OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Notes for Public Sector

2025

TABLE OF CONTENTS

DEFINITION OF TERMS

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

"Anonymisation" means the removal of personal identifiers from personal data so that the data subject is no longer identifiable.

"County Corporation" refers to a corporate entity established by a county government to deliver public services or carry out commercial activities on behalf of the county.

"County Department" means is a functional unit within a county government responsible for managing specific sectors or services at the county level.

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

"Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of Processing of Personal Data;

"Data Handler" means a data controller and/or data processor;

"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.

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

"Establishment documents" includes

(a) a Statute, Charter or statutory instrument in which a body is established;

(b) registration certificate;

(c) trust deeds in which a trust has been established; and

(d) other instruments by which a body is established including its governing and administrative structure.

For purposes of this guidance note, the Establishment document required is a list of all entities under the registering entity.

"Non-exempt mandatory registration Entities" means Entities that are required to register regardless of their Turnover/ Revenue, or the number of staff employed.

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

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

"Processing" means any operation or sets of operations which is performed on Personal Data or on sets of Personal Data whether or not by automated means, such as:

a) collection, recording, organisation, 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

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

"Public Sector" means organisations, institutions, and bodies that are part of the government and are responsible for delivering public services, governance, and managing public resources.

"Register of Data Controllers and Data Processors" means the list of registered Entities maintained and published by the Office of the Data Protection Commissioner.

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

"Revenue" means the total income of profit-making Data Controllers or Data Processors for the year immediately preceding the year of registration.

"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.

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

"Turnover" means the utilised annual budget of non-profit making Data Controllers or Data Processors for the year immediately preceding the year of registration

"Registering Entity" means a state or county department, a state or county corporation, which oversees and or funds all the entities under it.

FOREWORD

The protection of personal data is a constitutional right enshrined under Article 31 of the Constitution of Kenya, 2010. It is also the foundation upon which trust in digital government services and the broader digital economy must be built. As Kenya accelerates its digital transformation through the Digital Superhighway and the Bottom-Up Economic Transformation Agenda (BETA), safeguarding of citizens' personal information becomes not only a legal imperative but also a moral duty.

The Office of the Data Protection Commissioner (Office) established under the Data Protection Act, 2019, is mandated to regulate the processing of personal data and to enforce compliance across both the public and private sectors. Public institutions, in particular, hold vast amounts of personal data in the course of delivering essential services such as health, education, social protection, and public administration. This makes the role of the public sector central in embedding a culture of compliance, accountability and transparency in data processing practices.

This Guidance Note for the Public Sector has been developed to provide clear and practical direction to ministries, departments, state agencies, state corporations and county governments regarding their obligations under the Data Protection Act, 2019 and attendant Regulations. It sets out the principles, lawful bases for processing, data subject rights, and institutional responsibilities in a manner that reflects the unique realities and privacy risks inherent in public sector operations.

By adhering to this guidance, public sector entities will not only comply with the law but also strengthen public trust, enhance service delivery, and mitigate the risks associated with misuse or mishandling of personal data. The Office remains committed to supporting institutions in their compliance journey through continuous capacity building, stakeholder engagement and enforcement where necessary.

It is my expectation that this Guidance Note will serve as a critical reference point for all public institutions as they mainstream data protection into their policies, system and operations. In so doing, we collectively safeguard the dignity and rights of Kenyans while advancing Kenya's vision of a trusted and inclusive digital economy.

Immaculate Kassait, MBS
Data Commissioner

1. OFFICE

The Office of the Data Protection Commissioner (Office) is a government agency established to protect the privacy and security of personal data in our increasingly digital world. It is responsible for enforcing data protection laws and policies to safeguard the privacy, dignity, and fundamental rights of individuals. The Office is mandated to oversee the implementation and enforcement of the Data Protection Act, 2019, which regulates the processing of personal data of persons located in Kenya by both private and public sector organisations.

The Office plays a vital role in ensuring that individuals have control over their personal data and that organisations respect their privacy rights. The Office's work involves monitoring and enforcing compliance with data protection regulations, investigating data breaches, and imposing sanctions on entities that violate data protection laws. In addition, the Office is responsible for raising public awareness about data protection issues and educating individuals and organisations on how to protect personal data. With the growing importance of data protection in our digital age, the Office is a critical institution in maintaining trust and confidence in our data-driven society.

The Office is uniquely positioned to facilitate both the government and private sector entities in achieving Government's strategic goals under the "**Bottom-Up Economic Transformation Agenda**" and, in particular, its digital superhighway initiative. As the digital landscape expands, the need for robust data protection mechanisms becomes paramount. The Office, with its mandate to oversee, regulate, and ensure lawful data processing, plays a pivotal role in this transformation.

Kenya remains at the cutting edge of digital transformation while maintaining stringent data protection standards. The Office serves as a key stakeholder and regulator in guiding the nation's digital superhighway journey by ensuring that as we advance technologically, the rights and privacy of individuals remain safeguarded.

2. INTRODUCTION

2.1. Background

The Kenyan public sector has a multifaceted structure encompassing ministries, independent commissions, 47 county governments, semi-autonomous government agencies (SAGAs), state-owned enterprises, and various agencies. Public institutions are instrumental in policy implementation, achieving the government's goals and providing a wide range of essential services to citizens, including education, healthcare, public safety, and social services. State-owned enterprises in Kenya operate in various sectors and contribute to the country's economic development. They are typically government-owned or government-controlled entities that engage in commercial activities.

Public institutions are subject to the Act and Regulations when processing personal data relating to individuals. Data protection and privacy have become significant considerations in public sector operations, guided by the Act. The National Digital Master Plan further accelerates

the need to ensure data protection compliance in the public sector as the provision and management of e-government information and services, and a fully digitised ecosystem will result in the processing of large volumes of data. This means that proper data handling and management will have to be adopted to ensure that users are protected accordingly by ensuring that data is processed on reliance of a proper lawful basis, ensuring that data is accurate and up-to-date, and protecting data from unauthorised access, use, and disclosure.

The Office has published guidance notes which are relevant to the public sector, including but not limited to, the Guidance Note on Data Protection Impact Assessment (DPIA), Guidance Note on Consent and the Data Protection Handbook. Still, considering the public sector's pivotal role in establishing a culture of compliance and best practices at the national and county levels, the Office has developed this sectoral guidance to provide public institutions with a holistic and contextualised understanding of the data protection principles and requirements.

