is Processed	Lawful Basis for Processing	Is the Data Sensitive Personal Data?	Express Consent for Sensitive Data?	Link to / Location of Consent Form	Security Procedures in Place	Retention Period	Date of Last Review	Date of Last Change to Legal Basis	Has a DPIA Been Completed?	Active or Inactive Process?
Collect, View, Record, Store, Disclose	To calculate and disburse monthly salaries, statutory deductions and benefits	Contractual Necessity	No	Not applicable	Not applicable	Role-based access limited to HR and Finance; encrypted vendor platform; annual access review	7 years after employment ends, per statutory record-keeping requirements	2026-09-01	Not applicable	No	Active
Collect, View, Record, Store, Analyse	To assess and respond to digital security threats and incidents affecting at-risk individuals	Vital Interest, with Consent sought where the individual's safety is not in immediate danger	Yes	Yes, obtained at intake save where safety concerns make this unsafe or impractical	Secure intake form, retained in the case file	End-to-end encrypted case system; need-to-know access limited to helpdesk staff; pseudonymisation of case records; no local storage of case files	24 months from case closure, or earlier deletion on request	2026-09-15	2026-04-01, basis clarified to include Vital Interest for emergency cases	Yes	Active
Collect, Record, Store, Disclose	To provide legal representation and pursue litigation in digital rights cases	Legitimate Interest, with Legal Obligation for court-mandated disclosures	Yes	Yes, via signed client engagement letter	Client engagement letter, filed in the physical case file	Locked physical files; access-controlled case management system; privilege markers on correspondence	Duration of case plus 7 years, per Law Society record-keeping requirements	2026-08-10	Not applicable	Yes	Active
Collect, Record, Store, Combine, Analyse	To document and evidence patterns of digital rights violations for advocacy and reporting	Legitimate Interest, with Consent obtained from identifiable sources	Yes	Yes, obtained before any identifiable detail is recorded	Consent and source-protection form, retained in the case record	Restricted, need-to-know access; pseudonymised source identifiers; encrypted database	5 years from documentation, subject to ongoing advocacy need	2026-09-10	Not applicable	Yes	Active
Collect, Record, Store	To receive and assess confidential tips on digital rights violations	Legitimate Interest	Yes	Not applicable for anonymous submissions; obtained for named sources who agree to follow-up contact	Not applicable	Encrypted secure-drop tool; access restricted to two named investigators; no logging of source IP addresses	3 years from receipt, or earlier deletion once a tip is closed	2026-07-20	Not applicable	Yes	Active
Collect, Record, Store, Disclose	To coordinate advocacy campaigns and communicate with supporters	Consent	No	Yes, via opt-in checkbox at sign-up	Campaign sign-up form, logged in the platform	Vendor's SOC 2-certified infrastructure; role-based platform access	Until consent is withdrawn, reviewed every 24 months	2026-06-30	Not applicable	No	Active
Collect, Record, Store, View	To organise and deliver training and measure learning outcomes	Contractual Necessity, or Consent where attendance is voluntary and unaffiliated	No, save where a participant discloses accessibility or health-related needs	Unconfirmed for health-related disclosures on registration forms, see recommended action	Registration form, logged in the training platform	Access-controlled training platform; participant lists shared with facilitators on a need-to-know basis	24 months from training date	2026-05-12	Not applicable	No	Active
Collect, Record, Store, Disclose	To manage donor relationships, process donations, and meet funder reporting requirements	Contractual Necessity, with Legitimate Interest for donor stewardship communications	No	Not applicable, save for marketing communications, see Consent for e-newsletter list	Donation form, logged in the CRM	Role-based CRM access; encrypted payment processing; PCI-DSS compliant processor	7 years after last donation, per grant audit requirements	2026-08-05	Not applicable	No	Active
Collect, Record, Store, Disclose	To conduct due diligence and manage sub-grant relationships, including safeguarding checks	Legal Obligation, with Legitimate Interest for safeguarding checks	No	Not applicable	Not applicable	Access-controlled grants management system	Duration of grant agreement plus 7 years	2026-07-01	Not applicable	No	Active
Collect, Record, Analyse, Disclose	To understand website usage and send the organisation's newsletter	Consent	No	Yes, via cookie banner and newsletter opt-in	Cookie consent log and newsletter sign-up form	IP anonymisation enabled on the analytics tool; vendor data processing agreements in place	14 months for analytics data; until unsubscribe for newsletter list	2026-06-01	Not applicable	No	Active
Collect, Record, Store, Disclose	To obtain and use public records in support of transparency and accountability research	Legitimate Interest	No	Not applicable	Not applicable	Restricted to the research and legal team; redaction protocol applied before publication	5 years from receipt	2026-04-18	Not applicable	No	Active
Collect, Record, Combine, Analyse, Disclose	To detect, verify and report internet shutdowns and censorship events	Legitimate Interest	No, save where a report identifies an individual reporter	Not applicable for automated network data; obtained for named reporters	Not applicable	Aggregation and anonymisation prior to external sharing; access-controlled monitoring dashboard	3 years from collection	2026-09-05	Not applicable	No	Active
Collect, Record, Store	To onboard, manage and pay volunteers and consultants	Contractual Necessity	No	Not applicable	Not applicable	Access-controlled HR records system	Duration of engagement plus 7 years	2026-05-30	Not applicable	No	Active
Collect, Record, Store, Modify	To manage system access and enforce least-privilege and need-to-know security, particularly for systems holding at-risk user data	Legitimate Interest	No	Not applicable	Not applicable	Multi-factor authentication; centralised identity management; quarterly access reviews	Duration of engagement plus 1 year	2026-09-15	Not applicable	No	Active
Collect, Record, Store	To support governance, decision-making and statutory compliance	Legal Obligation, with Legitimate Interest for governance administration	No	Not applicable	Not applicable	Restricted access, board portal with two-factor authentication	7 years from the meeting date	2026-03-20	Not applicable	No	Active
Collect, Record, Store	To support governance, decision-making and statutory compliance	Legal Obligation, with Legitimate Interest for governance administration	No	Not applicable	Not applicable	Restricted access, board portal with two-factor authentication	7 years from the meeting date	2026-03-20	Not applicable	No	Active

4. COMPONENT 04 · GOVERNANCE

The Data Protection Officer

"Independence is not a title on an organogram. It is whether thze DPO can say no to a Programme Director and still have a job the next morning."

Legal Foundation
Section 28 of the Data Protection Act, 2019 requires organisations to designate a Data Protection Officer where they process personal data and their core activities require regular and systematic monitoring of data subjects on a large scale or involve large-scale processing of sensitive personal data. The DPO must have expert knowledge of data protection law and practice and must avoid conflicts of interest: they should not simultaneously hold a position that determines the purposes and means of processing personal data.

The DPO is best understood as an institutional function rather than an individual job title. In a large organisation, this may be a dedicated, full-time role. In a small nonprofit, it is more often an existing staff member, such as a compliance, MEAL, or legal officer, taking on the function alongside other duties, provided the independence requirement is respected.

Core Responsibilities

- Advising the organisation on compliance with the Data Protection Act and its Regulations.
- Training staff on data protection obligations.
- Supporting and overseeing Data Protection Impact Assessments.
- Acting as the primary point of contact with the Office of the Data Protection Commissioner.
- Owning and keeping current the ROPA, the incident log, and the audit-ready evidence file.

Independence matters in practice, not only on paper. A DPO who reports to, and can be overruled or dismissed by, the same person who decides what data the organisation collects and why (frequently the Executive Director or a programme director with strong incentives to move quickly) cannot meaningfully perform the function. The DPO should have a direct line to senior leadership or the board, sufficient time and resources to do the job, and protection from being penalised for raising uncomfortable findings.

Reflective Practice
Consider your own organisation's arrangements for the DPO function.

- Who currently performs this function, even informally, and do they have expert knowledge of data protection law and practice?
- Does this person have a genuine conflict of interest, for instance because they also decide what data is collected and why?
- Do they have a direct reporting line to senior leadership, and enough protected time to do the work properly?

- If they raised a serious finding that was inconvenient for a major donor relationship, would they be supported or overruled?

Getting Started This Week

- Identify who in your organisation could plausibly perform the DPO function today, even informally.
- Check that person's role for conflicts of interest, particularly whether they also decide what data is collected and why.
- Draft a one-page terms of reference for the role, including a direct reporting line to senior leadership.

5. COMPONENT 05 · RISK & SAFEGUARDS

Data Protection Impact Assessments (DPIA)

"A DPIA asks one uncomfortable question early, before launch, so the organisation never has to ask a worse one later, after harm."

Legal Foundation

Section 31 of the Data Protection Act and Regulation 41–45 of the Data Protection (General) Regulations, 2021 govern DPIAs. A DPIA must be conducted, at minimum, before commencing:

- Large-scale processing of sensitive personal data.
- Systematic monitoring of a publicly accessible area on a large scale.
- Processing involving new technologies, or the use of technology in a novel way, where the risk to data subjects is not yet well understood.
- Any other processing activity that, on assessment, is likely to result in high risk to the rights and freedoms of data subjects.

Stages of a DPIA

- Describe the processing. What data, from whom, for what purpose, using what systems, shared with whom, and for how long.
- Assess necessity and proportionality. Is this processing necessary to achieve the stated purpose, and is there a less intrusive way to achieve the same outcome?
- Identify risks to data subjects. Consider risks such as unauthorised access, loss, discrimination, exposure to physical harm (particularly relevant for beneficiaries such as survivors of violence or displaced persons), and loss of trust.

- Identify mitigating measures. For each risk identified, document a specific, proportionate measure that reduces it, and assign someone to implement it.
- Sign-off and record-keeping. The DPIA should be reviewed and signed off by the DPO, and where residual risk remains high after mitigation, the Data Commissioner should be consulted before processing begins.
- Review. A DPIA is not a one-time certificate. It should be revisited if the processing activity changes materially.

Case Study: Pwani Community Network CBO

Pwani Community Network CBO is piloting a fingerprint-based attendance system to reduce duplicate registrations in its nutrition programme. Before rolling the system out, the programme team should ask: does this involve large-scale processing of sensitive personal data (biometric data is sensitive personal data)? What happens if the device is lost or the local server is compromised? Is there a less intrusive alternative, such as a unique ID card, that would achieve the same anti-duplication goal with less risk? These are exactly the questions a DPIA is designed to ask before the system goes live, not after a data subject's fingerprint template has already been exposed.

Getting Started This Week

- List any processing activity currently planned or underway that could count as high risk under Section 31 and Regulation 41.
- Run the screening questions in this section against each one before the activity proceeds any further.
- Refer to the DPIA template in the 3rd Schedule of the Regulation and the guidance notes by ODPC
- Have the DPO sign off on the first DPIA before that activity goes live.

6. COMPONENT 06 · RISK & SAFEGUARDS

Technical and Organisational Measures

Legal Foundation

Section 41 of the Data Protection Act, 2019 places the primary security obligation on data controllers and processors to implement appropriate technical and organisational measures to secure personal data against loss, unauthorised access, destruction, and disclosure.

For nonprofits operating with constrained budgets, "appropriate" does not mean the most expensive enterprise security suite available. It means measures proportionate to the risk of the data held. A community organisation holding a spreadsheet of training attendees needs meaningfully different safeguards than one holding case files for survivors of gender-based violence, even though both are legally obliged to have some safeguards in place.

A Baseline for Resource-Constrained Organisations

- **Access controls.** Role-based access so that staff can see only the data relevant to their function; unique logins rather than shared accounts; prompt removal of access when staff or volunteers leave.
- **Device and account security.** Screen locks, up-to-date software, and multi-factor authentication on email and cloud accounts, most of which is available at no extra cost on platforms nonprofits already use.
- **Secure communication for sensitive data.** Avoiding plain SMS or unencrypted messaging apps for sensitive personal data where an encrypted alternative or the organisation's managed system is available.
- **Physical security.** Locked cabinets for paper files, controlled access to field offices, and secure transport of any physical records.
- **Backups and secure disposal.** Regular backups to guard against loss, and secure, irreversible deletion or shredding when retention periods expire.
- **Vendor security due diligence.** Basic checks on any third-party system before adopting it, does it offer encryption, access logs, and a clear data deletion process.
- **Staff training.** Technical measures fail quickly if staff are not trained to use them; organisational measures such as induction training and periodic refreshers are as important as any technical control.