2.2. Privacy Concerns

The nature of processing data in the public sector raises significant privacy concerns, including the potential misuse of personal data and lack of transparency around data collection and processing of personal data. A need has thus arisen for the public sector to take steps to ensure that personal data related to the provision of public services are processed fairly and transparently, with appropriate data protection measures in place to safeguard personal data against unauthorised access, disclosure, or loss.

The adoption of technologies and the digitisation of government services through platforms such as Integrated Financial Management Information Systems (IFMIS), E-Citizen Portal, Enterprise Resource Planning (ERP) Systems and Customer Relationship Management (CRM) Systems have allowed for the collection and analysis of data from various sources to make informed management decisions, enhancing the quality of services and increasing citizen satisfaction. However, this transition to digital applications has come with its own set of privacy concerns. They may become a target for cyberattacks, accidental leakage, and misuse, putting the privacy of collected and stored public data at risk.

Additionally, the digitisation of various processes from the traditional manual records such as Health Management Information System (HMIS), eHealth and mHealth applications entails the processing of highly sensitive personal data and must therefore be required to meet the data protection standards for proper mitigation of possible risks that come with the entire processing activities.

Similarly, personal data collected by public health agencies through projects that require online service delivery and mass collection of data electronically, such as Social Health Insurance Fund, must be done in a manner that is fully compliant with the Act by addressing the privacy concerns of the data subjects adequately.

These risks are often compounded by the lack of adequate data security measures and the involvement of parties in the public sector that may not follow the highest data protection standards, especially when public entities are in the processof digitising their paper-based records and operations. Therefore, the framework of data protection in the public sector in Kenya has become increasingly important.

2.3. Scope and Purpose of Guidance Note

The purpose of this guidance note is to provide the public sector with a clear understanding of their obligations under the Act and Regulations. The guidance note aims to cover various

aspects of data protection, including the collection, use, retention, disclosure, and disposal of personal data in the public sector.

This guidance was developed to guide public entities in ensuring legal compliance, upholding privacy rights, and protecting against various risks that come with processing of personal data.

It outlines the specific considerations and best practices for handling personal data in the context of all processing activities done by public entities. This includes addressing issues such as obtaining consent, protecting the privacy rights of individual stakeholders, and securely managing and storing personal data.

This guidance note shall apply to all public entities operating in Kenya across all sectors and should be regarded as a minimum standard that can be supplemented by additional measures for the protection of privacy and individual rights, which may impact or be impacted by the processing of personal data.

This Guidance Note considers:

a) The Data Protection Act, 2019;
b) The Data Protection (General) Regulations, 2021;
c) The Data Protection (Registration of data controllers and data processors) Regulations, 2021;
d) The Data Protection and Privacy Policy, 2018;
e) Other applicable laws and regulations and;
f) International Best Practices.

3. LEGISLATIVE FRAMEWORK

The public sector in Kenya is governed by several legislative framework including but not limited to:

i) The Constitution of Kenya,2010

Article 31 (c) and **(d)** guarantee individuals the right to privacy concerning information related to their family or private affairs that is unnecessarily required or disclosed, as well as protection against infringement of their communications.
Article 132 provides for the functions of the President, including responsibilities related to state departments and public services.
Article 152 provides for the accountability of Cabinet Secretaries for the state departments they oversee.
Article 235 establishes the County Public Service Board and provides for the staffing of county governments.
Article 248 provides for the establishment of commissions and independent offices
Article 155 establishes the office of Principal Secretary, which is an office in the public service.

ii) State Corporations Act (Cap 446)

This Act provides rules for the establishment, administration, management and operation of state corporations.

iii) The County Government Act (No. 17 of 2012)

This Act provides a framework for the establishment and governance of county governments in Kenya as outlined in the Constitution.

iv) The Data Protection Act, 2019

The public sector operates under an extensive array of laws and regulations and the legislative framework above only represents a portion of a substantive legal framework, which is designed to ensure accountability, transparency, and effective governance across various levels of government.

4. APPLICATION OF DATA PROTECTION PRINCIPLES

4.1. Lawfulness, fairness, and transparency

Personal data collected by the public entities must be processed lawfully, fairly, and in a transparent manner. Lawful processing requires identifying a legal basis for processing the personal data such as obtaining the consent of the data subject, fulfilling a contract, complying with a legal obligation, protecting the vital interests of a data subject, performing a task carried out in the public interest or exercising official authority, or pursuing legitimate interests.

Further, data handlers in the public sector need to treat individuals fairly and not use their data in ways that would have unjustified adverse effects. The personal data processed should be handled in a way that a data subject would reasonably expect and ensuring that it does not unjustifiably harm their rights and interests.

Data handlers should process personal data in a clear and transparent manner by ensuring they maintain a privacy notice that informs data subjects of the types of personal data collected, how it will be used, their rights and freedoms and how they can be exercised and the security measures in place to protect and secure that information. The privacy notice should be written in clear and plain language, be understandable and easily accessible. Where a Public entity processes personal data belonging to children, the entity should ensure that the processing is addressed in the privacy notice and that appropriate mechanisms are implemented for age verifications and management of parental/guardian consent.

Example 1

The Ministry of Education gathers information on students, including their names, ages, and academic achievements, in order to carry out a national digital learning initiative. This data processing is legally justified by the performance of an official task and the exercise of authority as outlined in the Basic Education Act and the Data Protection Act. The Ministry adheres to the transparency principle by ensuring that information about data processing is easily accessible and easy to understand by students, their parents and guardians, educational institutions, as well as the public.

Example 2

The XYZ County Government is currently providing support to individuals affected by drought by offering food aid and financial assistance. In doing so, the County relies on public interest as a lawful basis to collect personal data, such as names, ID numbers, contact details, and location for distribution purposes. To promote transparency and foster a just and lawful approach to data collection and processing, the County should ensure that individuals are fully informed about how their information will be used. Further, any publication of personal data is anonymised.

4.2. Purpose limitation

The purpose limitation principle requires data to be collected only for specified, explicit, and legitimate purposes and prohibits further processing in a manner that is incompatible with

those (initially determined) purposes. To comply with this principle, public sector entities must have clarity on what personal data will be used for and should not be used for any other purpose inconsistent with the identified legal purposes/basis.

However, considering the exemptions under Part VII of the Act, public institutions may undertake further processing of data if it is necessary for national security or public interest, where there are sufficient safeguards in place. In addition, according to Section 53, the further processing of personal data could be considered compatible with the initial purpose of collection if data is used solely for historical, statistical, or research purposes and will not be published in an identifiable form.