Practical Tool: Baseline TOM Self-Assessment
For each item above, rate the organisation as In Place, Partially in Place, or Not in Place, and assign an owner and a target date for closing each gap. Revisit the assessment at least annually, and whenever a new system or data type is introduced.

Getting Started This Week

- Complete the Baseline TOM Self-Assessment against the measures listed above.
- Turn on multi-factor authentication on your organisation's email and cloud accounts, if it is not already active.
- Identify the single highest-risk gap, often shared logins or an unencrypted device, and fix that one first.

7. COMPONENT 07 · RISK & SAFEGUARDS

Policies and Notices

A privacy programme that exists only in practice, and not on paper, cannot demonstrate its own consistency, cannot survive staff turnover, and cannot meet the transparency obligations the Act places on organisations that process personal data. This section identifies the core instruments most nonprofits need, without prescribing a rigid template that will not fit every organisation's size and context.

Core Instruments

- **Privacy Notice.** The external-facing document, or layered notice as introduced in Module 7 for low-literacy and resource-constrained settings, that tells data subjects what is collected, why, and how, satisfying the duty to notify under Section 29 of the Act.
- **Data Protection Policy**. The internal governance document setting out the organisation's overall approach, roles, and responsibilities for data protection.
- **Data Retention and Disposal Policy.** Setting out how long each category of data is kept and how it is securely disposed of when no longer needed.
- **Data Breach Response Policy.** Documenting the incident response process described in the Incident Management and Breach Reporting component, so that it does not have to be improvised during an actual incident.
- **Acceptable Use / IT Security Policy.** Setting expectations for staff use of devices, accounts, and systems that touch personal data.
- **Data Sharing Agreement template.** A reusable template reflecting the due diligence requirements in the Data Sharing Arrangements component, so that each new partnership does not require drafting from scratch.
- **Data Subject Request procedure.** An internal procedure describing how the organisation receives, verifies, and responds to the DPG1–DPG5 requests introduced in Module 8, within the statutory timelines.

Practical Tool: Policy Inventory Checklist
Against each instrument above, record: does it exist; when was it last reviewed; is it available in the languages and formats data subjects can understand; and has it been communicated to staff, and understood, rather than only filed for record-keeping purposes.

Getting Started This Week

- Complete the Policy Inventory Checklist against the instruments listed above.
- Draft or update your Privacy Notice first, since it is the instrument data subjects see.
- Simplify at least one notice into a layered, low-literacy-friendly version, as introduced in Module 7.

8. COMPONENT 08 · DATA IN MOTION

Data Sharing Arrangements

Nonprofits rarely hold personal data in isolation. Donors request beneficiary-level data for reporting, implementing partners share case files for joint programming, cloud and software vendors process data on the organisation's behalf, and government agencies sometimes request data for coordination purposes. Each of these relationships is a data sharing arrangement, and each carries its own risk if it is entered into informally, on the strength of an email request, rather than through a documented, purpose-limited agreement.

Sharing With Processors vs. Sharing with Other Controllers

It matters, legally and practically, whether the organisation receiving the data is acting as a processor (handling data strictly on the sharing organisation's instructions, such as a cloud storage provider) or as an independent controller in its own right (such as a donor that will use beneficiary data for its own separate reporting and research purposes). Under Section 41(2) of the Data Protection Act, 2019, a written data processing agreement is required wherever a processor is engaged. Where the recipient is an independent controller, a data sharing agreement is the appropriate instrument instead, and it must be grounded in a valid lawful basis for the disclosure, not that the recipient has requested the data.

Practical Tool: Data Sharing Due Diligence

Before agreeing to share personal data with any partner, donor, or vendor, the organisation should be able to answer:

- What is the specific, documented purpose of this disclosure, and does it fall within the purpose for which the data was originally collected?
- What is the lawful basis for this specific disclosure?
- Is a written data sharing agreement, or data processing agreement, in place, covering permitted uses, security obligations, sub-sharing restrictions, breach notification duties, and what happens to the data at the end of the relationship?
- Has the minimum necessary dataset been shared, rather than the full dataset because it was easier to export?
- If the recipient is outside Kenya, has the cross-border transfer assessment required under Module 10 and the Cross-Border Data Transfers component of this module been completed?

A recurring failure pattern among nonprofits is sharing a full, unredacted beneficiary dataset with a donor because a partial extract would take longer to prepare, or because nobody was confident enough to push back on the request. A documented data sharing agreement, established through prior negotiation and approved for reuse, streamlines recurring reporting cycles by eliminating the need to revisit and renegotiate the same considerations each time.

Getting Started This Week

- List every partner, donor, and vendor your organisation currently shares personal data with.
- Check each relationship against the due diligence questions set out above.
- Draft one reusable data sharing agreement template rather than renegotiating terms for every new request.

9. COMPONENT 09 · DATA IN MOTION

Cross-Border Data Transfers

Module 10 addressed the full legal framework for cross-border data transfers in detail: adequacy decisions, standard contractual clauses, binding corporate rules, consent-based transfers, and transfer impact assessments. This section does not repeat that analysis. Instead, it addresses the narrower, operational question this module is concerned with throughout: how does cross-border transfer assessment become a routine, embedded part of the privacy programme, rather than a one-off legal exercise performed only when a donor first asks for offshore data hosting?

- **Embed it in data mapping.** Every entry in the data mapping register and ROPA should flag whether the data involved leaves Kenya, whether physically or through remote access by staff, partners, or vendors located abroad.
- **Maintain a standing transfer register.** Rather than assessing each transfer from scratch, maintain a register of recurring cross-border recipients (cloud providers, international donors, regional systems), the safeguard relied on for each, and the date it was last reviewed.
- **Fold it into data sharing due diligence.** The due diligence questions in the Data Sharing Arrangements component should automatically trigger a transfer impact assessment whenever the recipient identified is outside Kenya.

Treating cross-border transfer as a standing feature of the programme, rather than an exception handled reactively, is what allows an organisation to answer a donor's hosting question in minutes rather than in weeks.

Getting Started This Week

- Flag, in your data mapping register, every activity where data leaves Kenya, physically or by remote access.
- Start a standing transfer register listing each recipient, the safeguard relied on, and the date it was last reviewed.
- Revisit Module 10 for any recipient whose safeguard has not yet been confirmed.

10. COMPONENT 10 · RESPONSE & ASSURANCE

Incident Management and Breach Reporting

Legal Foundation
Section 43 of the Data Protection Act, 2019 requires a data controller to notify the Data Commissioner of a personal data breach within 72 hours of becoming aware of it. Where the breach is likely to result in high risk to the rights and freedoms of affected data subjects, they must also be notified without undue delay, under Section 43(1)(b) and Regulation 38(2) of the General Regulations, 2021. A data processor must notify the controller within 48 hours of becoming aware of a breach, under Regulation 38. Regulation 37 sets out the categories of notifiable breach, and Regulation 38 sets out the required content of a breach notification.

A Working Incident Response Process

- **Identify and contain.** The moment a suspected breach is discovered, whether a lost laptop, a misdirected email, or unauthorised access, the immediate priority is to stop further exposure: revoke access, recover the device, or take the affected system offline.
- **Assess.** Determine what data was involved, how many data subjects are affected, and whether the breach is likely to cause them harm, this assessment drives every notification decision that follows.
- **Notify internally.** Escalate to the DPO immediately. The 72-hour clock for notifying the ODPC starts running from the moment the organisation becomes aware, not from the moment a full investigation concludes.
- **Notify externally where required.** Notify the ODPC within 72 hours and affected data subjects without undue delay where the breach poses high risk to them. Where a processor caused or discovered the breach, they must notify the controller within 48 hours.
- **Document.** Record what happened, when it was discovered, who was notified and when, and what containment and remediation steps were taken. This record is itself required content under Regulation 38 and is also the organisation's evidence of accountability if questioned later.
- **Remediate and review.** Fix the underlying cause, not only the immediate symptoms, and update the risk assessment, training, or technical measures that allowed the incident to occur.

Practical Tool: Incident Log
Maintain a simple, continuously updated incident log with columns for: date and time discovered; description of the incident; data categories and number of data subjects affected; severity assessment; whether the ODPC was notified and when; whether affected data subjects were notified and when; containment and remediation actions; and date closed.

Administrative penalties for non-compliance under the Act can reach up to KES 5 million, or one per cent of the organisation's annual turnover for the preceding financial year, whichever is lower, in addition to the reputational cost to an organisation whose work depends on the trust of the communities it serves. A well-rehearsed incident response process is therefore not only a legal safeguard, but also a practical way of containing harm to real people before it compounds.

Getting Started This Week

- Set up a simple, shared incident log using the template above, even if it starts out empty.
- Brief all staff on one thing only: who to tell, immediately, if they suspect a data incident.
- Confirm your DPO knows that the 72-hour ODPC notification clock starts the moment the organisation becomes aware, not once an investigation concludes.

11. COMPONENT 11 · RESPONSE & ASSURANCE

Audit Readiness

This section addresses the organisation's side of that relationship: what does it mean, in practice, to be ready for a regulatory audit or inspection at any time, rather than only in the weeks before a known review? Audit readiness is not a standalone activity but the result of the effective implementation and integration of the other twelve components functioning together. An organisation that maintains a current ROPA, keeps DPIAs on file, has a documented incident log, holds signed data sharing agreements, and can show evidence of staff training does not need to prepare for an audit. It only needs to assemble what it already has.

Practical Tool: Audit-Ready Evidence File

Maintain a single, organised evidence file, physical or digital, containing:

- Current ROPA and data mapping register
- ODPC registration certificate and renewal history
- Completed DPIAs for high-risk processing activities
- Signed data sharing and data processing agreements
- Data protection policies and notices, with version history
- Incident log and evidence of breach notifications made
- Staff training records
- Records of data subject requests received and how they were resolved
- The completed Organisational Self-Assessment Checklist introduced in Module 5

Assign a single owner for keeping this evidence file current, and rehearse producing it, even informally, at least once a year, so the first time it is assembled under real time pressure is not during an actual ODPC inspection.

Getting Started This Week

- Start assembling the Audit-Ready Evidence File folder by folder, even where some items are still incomplete.
- Assign a single owner responsible for keeping the evidence file current.
- Rehearse producing it once, informally, before a real inspection ever forces the question.

12. COMPONENT 12 · RESPONSE & ASSURANCE

Monitoring the Privacy Programme

The opening section of this module, What Is a Programme? identified monitoring and evaluation as one of the defining elements of a genuine programme. A privacy programme that is never measured cannot demonstrate, to its own leadership or to the ODPC, whether it is working, and cannot identify where it is quietly failing until an incident forces the question.

Indicator	What It Tracks
Data mapping coverage	Percentage of known processing activities that have been mapped and entered into the ROPA.
ROPA currency	Date the ROPA was last fully reviewed, against the target annual review cycle.
DPIA completion	Number of high-risk processing activities identified vs. number with a completed DPIA on file.
Registration status	Current registration status with the ODPC and the date of next renewal.
Data sharing coverage	Number of active external data-sharing relationships vs. number covered by a signed agreement.
Incident metrics	Number of incidents logged, number notified to the ODPC within 72 hours, and number of open vs. closed cases.
Training completion	Percentage of staff and relevant volunteers who have completed data protection training in the past twelve months.
Data subject request compliance	Number of requests received and percentage responded to within the statutory timelines.

The dashboard does not need to be sophisticated software; a single shared spreadsheet, reviewed quarterly by the DPO and reported at least annually to senior management or the board, as identified under the Governance and oversight element earlier in this module, is sufficient for most nonprofits. What matters is that the review happens on a fixed schedule, and that its findings, feed back into closing the gaps in the other twelve components, so that the privacy programme, like any other well-run programme, improves each year rather than persisting.

Getting Started This Week

- Build a simple one-tab spreadsheet using the eight indicators listed above.
- Set a fixed quarterly review date and put it on the DPO's calendar now.
- Agree who above the DPO receives the annual summary, whether that is senior management or the board.