Example

A county government department collects citizens' personal data, including full name, national identification number, and physical address strictly for the purpose of enrolling eligible individuals into a public health subsidy program. The department is prohibited from using this data for any secondary or unrelated purpose, such as political mobilisation, or commercial marketing, unless the data subject has explicitly consented to such use, or the further processing is otherwise authorized under applicable law.

4.3. Data Minimisation

The data minimisation principle requires that only personal data, which is adequate, relevant, and limited to what is necessary for a specific, lawful purpose should be collected and processed. This means public entities must not collect more data than is needed to fulfil an intended function. By collecting what is necessary, public entities demonstrate that they respect data subjects' privacy, simplifies data management, and reduces legal and reputational risks.

Therefore, for each processing activity, they must identify the minimum data required to achieve the intended purpose.

Example 1

The Mamboleo government agency has launched an online service for citizens to access the social welfare program. In applying the data minimisation principle, the agency strictly limits the personal data it collects to only what is necessary for processing applications. Applicants are required to provide only basic identification details, including, name, date of birth, national ID number, and contact information. The agency avoids collecting any additional personal information that is not directly relevant to determining eligibility for the service.

Example 2

Department Q is conducting a national census to gather accurate population data. In doing so, the department collects only the information that is necessary and relevant to the purpose, including basic details such as age, gender, location, and household size. In applying the data minimisation principle, the department avoids collecting unnecessary sensitive information, such as health status, unless it is directly required for a specific government programme. This ensures that the census meets its goals while also respecting individuals' rights and limiting the collection of personal data.

4.4. Accuracy

This principle, mandates that personal data collected and processed must be accurate and, where necessary, kept up to date, with necessary steps being taken to ensure that inaccurate data is erased or rectified. Data handlers in the public sector should take every reasonable step to ensure that inaccurate personal data is erased or rectified without delay. To comply with this principle, and as part of their data management, public institutions should implement clear procedures enabling prompt detection/reporting of inaccuracies, correction, or erasure of any inaccurate personal data.

Example

Commission (IEBC) maintains a precise and current voter registration log. Before the elections, they carry out routine verification processes and provide chances for citizens to revise their details, guaranteeing the accuracy of the data they maintain.

4.5. Storage Limitation

This principle requires data handlers in the public sector to ensure that personal data is not stored for longer than is necessary to fulfil the purposes for which it was collected. public sector entities should establish personal data retention schedule with appropriate timelines and ensure it is reviewed periodically to assess the need for continued storage. Additionally, personal data should be erased, deleted, pseudonymised or anonymised where it is no longer needed. However, personal data may be stored for more extended periods for reasons of public interest, scientific or historical research purposes, or statistical purposes if there are appropriate technical and organisational safeguards measures to protect the rights and freedoms of the data subjects.

Example 1.

Kazi Mtaani Program focuses on carrying out community projects within the country where they collect and store information about seasonal employees. To comply with the storage limitation principle on retention and deletion, they should periodically review this employee information and erase or anonymise the data once it is no longer needed for the project's purposes and only retain this data for the required timeframe before proceeding with deletion or anonymisation.

Example 2.

When an individual submits an application to a government organisation X, their personal details, educational background, and references are gathered. Once the selection procedure is completed, the principle of storage limitation requires the government organisation to either delete or securely discard the personal information of unsuccessful candidates after a reasonable period, unless there is a valid justification for retaining it for a longer duration.

4.6. Integrity and Confidentiality

This principle requires that personal data be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing against accidental loss, destruction, or damage. Therefore, all technical procedures used to gather, process, store, use, or distribute data should make use of strong security safeguards, for which threshold standards must be established. This may involve but is not limited to data encryption, security keys, two-factor authentication, and password requirements.

Example

State Department Y collects and processes farmers personal data for the purpose of mango seedlings distribution. To ensure the integrity and confidentiality of the data, the department ensures that all personal data collected from the farmers such as Name, ID numbers and contact information is stored in a secure and encrypted database. Access to the database is only restricted to authorised persons using two-factor authentication and role-based access. The department does regular validation assessment checks and audit trails of its system and processes to identify and address any vulnerabilities or risks that could compromise the security of the stored personal data.

4.7. Accountability

Accountability involves taking proactive steps to protect personal data and demonstrating of adherence to data protection principles. The accountability principle within the public sector refers to the responsibility of data handlers to ensure compliance with relevant laws and regulations related to the collection, use, and disclosure of personal data and sensitive personal data.

Data handlers in the public sector should have policies and procedures in place to govern the processing of personal data which should be reviewed and updated regularly to ensure compliance with changing legal and regulatory requirements.

Example

The Uwezo Ministry has demonstrated compliance with data protection principles by adopting and implementing data protection practices in its processing activities e.g. conducting data protection impact assessment (DPIAs), regular audits and assessments, robust data breach response plan and staff training. The company maintains a privacy policy and records of the processing activities and has appropriate data security measures in place. It has also designated one of its employees to be the Data Protection Officer responsible for ensuring compliance with the Act.

5. APPLICATION OF THE LAWFUL BASIS OF PROCESSING PERSONAL DATA

5.1. Performance of a task carried out by public authority

Personal data may be processed where it is necessary for the performance of a task carried out in the exercise of official authority vested in a public entity. Compliance with public authority is essential for public sector entities to operate legally, protect their interests, and maintain trust with the public. The exercise of public authority may apply in various contexts including, public health programmes, law enforcement activities, social protection services, regulatory oversight and administrative functions. Entities in the public sector may rely on public authority as a lawful basis to process personal data necessary for the performance of

their tasks in the public interest or in the exercise of official authority and ensure the protection of the data in accordance with the data protection laws.

Example

John, a Kenyan citizen, applies for a driver's license at the Transport Regulatory Authority (TRA). He submits his personal information, including his full name, National ID number, and contact details. TRA verifies John's eligibility by cross-referencing his National ID number with government databases to confirm his age and citizenship status. The Authority uses his contact information to notify him about his upcoming driving test and later informs him when his driver's license is ready for collection.

John's personal data is securely stored in TRA's database, and his license details are maintained in the national driver registry. If John commits a traffic offense, TRA may share his license information with law enforcement agencies, but only within the scope of their public safety responsibilities.