13. COMPONENT 13 · REGULATORY STANDING

ODPC Registration and Self-Audit

Note on Sequencing

This module places registration last, after mapping, classification, the ROPA, the DPO, DPIAs, safeguards, policies, sharing arrangements, and incident preparedness are already in place. That is a deliberate teaching choice, not a statement of legal timing. Section 18 of the Act requires registration before an organisation acts as a controller or processor at all, so a genuinely new organisation, or one starting a genuinely new processing activity, must still register before processing begins. For an existing nonprofit retrofitting a privacy programme, however, an accurate registration under Section 19 depends on already knowing what data it holds, on what basis, and with what safeguards, which is precisely what the preceding thirteen components establish. Registration completed before that work is accurate on paper only.

Legal Foundation

Section 18 of the Data Protection Act, 2019 provides that no person shall act as a data controller or data processor without being registered with the Data Commissioner. The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 set the thresholds that determine whether registration is mandatory, having regard to factors including the nature of the sector, the volume of personal data processed, whether sensitive personal data is involved, and whether personal data is transferred outside Kenya.

Registration is not a formality to be completed once and forgotten. Under Section 19, organisations must accurately disclose the categories of personal data collected, the purposes of processing, the categories of data subjects, the security safeguards in place, and the risks involved. Providing false or misleading information is a criminal offence. Registration is subject to renewal every two years, and any material change to registration details must be notified to the Data Commissioner. Because the register of data controllers and processors is publicly accessible, registration status is also a matter of public accountability.

The Self-Audit Process

Before registering, and periodically thereafter, an organisation should conduct an internal self-audit to verify that what it will tell, or has told, the Data Commissioner is true in practice. A self-audit compares the organisation's registration disclosures and its ROPA against what data mapping has found and flags any gap between the two for correction before, not after, the ODPC finds it first.

Practical Tool: Registration Readiness Checklist

- Have we determined, against the current thresholds, whether registration is mandatory for our organisation?
- Does our registration application accurately reflect our current data mapping and ROPA, not an outdated description of our activities?
- Do we have a designated person responsible for tracking our renewal date, two years from registration?
- Do we have a process for notifying the ODPC of material changes, such as a new processing activity or a new category of sensitive personal data?
- Have we budgeted staff time for the self-audit as a recurring exercise, not a one-time event before initial registration?

Getting Started This Week

- Confirm whether your organisation currently meets the mandatory registration thresholds under the 2021 Regulations.
- Run the Registration Readiness Checklist above before submitting or renewing your registration.
- Calendar the two-year renewal date the moment registration is confirmed.

11.17 Key Takeaways

1. A programme is built, not written – A privacy programme is not a single policy document. It takes shape through the ongoing work of assessing, selecting, documenting, and embedding practice across the organisation.
2. You cannot manage what you have not mapped – Data mapping and the Record of Processing Activities (ROPA) provide the factual foundation every other programme decision rests on. Without them, risk assessments and registrations are guesswork.
3. Registration and cross-border transfers require deliberate judgement – ODPC registration and any transfer of personal data outside Kenya must be evaluated within the specific context of your organisation's own operations, not treated as generic legal knowledge.

4. A programme only works if it stays alive – Policies, technical measures, and audit readiness only protect the organisation if they are maintained and revisited. The programme should therefore be embedded as a practice rather than a one-time compliance exercise.

11.18 Assessment

Part A: Knowledge and Conceptual Understanding

1. What are the defining elements of a genuine organisational programme, and how does each apply to a privacy programme specifically?
2. Explain the relationship between data mapping and the Record of Processing Activities. Why must the ROPA be treated as a living document rather than a one-time deliverable?
3. Under Section 31 and Regulations 41–45 of the Data Protection (General) Regulations, 2021, when is a DPIA required, and what are its key stages?
4. What are the notification timelines under Section 43 of the Data Protection Act, 2019 for (a) a controller notifying the ODPC, (b) a controller notifying affected data subjects, and (c) a processor notifying a controller?
5. Explain the independence requirement for a Data Protection Officer under Section 28 of the Act and describe a scenario in which that independence could be compromised in a small nonprofit organisation.
6. Why is cross-border data transfer addressed as a routine part of data mapping and data sharing in this module, rather than only in Module 10?

Part B: Applied Analysis

1. Pwani Community Network CBO has never conducted a data mapping exercise. Its Executive Director asks you where to begin. Outline, in order, the first five practical steps you would take, and explain why you sequenced them that way.
2. Pwani's programme team wants to launch the fingerprint attendance system described earlier in the Data Protection Impact Assessment component within two weeks, ahead of a donor visit. Using the DPIA stages set out in this module, explain what you would tell them about that timeline, and what minimum steps could not be skipped.

Part C: Organisational Reflection

1. Using the Registration Readiness Checklist and the Audit-Ready Evidence File in this module, assess how prepared your organisation currently is for an ODPC registration renewal or inspection. Identify your three largest gaps.
2. Who in your organisation currently performs, or could perform, the Data Protection Officer function, and what would need to change for that person to do the job with independence?
3. Looking across all thirteen components in this module, which single component, if implemented well this year, would reduce the most risk for your organisation? Explain your reasoning.

12.

The Office of the Data Protection Commissioner

About This Module

This module expounds on the Office of the Data Protection Commissioner (ODPC), its mandate, powers, and key functions. It equips organisations to engage effectively with the ODPC, whether as regulated entities, complainants, or participants in Kenya's broader data governance ecosystem.

12.1 Introduction

The Data Protection Act, 2019 established the Office of the Data Protection Commissioner (ODPC) as the principal regulatory authority responsible for overseeing data protection in Kenya. Since its establishment in November 2020, the ODPC has played a central role in protecting personal data, promoting privacy rights, and enforcing compliance with data protection obligations.

12.2 Objectives

1. To outline the legal establishment of the ODPC and its role within Kenya's data governance ecosystem.
2. To examine the scope of the ODPC'S functions, powers, and responsibilities.
3. To explain the procedure for lodging and handling complaints before the ODPC.
4. To interrogate the ODPC's enforcement mechanisms, including enforcement notices, penalty notices, and determinations.
5. To explain the right of appeal against the ODPC decisions and the procedure for exercising the right.