5.2 Public Interest

The Act provides that personal data may be lawfully processed if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller provided it aligns with the principles of lawfulness, fairness, and transparency.
Areas where public interest justifies the processing of personal data include:

a) Health and Safety

Public authorities may collect, store, and analyse personal information to effectively respond to health emergencies, prevent diseases from spreading, ensure food safety regulations are followed, and address other health-related concerns.

Example

Misitu Ministry processes personal data, such as names, contact information, and medical details, under the lawful basis of public interest. This data processing is essential for coordinating rescue and relief operations after a landslide, ensuring effective deployment of resources, and prioritising assistance to those most affected. The Ministry follows transparency, security, and data retention practices to comply with the Data Protection Act and protect individuals' rights during the disaster response.

b) Policy Development

Personal data can be processed for policy development purposes aimed at addressing social issues or improving governance. This may involve collecting and analysing personal information to inform policymaking decisions related to education, healthcare systems improvements, poverty alleviation strategies, crime prevention initiatives or research that contributes to scientific advancements with potential societal benefits.

Example

Kilimo Ministry processes personal data such as farmer names, crop yields, farming practices, and pest reports under the lawful basis of public interest. This data is used to develop policies aimed at enhancing agricultural productivity, sustainability, and food security. By analysing the data, the Ministry can identify effective farming practices, understand climate impacts, and create targeted support programs for farmers. This approach improves agricultural practices, supports technology adoption, and contributes to better livelihoods for Kenyan farmers.

C) Strategic Interventions

Personal data may be processed in support of strategic intervention efforts undertaken by public authorities that aim to improve service delivery or promote economic growth.

Example

RUNA LABS collects data on participant profiles, training progress, skills acquired, employment status, and ICT center usage. This helps provide youth across Kenya with digital skills training and remote work opportunities at government-owned ICT centers. By analysing the data, RUNA LABS can tailor training programs to regional needs and monitor their impact on youth employment. This will enable RUNA LABS to equip young people with relevant skills, allowing them to work online and participate in the digital economy. This initiative reduces unemployment, improves digital skills and boosts economic growth in various regions of Kenya.

5.3. Consent

For public authorities, obtaining an individual's consent is one of the lawful bases to process personal data. However, consent is not always required where the entity can rely on another valid basis. Section 2 of the Act defines the meaning of consent as being:

- **Specific:** The data subject shall be informed about the specific purpose for which their data will be processed.
- **Informed:** The data subject must be provided with sufficient information to make an informed decision about whether or not to give consent. This includes information about the types of personal data that will be processed, how the data will be used, who will have access to the data, and how long the data will be retained.
- **Freely given**: The data subject must be given a genuine choice about whether to give consent or not. Consent cannot be coerced or forced, and there must be no negative consequences for the data subject if they refuse to give consent.

Example 1

John is set to participate in an event organised by Utawala Ministry. To register for the seminar, attendees are required to complete an online form. The form includes an optional checkbox, allowing John to provide consent for receiving notifications about future ministry events via email.

Additionally, the form outlines that John retains the right to revoke his consent for marketing communications at any time by contacting the ministry.

5.4. Performance of a contract

Personal data may be lawfully processed where it is necessary to fulfill a contractual obligation between the data subject and a public entity.

Example 1.

The public transport agency XYZ engages TransitKE Ltd. to operate a fleet of buses. The lawful basis for processing personal data, such as driver and passenger information, is the performance of the contract. This involves managing bus operations, ensuring safety, and delivering services effectively. Data is collected and processed transparently and securely and is retained only as long as necessary for contract fulfillment and regulatory compliance.

5.4. Legal Obligation

Data handlers in the public sector must adhere to specific conditions when processing personal data. Primarily, they must ensure the processing meets a lawful purpose, including complying with the legal obligation to which the entity is bound. The law underpinning the obligation must be clear and precise, ensuring its application is foreseeable to those subject to it. While the law may not explicitly demand specific data processing activities, the processing must be **genuinely necessary to fulfill the legal obligation**. This necessity criterion ensures that data controllers and processors do not engage in data processing arbitrarily but rather as a proportionate means to achieve compliance with legal requirements.

(i) Necessity and Clear Nexus

To justify data processing under the pretext of complying with a legal obligation, there must be a clear nexus between what is stated in the law and the processing activity. The processing must be genuinely necessary to fulfill the legal obligation, ensuring it is not conducted arbitrarily but as a proportionate means to achieve compliance.

(ii) Framework for Assessing Necessity and Clear Nexus

a. Identify the Legal Obligation:

- Determine the specific legal obligation under national or regional law that mandates the processing of personal data.
- Ensure the obligation is clear, precise, and its application is foreseeable.

b. Establish the Connection:

- Identify the specific processing activities required to comply with the legal obligation.
- Ensure there is a direct and clear connection (nexus) between the legal obligation and the processing activity.

c. Assess Necessity:

- Evaluate whether the processing is genuinely necessary to comply with the legal obligation.

- Consider whether the processing is a reasonable and proportionate means to achieve compliance.

d. Consider Alternatives:

- Determine if there are less intrusive means available to comply with the legal obligation.
- If an alternative, less intrusive method exists, the processing may not be considered necessary.

e. Evaluate Proportionality:

- Assess whether the scope and extent of the data processing are proportionate to the legitimate aim or goal pursued.
- Ensure the processing adheres to the principle of data minimisation, limiting the data processed to what is relevant and necessary.

f. Document and Justify:

- Maintain documentation that demonstrates the necessity and proportionality of the processing.
- Ensure there is a clear justification for why the specific processing activities are required to comply with the legal obligation.

The processing must be based on and must be grounded in clear and precise laws, ensuring a direct connection between the legal requirement and the processing activity. By following the framework for assessing necessity and establishing a clear nexus, data controllers and processors can ensure that their data processing activities are justified, reasonable, and proportionate to the legal obligations they are fulfilling.

Example

A County Public Service Board (CPSB) is mandated to perform human resource functions, including recruitment and staff performance management. The CPSB collects and processes personal data such as KRA PIN, and NSSF numbers during recruitment and throughout the employment period of a public officer. To comply with the statutes requiring employers to remit these statutory deductions, the CPSB will process this data to to comply with legal requirements.

5.5. Vital Interest of the Data Subject or another natural person

The Act recognises situations where processing personal data is necessary to protect the vital interests of the data subject or another natural person. Vital interests are those fundamental aspects of their life that are crucial for their well-being, survival, and fulfilment. In such cases, organisations, including entities in the public sector, may process personal data without the explicit consent of the data subject, especially if obtaining consent is impossible.

Example

The disaster response unit, Usalamakwanza processes personal data, such as contact information and medical details, under the lawful basis of vital interest. This process is essential for providing emergency relief, conducting rescue operations, and ensuring public safety during a natural disaster. Usalamakwanza follows transparency, security, and data retention practices to comply with the Data Protection Act.

5.6. Legitimate Interest

The Act provides that personal data may be processed if it is necessary for the purposes of the legitimate interests pursued by the data handler or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection. Public sector entities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.

RIGHTS OF DATA SUBJECTS

These are rights of a data subject exercisable with respect to the processing of their personal data. The Act provides data subjects with certain enforceable rights regarding their personal data.

The Act aims to empower citizens to exercise their rights in a world increasingly dominated by technological companies and other players that process vast amounts of data relating to citizens. Adherence to the rights of data subjects is of utmost importance in the context of public institutions. It is the duty of public sector service providers to provide data subjects with mechanisms and avenues where the data subject can exercise their rights.

To facilitate this, public entities can develop privacy notices and ensure that they are up to date and fit for the purpose. A privacy notice can be published on website and directed externally to explain how the entity processes and protects personal data, for which purpose and based on which legal grounds they are collected, how long it will be retained, what security measures are applied and how the data subjects can exercise their rights. It should be concise, intelligible and easily accessible, written using a clear and plain language.

Right to be informed

This is the right to be informed of the use of the data. It allows data subjects to know what personal data is collected about them, why, and who is collecting data, how long it will be kept, how they can file a complaint, and with whom they will share to. The duty to inform can be exercised at the time of collecting personal data or any time after it has been processed.

Example

The State Department ABC collects personal data from data subjects during onboarding to the registration portal, including names, ID numbers and contact information. To comply with the right to be informed, the Department provides a privacy notice accessible over their portal to all relevant individuals explaining how their personal data will be used, who will have access to it, how long it will be retained and the safeguard measures in place to secure the personal information.

Right to access personal data

A data subject has the right to access personal data in the custody of the public institutions that is, which type of data is held about them, details of the data control, details of any

recipients, and data retention period. This right allows the data subject to have visibility on what personal data is being processed.

To exercise this right, a data subject can make an access request. The Regulations require that an access request be fulfilled within 7 days and should be free of charge.

Example

Tenge, wants to access her personal data held by a public utility company responsible for providing water and sewerage services. This access should be granted within 7 days upon request.

Right to rectification of personal data

This means that individuals have the right to request corrections to inaccurate or incomplete information held about them in the public institution's records. The public institutions must implement a process and the technical capabilities to verify the request, correct the data and confirm correction with the data subject.
Overall, the right to rectification of personal data is important for ensuring that individuals have accurate and complete information, which can ultimately lead to better service delivery.

Example

Omweno discovers that his personal details, such as his address and next of kin information, are incorrect in the records held by his employer in Ministry of ABC. He wants to rectify these inaccuracies. The ministry has made it easy for individuals to request corrections by implementing a straightforward process, having the necessary technical capabilities and a data protection policy that guides data subjects on how to exercise their rights. Omweno can easily submit his request for correction through an online portal. The ministry promptly verifies the request by confirming his identification details, corrects the data, and confirms the correction with Omweno. This ensures that individuals have accurate and complete information.

Right to object to all or part of their personal data being processed

This right allows data subjects to object to the processing of their personal data. This involves stopping the processing of personal data. Whether a data subject can object to processing depends on the legal basis on which such personal data is processed. A data subject may not object to processing if the personal data is being used:

i. For a task carried out in the public interest;
ii. For the exercise of official authority; and
iii. For the legitimate interests of the data controller/processor that override the data subject's interests.

A request to object to processing cannot be fulfilled where the personal data is required to establish, exercise or defend a legal claim and where a data controller's legitimate interests override the data subject's interests.
A data subject may exercise this right by;

i. Giving a verbal or written reason(s) why the controller should stop using the data; and
ii. Stating what should happen to the personal data.

A data controller will then be required to inform the data subject of the objection's result.

Example 1

Kamau, applied for a student loan from Masomo loan government program which also sends notification messages on loan repayment progress. Kamau, after completion of loan payment noted that he still received messages on loan repayment and decided to communicate to the Masomo loan to stop the sharing of messages. Masomo loan after verifying Kamau's credentials noted that he had already cleared his loan but was erroneously not cleared from the system. Masomo loan complied with Kamau's request by clearing his details from the system and confirming with him that no further messaging will take place.

Example 2

A National Health Agency collects personal health data for the purpose of surveillance of infectious disease under a legal mandate. When a data subject objects to this processing based on privacy concerns, the agency lawfully rejects the objection by demonstrating that the processing is legally required, necessary, proportionate, and aimed at protecting public health, with appropriate safeguards in place. Therefore, the data subjects' right to object is overridden by the legitimate public interest in controlling and preventing disease outbreaks.

Right not to be subjected to automated decision making

This right protects a data subject from being subjected to a fully automated decision. An automated decision takes place when an electronic system uses personal data to make a decision without human intervention.

As with other data subject rights, this is not an absolute right, and a data processing subjected to decision making that is based solely on automated processing under certain circumstances; such as where a data subject consents, where a decision is necessary for entering or performing a contract between a data subject and a data controller, and where such automated decision making is authorised by a law that has suitable safeguards. Public entities that make decisions which produce legal effects or significantly affect the data subject based solely on automated processing must notify the data subject as soon as reasonably practicable and take necessary steps such as reconsidering the decision or making a new decision not based solely on automated processing.

Example 1

Ministry X has launched a new online social welfare platform that collects applicant details, that is Name, ID no, Contact information, income, employment status. The platform uses automated algorithms to screen and reject applicants based solely on keywords or

predetermined criteria without any human review. In this scenario, Ministry X should ensure that there is a human component involved in the application review process to prevent unfair treatment and ensure that all applicants are fairly evaluated based on merit.

Example 2

Wezesha Youth Development Fund uses an automated system to determine the loan amount to be advanced to the youths based on the information collected from them when applying for the same such as the financial background of their family. The process must involve human intervention to ensure prevention of any possible bias that could result from the automated processing in the determination of the amount of public funds to be allocated to the respective youths.

Right to erasure

This right, commonly referred to as the right to be forgotten, allows individuals to request the deletion or removal of their personal data held by the public entity. A data subject may request a data handler to delete personal data concerning them when the data handler is no longer authorised to retain the personal data, the personal data is irrelevant, the personal data held by the data handler is excessive or the personal data was obtained unlawfully.