12.3 Learning Outcomes

Upon completion of this module, learners should be able to demonstrate the following competencies:

Outcome	Demonstrated Competence
Describe the establishment, mandate, and governance structure of the ODPC	Explain how the ODPC was established under the Data Protection Act, 2019, its constitutional and statutory basis, and describe its governance structure, including the role of the Data Commissioner.
Explain the ODPC's functions and powers	Distinguish between the ODPC's regulatory, enforcement, and advisory roles, and give examples of specific functions falling under each category
Identify registration obligations under the DPA	Determine whether their organization is required to register as a data controller and/or data processor, and explain the steps, requirements, and timelines involved in registering with the ODPC
Explain the complaints process before the ODPC	Describe the end-to-end process for lodging a complaint with the ODPC, from initial submission through investigation to resolution, including the organisation's obligations at each stage.
Distinguish enforcement mechanisms available to the ODPC	Differentiate between enforcement notices, penalty notices, and criminal prosecution, explaining what triggers each, and the specific obligations or consequences each imposes on an organisation
Explain the right to appeal an ODPC determination	Describe the grounds and procedure for appealing an ODPC determination and the relevant timelines.
Training completion	Percentage of staff and relevant volunteers who have completed data protection training in the past twelve months.
Data subject request compliance	Number of requests received and percentage responded to within the statutory timelines.

12.4 The Establishment of the ODPC

The Office of the Data Protection Commissioner (ODPC) is established under Section 5 of the Data Protection Act, 2019 as Kenya's principal data protection regulator.
Operational since November 2020, the ODPC is an independent office. ODPC is headed by the Data Protection Commissioner who is appointed by the president.

12.5 Functions of the ODPC

The Office of the Data Protection Commissioner (ODPC) is responsible for overseeing the implementation and enforcement of the Data Protection Act, 2019. Its functions extend beyond regulation and enforcement to include public education, capacity building, research, and international cooperation.

The ODPC's key functions include:

1. Oversee the implementation of and be responsible for the enforcement of the Act
2. Establish and maintain a register of data controllers and data processors
3. Exercise oversight on data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with the Act
4. Promote self-regulation among data controllers and data processors
5. 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 the Act
6. Receive and investigate any complaint by any person on infringements of the rights under the Act
7. Take such measures as may be necessary to bring the provisions of the Act to the knowledge of the public.
8. Carry out inspections of public and private entities with a view to evaluating the processing of personal data.
9. Promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements
10. 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
11. Perform such other functions as may be prescribed by any other law or as necessary for the promotion of object of the Act.

For ease of understanding, these functions can be grouped into five broad areas:

1. Oversight and regulation
2. Registration
3. Complaints handling and enforcement
4. Public awareness and guidance
5. International cooperation

12.5.1 Oversight and Regulation of Data Processing

The ODPC's primary mandate is to oversee data processing activities undertaken by both public and private sector organisations, including nonprofits. In carrying out this role, the ODPC monitors compliance with the DPA, oversees how personal data is collected, stored, used, shared, and deleted, and assesses whether organisations are processing personal data lawfully.

This function includes:

- Monitoring compliance with the DPA by data controllers and data processors.
- Exercising oversight over data processing activities across all sectors.
- Conducting inspections, assessments, and compliance audits.
- Verifying whether personal data is being processed in accordance with the law.
- Promoting self-regulation among data controllers and processors.

Oversight is not limited to responding to complaints. The ODPC may proactively assess data processing practices to determine whether organisations are meeting their obligations under the law. This includes reviewing organisational policies, procedures, security measures, and record-keeping practices.

Reflection: What This Means for nonprofits

As a data controller or processor, your organisation is subject to ODPC oversight. The ODPC may review your data processing practices, request information, or conduct compliance audits. Nonprofits are therefore expected to maintain appropriate data protection policies, procedures, and records demonstrating compliance with the DPA. For example, a nonprofit implementing a humanitarian programme may be required to show how beneficiary information is collected, who has access to it, how it is stored, and when it is deleted. Maintaining Records of Processing Activities and clear policies can help organisations demonstrate compliance if questions arise.

12.5.2 Registration of Data Controllers and Data Processors

One of the ODPC's core regulatory functions is maintaining a register of data controllers and data processors operating in Kenya. Registration promotes transparency and enables the ODPC to identify organisations engaged in personal data processing activities.

Under Section 18 of the Data Protection Act and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, organisations that meet the prescribed registration thresholds (highlighted in module 9) are required to register with the ODPC. Registration enables the ODPC to identify entities processing personal data and to exercise effective regulatory oversight.

Registration is undertaken through the ODPC online portal. Applicants are required to provide information relating to their organisation, the categories of personal data processed, the purposes of processing, and the nature of their data processing activities. Upon approval, the organisation is issued with a registration certificate.

Reflection: What This Means for nonprofits

Many nonprofits process significant volumes of personal data relating to beneficiaries, staff, donors, volunteers, and community members. Organisations should assess whether they fall within the registration requirements and ensure that registration and renewal obligations are met where applicable. Failure to register when required may expose an organisation to regulatory action and undermine its overall compliance efforts.

12.5.3 Complaints Handling and Enforcement

The ODPC serves as the primary institution for receiving, investigating and determining complaints relating to violations of data protection rights. Any person whose personal data has been processed unlawfully or their rights under the DPA have been infringed may lodge a complaint with the Commissioner.

Upon receiving a complaint, the ODPC may conduct investigations, request information from the relevant parties, inspect records, and assess whether the organisation's conduct complies with the law. At the conclusion of an investigation, the Commissioner may issue a determination, make recommendations, or direct an organisation to take specific corrective measures.

12.5.3 Public Awareness, Guidance, and Capacity Building

A significant aspect of ODPC's mandate involves promoting awareness and understanding of data protection rights and responsibilities among individuals, organisations, and public institutions.

To fulfil this mandate, the ODPC develops educational materials, conducts outreach and awareness programmes, publishes guidance documents, and engages with stakeholders across different sectors. The office also supports efforts to build data protection capacity within organisations and to promote a culture of responsible data use.

The ODPC may issue guidance notes, advisories, compliance frameworks, and codes of practice to assist organisations in understanding how the requirements of the DPA apply in specific contexts. These instruments provide practical guidance on how organisations can implement good data protection practices.

12.5.4 International Cooperation and Cross-Border Data Transfers

As personal data increasingly moves across national borders, the ODPC plays an important role in ensuring that international data transfers are undertaken in a manner that protects the rights of data subjects. The office works with data protection authorities in other jurisdictions, participates in regional and international initiatives, and contributes to the development of data protection standards and best practices.
The ODPC is also responsible for overseeing compliance with the DPA's requirements relating to cross-border transfers of personal data. This includes assessing whether adequate safeguards exist to protect personal data transferred outside Kenya and providing guidance on lawful transfer mechanisms.

12.6 Complaints to the ODPC

Under section 56 of the DPA, a data subject who is aggrieved by a decision, action, omission, or practice relating to the processing of their personal data may lodge a complaint with the Commissioner. The Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 establish the procedures governing how complaints are lodged, investigated, and determined.
Importantly, complaints are not limited to obvious data breaches. A complaint may arise where an organisation collects excessive personal information, refuses to honour a data subject's rights, unlawfully discloses information, retains data for longer than necessary, transfers data unlawfully, or otherwise fails to comply with its obligations under the DPA.

12.6.1 Who May Lodge a Complaint?

The right to lodge a complaint is provided under Section 56(1) of the DPA and Regulation 4 of the Complaints Handling Procedure and Enforcement Regulations, 2021.

Complaints may be lodged by:

- A data subject acting on their own behalf.
- A person acting on behalf of a data subject such as a parent on behalf of a minor
- A person authorised by law to act on behalf of another person.
- An anonymous complainant where circumstances justify anonymity.

This broad approach is particularly important for vulnerable individuals (children, survivors of violence, refugees, persons with disabilities among others) confidence, or capacity to pursue complaints independently.

12.6.2 How is a Complaint Lodged?

The procedure for lodging complaints is set out under Regulation 4(2) and the prescribed Form DPC 1 is found within the Schedule to the Regulations.

A complaint may be submitted:

a) Orally;
b) Electronically through email, the ODPC's online complaint management system.
c) Through any other means approved by the Commissioner.

The complaint should contain:

a) The identity and contact details of the complainant or representative;
b) The identity of the respondent;
c) A description of the alleged violation;
d) The date on which the complainant became aware of the alleged breach or violation;
e) Supporting evidence;
f) The remedies sought; and
g) Details of any other proceedings concerning the matter.

Regulation 5 provides that complaints are lodged free of charge.

Once a complaint is received, the Commissioner must acknowledge receipt within seven days, maintain a register of complaints, and assign a reference number for purposes of tracking and follow-up.

12.6.3 Preliminary Assessment of Complaints

Upon receipt, the Commissioner undertakes a preliminary assessment of the complaint.
This power derives from Section 57 of the Data Protection Act and Regulations 7–10 of the Complaints Regulations.

At this stage, the Commissioner considers:

- Whether the complaint falls within the mandate of the ODPC;
- Whether it raises issues under the Data Protection Act;
- Whether sufficient information has been provided; and
- Whether another institution is better placed to address the dispute.

Following review, the Commissioner may admit the complaint, reject the complaint with reasons, request for additional information or refer the matter to another competent authority.

12.6.4 Notification of the Respondent

Where a complaint is admitted, Regulation 11 requires the Commissioner to notify the respondent using Form DPC 3.

The respondent is required to respond within twenty-one (21) days by:

- making written representations;
- providing relevant documents or evidence;
- proposing resolution measures; or
- responding to the allegations raised.

Failure to respond does not stop the proceedings. The Commissioner may proceed and determine the complaint based on the information available.

12.6.5 Investigation Powers of the Commissioner

Where necessary, the Commissioner may conduct a formal investigation under Section 57 of the Act and Regulation 13.

The investigative powers of the Commissioner include:

- summoning witnesses;
- examining persons under oath;
- requiring production of documents;
- compelling the provision of information;
- inspecting records; and
- obtaining court warrants to enter premises, conduct searches, and seize relevant materials.

These powers are significant and reflect the quasi-judicial nature of the Commissioner's complaint-handling mandate.

In exercising these powers, the Commissioner must comply with the principles of procedural fairness under Article 47 of the Constitution and the Fair Administrative Action Act.

12.6.6 Determination of Complaints

Following investigation, the Commissioner must issue a written determination.
Under Regulation 14, the determination should contain:

- the issues for determination;
- relevant facts;
- evidence considered;
- findings;
- reasons for the decision; and
- remedies granted.

The determination must be communicated to the parties within seven days.

Regulation 14(5) provides that determinations of the Commissioner are binding and enforceable.

12.6.7 Alternative Dispute Resolution

The ODPC may facilitate:

- mediation;
- conciliation;
- negotiation; or
- other forms of alternative dispute resolution.

This authority is recognised under **Regulation 12.**
Where parties reach agreement, the settlement is reduced into writing using **Form DPC 5** and is treated as a determination of the Commissioner.

Stage of Complaint Process	Key Requirements and Timeframes
Lodging of complaint	Free of charge; oral, electronic, or written; Form DPC 1; may be submitted anonymously or through a representative
Acknowledgement	ODPC must acknowledge receipt within seven days
Preliminary review	Commissioner assesses whether complaint falls within mandate and raises issues under the Act
Notification to respondent	Commissioner notifies respondent using Form DPC 3; respondent has twenty-one days to respond or make representations
Investigation	Commissioner may issue summons, examine persons, require documents, and enter premises with a warrant
Determination	Written determination communicated to parties; binding and enforceable as a court order
Alternative dispute resolution	Available at any stage prior to formal determination; agreement signed in Form DPC 5 and enforceable as a determination
Data subject request compliance	Number of requests received and percentage responded to within the statutory timelines.

12.7 Enforcement, Penalties and Prosecution

The enforcement powers of the ODPC are contained in:

- Sections 58–65 of the Data Protection Act, 2019;
- the Complaints Handling Procedure and Enforcement Regulations, 2021; and
- the general offences provisions under Sections 72–73.

The framework adopts a graduated approach to enforcement, beginning with corrective measures and escalating to financial penalties, compensation orders, and criminal sanctions where appropriate.

12.7.1 Enforcement Notices

Under Section 58(1), the Commissioner may issue an enforcement notice where satisfied that a data controller or processor has contravened the Act or is likely to do so.

The notice must specify:

- the breach identified;
- corrective measures required;
- timelines for compliance; and
- consequences of non-compliance.