Where the data handler has shared the personal data with a third party for processing purposes, the data handler shall take all reasonable steps to inform third parties processing such data, that the data subject has requested for the erasure or destruction of such personal data.

However, the right to erasure is not absolute, and a data controller may decline upon a request to erase personal data in its custody when the personal data is required for evidence. In this case, the data controller shall restrict processing and inform the data subject within a reasonable time frame. A request to erase data shall be met within 14 days.

Example

Maria wants to exercise her right to erasure (also known as the right to be forgotten) regarding her personal data held by a public housing authority. Maria had applied for public housing assistance, but her circumstances have changed, and she no longer requires or wants her personal data to be stored by the authority. The public housing authority also notices that the prescribed 6 months retention period as per their Data Retention Policy had already lapsed. Upon verification of the request, public housing authority goes ahead and securely deletes /anonymises the records from their database and notifies all third-party contractors to do the same within 14 days.

Right to data portability

This right allows a data subject to receive a copy of their personal data in a structured, commonly used, and machine-readable format, and the right to transmit that data to another data controller without hindrance, where this is technically possible.

A data controller may charge a reasonable fee for the request. While there is no stated figure, best practice dictates that the fee must be reasonable and should not exceed the cost of implementing the request.

Example

David has secured employment in parastatal ABC. He requires Ministry XYZ where he works to transfer to the parastatal a copy of his records to streamline his records and ensure consistent information regarding pension benefits. The Ministry XYZ must port the requested personal data to the recipient parastatal within thirty days of the request or if declined, provide a justification for the same within seven days.

OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

Registration

The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 provide that State agencies/departments or County departments shall register and pay the fees on behalf of their respective Entities. These Entities must be public Entities at national or county government which

(a) operates within a state department or county department;
(b) is wholly funded from the Consolidated Fund; and
(c) provides a public service.

For example, the State Department of Broadcasting and Telecommunications in the Ministry of Information, Communication and the Digital Economy has several directorates and agencies under it that are not deemed to be State Corporations by virtue of the State Corporations Act, 2012.

In submitting the registration application, the State Department of Broadcasting and Telecommunications will need to identify and list all public Entities that operate under it and submit one application that will cater for the State Department and the public agencies under it. However, any Entity that is a state corporation, such as KBC (for example) will need to make its own application. In understanding if an entity falls under State Department, please refer to Executive Orders (e.g the Executive Order No.2 of 2023) on the Organisation of the Government of the Republic of Kenya, available here.

The single registration fee of Kshs. 4,000/- and renewal fee of Kshs. 2,000/- after 2 years to be paid by the State department or County department will cater for all specified Entities registered or under the concerned state department or county department. A State/County Corporation or a State/ County Department will be required to register as a Data Controller or Data Processor or both in respect of their Processing activity.

Provision of Basic Details (Establishment Documents)

In the ODPC registration portal public entities falls under the State or County Department section. During the registration process, under the "Establishment document" section highlighted, below should be considered;

- If this is an independent government agency, or an entity with its own budget and no other institutions under it, upload your charter, act or order creating the public entity.
- If an entity is a state department, it will need to identify and list all public Entities that operate under it and submit one application that will cater for the State Department and the public agencies under it. For example, a list of all the schools under the State Department of Basic Education and the schools that they fund.

The Office has published a Guidance Note on Registration of Data Controllers and Data Processors which is accessible through *www.odpc.go.ke* The Guidance Note includes a step by-step guide on how to complete the registration process and the information required during the registration process.

Privacy by design and default

The Act, in Section 41, outlines the requirement for entities in the public sector to implement appropriate technical and organisational measures to ensure the effective implementation of data protection principles and necessary safeguards in data processing. Additionally, the Act requires that only necessary personal data is processed, considering the amount of data collected, the extent of its processing, storage period, accessibility, and cost of processing.

Data protection by design is an approach that ensures data controllers and data processors consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle. Data protection by default requires institutions to ensure that only data that is necessary to achieve its specific purpose is processed. Data protection by default requires entities to ensure that data protection issues have already been considered, and protection methods incorporated into existing systems and practices. This could be achieved by institutions specifying the personal data required before the processing starts, appropriately informing individuals, only processing the personal data needed for the specific purpose and implementing stringent privacy-oriented settings by default.

Example

Afya Nzuri National Hospital embraced privacy by design and default when implementing its new EMR system. The hospital conducted a DPIA, integrated privacy considerations at every stage of system design, ensured default privacy settings were applied, and trained employees on privacy principles. By doing so, the hospital ensured compliance with the Kenya Data Protection Act, safeguarded patient data, and built trust with its patients, all while maintaining efficient healthcare delivery.

Data Protection Impact Assessment (DPIA)

Public sector entities are required to conduct a DPIA where a processing operation is likely to result in high risk to the rights and freedoms of data subjects. The DPIA should include the description of the processing activities, an assessment of the necessity and proportionality for

processing, an assessment of the risks to the rights of the data subjects and the mitigation measures for addressing the risks.
Public sector entities must consult with the Office when conducting the DPIA and ensure that it is submitted to the Office sixty days prior to the processing of personal data. The Guidance note for DPIA can be accessed through https://www.odpc.go.ke/

Example.

The Kenya Social Security Agency undertakes a DPIA before implementing its digital social security platform. The assessment identifies potential privacy risks, facilitates stakeholder engagement, and proposes risk mitigation measures such as data encryption, access controls, and automated data deletion. By submitting the DPIA for review and implementing a comprehensive staff training program, the agency ensures compliance with the Kenya Data Protection Act, safeguards citizen data, and builds public trust in its services.

Notification and Communication of a Breach

Data Controllers and data processors are required to report personal data breaches to the ODPC without delay within 72 hours of becoming aware of the breach. Where there has been unauthorised access, public entities should communicate to the affected data subjects in writing within a reasonable period, unless the identity of the data subject cannot be established or justified reasons submitted to the Data Commissioner and approved. To fulfil these and other obligations under Section 43 of Act, Public Institutions should have documented robust breach detection, investigation and internal reporting procedures.