An enforcement notice is intended primarily to secure compliance rather than punish misconduct.

12.7.2 Penalty Notices and Administrative Fines

Where an organisation fails to comply with an enforcement notice, the Commissioner may issue a penalty notice under Section 62.

In determining whether to impose a penalty and the amount payable, the Commissioner must consider the factors listed under Section 62(2), including:

- the nature and seriousness of the breach;
- the number of affected data subjects;
- the duration of the breach;
- whether the breach was intentional or negligent;
- measures taken to mitigate harm; and
- previous compliance history.

Under Section 63, administrative fines may reach:

- KES 5 million per breach; or
- up to one percent of its annual turnover for the last financial year in the case of an undertaking.

12.7.3 Compensation Orders

Under Section 65, any data subject who suffers damage because of a violation of the Act is entitled to compensation.

Compensation may be awarded for:

- financial loss;
- emotional distress;
- reputational harm;
- invasion of privacy; and
- other proven damage arising from unlawful processing.

This remedy is particularly significant because it creates direct financial consequences for organisations that mishandle personal data.

12.7.4 Criminal Liability

Certain violations attract criminal sanctions.

For example:

- Section 72 criminalises unlawful disclosure of personal data.
- Section 73 provides the general penalty framework for offences under the Act.

Criminal liability may attach not only to organisations but also to directors, officers, employees, and other individuals responsible for unlawful conduct.

Reflection: What This Means for nonprofits

The enforcement framework under the Data Protection Act demonstrates that compliance is a legal obligation rather than a voluntary best practice. Nonprofits should therefore ensure that appropriate data protection measures are integrated into their operations, particularly where they process sensitive personal data relating to beneficiaries and vulnerable groups. Responding promptly to complaints, addressing compliance gaps, and engaging constructively with the ODPC can help organisations avoid more serious enforcement action and strengthen trust with the communities they serve.

12.8 Right of Appeal

Judicial oversight of the Commissioner's decisions is provided under Section 64 of the Data Protection Act. Any person aggrieved by an administrative action of the Commissioner may appeal to the High Court.

Appeals may arise from:

- enforcement notices;
- penalty notices;
- complaint determinations; and
- other administrative actions taken under the Act.

The right of appeal promotes accountability and ensures that the ODPC's powers remain subject to judicial scrutiny.

Under Regulation 19, appeals relating to enforcement notices must be lodged within thirty (30) days of service.

As an alternative, Regulation 18 permits an affected organisation to seek review by the Commissioner before the compliance period expires.

Grounds for review include:

- emergence of new facts;
- changed circumstances; or
- evidence that compliance with part of the notice is unnecessary to remedy the breach.

12.9 Key Takeaways

- The ODPC is a constitutionally established independent office.
- The ODPC's mandate can be grouped into three roles; regulatory, enforcement, and advisory
- The ODPC provides a real, accessible complaints pathway for data subjects. Understanding the end-to-end complaints process equips organisations to respond appropriately when a complaint is lodged against them.
- Enforcement notices, penalty notices, and criminal prosecution are triggered by different types and severities of non-compliance and carry different obligations.

12.10 Assessment

Part A: Knowledge and Conceptual Understanding

1. Identify five key functions of the ODPC and provide one example of an activity undertaken under each function.
2. Who may lodge a complaint with the ODPC under Regulation 4 of the Complaints Handling Procedure and Enforcement Regulations, 2021?
3. What information should be contained in a complaint submitted through Form DPC 1?

Part B: Applied Analysis

A community-based organisation operating a nutrition programme collects detailed medical information from beneficiaries. A beneficiary later discovers that her health records were shared with a private pharmaceutical company without her consent.

1. How can the beneficiary initiate a complaint?
2. What steps would the ODPC take after receiving the complaint?
3. What remedies could be awarded if the complaint is upheld?

Part C: Organisational Reflection

1. Is your organisation currently registered with the ODPC? If not, what steps do you need to take?
2. Does your organisation have a documented procedure for responding to an ODPC audit or complaint investigation?
3. If a beneficiary reported a data protection violation to the ODPC about your organisation, what evidence of compliance could you produce?

Annexures

9.13 KEY LEGAL REFERENCES

Legal Instrument	Key Provisions Covered in This Module
DPA 2019, Sections 2, 18–22	Definitions; Mandatory registration of data controllers and processors
DPA 2019, Section 23	Regulatory audits by the Data Commissioner
DPA 2019, Section 26	Data protection principles; general data subject rights
DPA 2019, Sections 27–38	Full range of individual data subject rights
DPA 2019, Section 28	Data Protection Officer appointment and role
DPA 2019, Section 29	Duty to inform data subjects before or during collection
DPA 2019, Section 35	Processing personal data relating to a child
DPA 2019, Sections 41–42	Security obligations; factors for determining measures
DPA 2019, Section 43	Data breach notification — 72-hour controller obligation
DPA 2019, Section 46	Sensitive personal data — stricter processing grounds
DPA 2019, Sections 48–49	Cross-border transfer of personal data
DPA 2019, Sections 58, 62, 65, 72	Enforcement notices, administrative fines, civil liability, criminal penalties
General Regulations 2021, Regs. 6, 27–36	Data protection by design/default; elaboration of each principle
General Regulations 2021, Regs. 37–38	Categories of notifiable data breach; breach notification procedure
General Regulations 2021, Regs. 41–45	DPIA requirements, conduct, prior consultation
General Regulations 2021, Regs. 7–20	Data subject rights procedures and response timelines

ABOUT THIS MANUAL

Kenya's non-profits handle some of the country's most sensitive personal data, including beneficiary records, health information and donor details, often without a clear path to compliance. This toolkit closes that gap with a practical, chapter-by-chapter guide to the Data Protection Act, 2019, built for programme staff, data protection officers and leadership teams across the sector.

Includes an in-depth chapter on Consent & Vital Interests as lawful bases for processing, a core focus of this manual.

- Privacy fundamentals & key concepts
- The legal & regulatory framework, incl. the DPA 2019
- Lawful bases, consent & data subject rights
- Enforcement, penalties & the right of appeal
- Checklists, case studies & self-assessments in every chapter

1ST EDITION 2026

dpo 360 | ICN DATA AND LEARNING | KENYA AMNESTY INTERNATIONAL