In reporting a data breach to the Office, Public Institutions need to provide the following:

1. The date on which and the circumstances in which the data controller or data processor first became aware that the data breach had occurred;
2. A chronological account of the steps taken by the data controller or data processor after the data controller or data processor became aware that the data breach had occurred, including the data controller or data processor's assessment that the data breach is a notifiable data breach;
3. Details on how the notifiable data breach occurred, where applicable;
4. The number of data subjects or other persons affected by the notifiable data breach;
5. The personal data or classes of personal data affected by the notifiable data breach;
6. The potential harm to the affected data subjects as a result of the notifiable data breach;
7. Information on any action by the data controller or data processor, whether taken before or to be taken after the data controller or data processor notifies the Data Commissioner of the occurrence of the notifiable data breach to
    i. eliminate or mitigate any potential harm to any affected data subject or other person as a result of the notifiable data breach; or
    ii. address or remedy any failure or shortcoming that the data controller or data processor believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach; the affected individuals or the public that the notifiable data breach has occurred and how an affected data subject may

eliminate or mitigate any potential harm as a result of the notifiable data breach; and

iii. contact information of an authorised representative of the data controller or data processor.

Example

National Tax Agency follows the Data Protection Act by detecting a data breach, containing it, and notifying both the Data Commissioner and the affected individuals within 72 hours. A detailed report is submitted to the Data Protection Commissioner within 5 days. The tax agency also takes steps to support affected individuals and improve data security, with ongoing communication to restore public trust.

Engagement of Data Processor

Public sector institutions often engage vendors and service providers (data processors) to manage various types of data. Examples include IT service providers maintaining government databases, legal firms handling sensitive legal information, financial institutions processing government transactions, research organisations conducting studies, and marketing agencies managing public communication campaigns.

Public Institutions must exercise due diligence in selecting registered vendors that provide sufficient guarantees of compliance with the Act and protection of data subjects' rights. Despite outsourcing, public-sector entities retain full responsibility as data controllers and are obligated to ensure that data processors implement appropriate measures to safeguard personal data. The Act mandates that a written contract must be in place when engaging data processors. This contract should specify that processors act only on the controller's instructions and adhere to the controller's obligations. Both parties must ensure compliance with security measures. The contract should cover the subject matter of processing, types of personal data, nature and duration of processing, and required security measures. It must also outline obligations for staff confidentiality, assistance in meeting legal requirements, and handling data at the contract's end. Additionally, provisions for auditing, inspection, and liability must be included.

Data controllers have an obligation to engage processors who are registered with the Office.

Data Sharing

Sharing personal data within the public sector, including with NGOs and donor organisations, must comply with the Act and Regulation 21 of the Data Protection (General) Regulations, 2021 which outlines the framework for data sharing. An entity may share personal data upon request by another controller, processor, third party, or data subject. The sharing must 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. Clear information about data sharing practices must be provided, and strict access and security controls should

protect shared data. Data controllers and processors must determine the purpose and means of sharing personal data and enter into agreements prior to routine data sharing.

Data sharing arrangements should be regularly reviewed for compliance and risk management. Requests for sharing personal data must be in writing, specifying the purpose, retention duration, and safeguards against unlawful disclosure. Sharing within the organisational structures of a data controller or processor is not considered data sharing.

Data Localisation

Data localisation is the legislative or regulatory requirement to domicile specific data in Kenya or the jurisdiction in which the legal requirement is enacted. The Act requires that personal data prescribed by the Cabinet Secretary (ICT) as being of **strategic interest** must have a copy domiciled in Kenya. A data controller or data processor who processes such prescribed personal data for the purpose of strategic interest or special interest purpose of the state **must**:

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

A Strategic Interest purpose includes:

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

Data Transfer

Public Sector Institutions transferring personal data outside the country must ensure that the transfers comply with appropriate data protection safeguards, are a necessity, or are based on the explicit consent of the data subject. Where personal data is transferred to a third country or an international organisation, appropriate safeguards must be in place. These may include data protection legislation equivalent to Kenya's Data Protection Act or assessments made by the data controller that appropriate safeguards exist to protect the data. The public institutions also have the obligation to document the transfer and provide documentation to the Data Commissioner upon request. If the transfer is a necessity, it must be strictly necessary for purposes such as performing a contract or establishing a legal claim, and the data subject's fundamental rights and freedoms must not be overridden.

If there are no appropriate safeguards or necessities for the transfer, then the data subject must explicitly consent to the transfer and be informed of the possible risks. Sensitive personal data can only be transferred with the consent of the data subject, and a written agreement can be made between the transferring entity and the recipient with provisions for accessing a robust information system and identifying the countries and territories to which the personal data may be transferred.

EXAMPLE

Ministry X in Kenya has contracted service provider who stores data in a data centre located outside Kenya. While contracting, the ministry assesses the requirement of data localisation, security safeguard implemented by the service provider and ensures the transfer complies with the requirement under the Act before transferring personal data outside Kenya. In case there is sensitive personal data involved in the transfer, the ministry ensures obtaining consent from the data subject. In addition, the ministry must ensure that the contract outlines the requirement under regulation 24 of the data protection General Regulations.

Duty to Notify

One of the fundamental principles of data protection is transparency, which means that personal data collected by entities in the public sector must be processed in a fair and transparent manner. In accordance with Section 29 of the Act, data controllers and data processors are obligated to notify data subjects of their rights as outlined in the Act. They must also provide clear information about the purpose of data collection, disclose any third parties who may receive the data and the safeguards adopted, describe the technical and organisational measures implemented to ensure data security, and outline the consequences if data subjects fail to provide all or part of the requested data.

All the above information should be contained in a data protection policy, or privacy notices which should be made available to data subjects before or as soon as possible after the collection of their personal data. When drafting a privacy policy, it is important to use clear and plain language that is easily understandable, avoiding technical or legal jargon as much as possible. The policy should be comprehensive and include all relevant information that data subjects need to know about the processing of their personal data, including their rights, the purpose of data collection, third-party recipients, and safeguards in place. The policy should also be accessible to data subjects, for example, by providing it on the entity's platform or upon request.
Regular review and updates of the policy are necessary to ensure that it reflects any changes in data processing practices or relevant laws and regulations. To ensure that privacy policies are comprehensible for data subjects without discrimination, entities can utilise various methods, such as incorporating visual aids like illustrative elements and visual representations, implementing a question-and-answer structure, and dividing the policy into shorter sections with distinct headings. Additionally, giving practical examples of how personal data might be utilised can assist data subjects in comprehending the policy and understanding the consequences of sharing their personal information.

Appointment of a Data Protection Officer

A data controller or data processor may designate or appoint a data protection officer (DPO) in accordance with section 24(1) of the Data Protection Act. The DPO plays a crucial role in ensuring compliance with data protection regulations within the organisation. The designation of a DPO demonstrates an entity's commitment to safeguarding personal data and upholding data protection principles. DPOs assist in monitoring internal compliance, offering advice on

data protection obligations, and providing advice regarding Data Protection Impact Assessments (DPIA).

Example 1

Public agency appoints a data protection officer in compliance with the requirement of the section 24 of the Act. The agency published the contact details of the data protection officer on the website (eg DPO@Agency.go.ke) and communicated those details to the Data Commissioner. The DPO is provided with relevant resources required to undertake compliance mandate. To ensure this, the DPO has direct access to the director to raise any data protection concerns within the entity.

Example 2

Kangethe an employee and Boresha Ltd raised the issue on the potential conflict that would arise with his appointment as a Data Protection Officer and his position as a legal officer. He opted to take up the role as a data protection Officer.

Example 3

Boresha Authority of Kenya wishes to comply with data protection Act on the aspect of appointing a data protection Officer. However, the staff establishment doesn't allow for the position of a Data Protection Officer. Therefore, they appoint a committee instead to assist with data protection compliance with the relevant data protection regulations, develops policies, manages risks, coordinates responses to data breaches.

ANNEX 1: COMPLIANCE CHECKLIST

Questions	Yes	No	Comments/ Remedial Action
General Compliance			
We respect the right to privacy as a fundamental human right as provided by Article 31(c) and (d) of the Constitution.			
We have identified an appropriate legal basis for our processing under Section 30 of the Data Protection Act (DPA).			
If we are processing sensitive data, we have identified permitted grounds under section 44 of the DPA			
We grant the highest degree of autonomy possible with respect to control over their personal data.			
We restrict processing where the legal basis or legitimate interests cease to apply.			
We do not do anything generally unlawful with personal data or inconsistent purpose for processing.			
If we are subject to mandatory registration, we have submitted accurate and up-to-date information concerning our processing activities to the Office of Data Protection Commissioner (ODPC).			
We have considered how the processing may affect the individuals concerned and can justify any adverse impact.			
We only handle data about individuals in ways they would reasonably expect, or we can clearly explain why any unexpected processing is justified			
We do not allow any discrimination or exploitation of the needs or vulnerabilities of a data subject.			
We do not deceive or mislead people when we collect their personal data.			
We have clearly identified our purpose or purposes for processing and have clearly documented those purposes.			
We include details of our purposes in our privacy notices.			

We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitations.			
If we plan to use personal data for a new purpose, we check that this is compatible with our original purpose, or we obtain specific consent for the new purpose.			
We use technical measures to limit the possibility of repurposing personal data.			
We only collect personal data that is adequate, relevant, and limited to what is necessary for our specified purposes.			
We can demonstrate the relevance of the data to the processing in question.			
We periodically review the data we hold and delete anything we don't need.			
We avoid the creation of more copies or entry points for data collection than is necessary.			
We ensure that it is not possible to re-identify anonymised data or recover deleted data and test whether this is possible.			
We ensure the accuracy of any personal data we process and the reliability of our sources.			
We have appropriate processes in place to check and verify the accuracy of the data we collect, and we record the source of that data.			
We carry out tests for accuracy at critical steps.			
We use technological and organisational design features to decrease inaccuracy and mitigate the effect of an accumulated error in the processing chain.			
We have a process in place to identify when we need to keep the data updated to fulfill our purpose properly, and we update it as necessary.			
If we need to keep a record of a mistake, we clearly identify it as a mistake.			
We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.			

As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.			
We know what personal data we hold and why we need it.			
We carefully consider and can justify how long we keep personal data.			
We have a policy with standard retention periods where possible.			
We regularly review our records with a view of identifying personal data that no longer requires to be retained and delete or anonymise such data.			
We have appropriate processes in place to comply with individuals' requests for rectification and/or erasure of false or misleading data about them.			
We identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.			
We do not transfer data outside Kenya unless there is proof of adequate data protection safeguards or valid consent from the data subject.			
We checked and fulfilled all conditions set under part VI of the DPA and Regulations 2021.			
We have clearly identified our purpose or purposes for processing.			
We have documented those purposes.			
We include details of our purposes in our privacy notices.			
If one of the purposes is direct marketing, we make sure that the data subject is notified that direct marketing is one of the purposes for which personal data is collected or consented to the use of this/her data for the purpose of direct marketing and in any case, is provided with a simplified opt-out mechanism.			

We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitations.			
If we plan to use personal data for a new purpose, we check that this is compatible with our original purpose, or we obtain specific consent for the new purpose.			
We use technical measures to limit the possibility of repurposing personal data.			
Processing personal data based on consent			
Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of a statement or a clear affirmative action			
Are procedures in place to demonstrate that an individual has consented to their data being processed?			
Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data?			
Processing children's personal data			
Are procedures in place to verify the age of a child?			
Have you obtained consent from a parent/ legal guardian?			
Processing personal data based on legitimate interest			
If legitimate interest is a legal basis on which personal data is processed, has an appropriate analysis been carried out to ensure that the use of this legal basis is appropriate?			
Does the analysis must demonstrate that: • there is a valid legitimate interest, • the data processing is strictly necessary in pursuit of the legitimate interest, and • the processing is not prejudicial to or overridden by the rights of the individual			
Data Subjects Rights			

Is there a documented policy/procedure for handling Data Subject Access Requests?			
Is your organisation able to respond to Data Subject Access requests within 14 days?			
Are procedures in place to provide individuals with their personal data in a structured format, including a machine-readable format?			
Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable)?			
Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing?			
Are individuals told about their right to object to certain types of processing such as direct marketing?			
Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing?			
If automated decision-making, which has a legal or significant similar effect for an individual, is based on consent, has explicit consent been collected?			
Where an automated decision is made which is necessary for entering into, or performance of, a contract, or based on the explicit consent of an individual, are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision?			
Accuracy and Retention			
Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the necessary changes are made without delay?			
Are retention policies and procedures in place to ensure data are held for no longer than is necessary for the purposes for which they were collected?			

Do you have procedures in place to ensure data are destroyed securely, in accordance with your retention policies?			
Transparency Requirements			
Are individuals fully informed of how you use their data in a concise, transparent, intelligible, and easily accessible form, using clear and plain language?			
Where personal data are collected directly from the individuals, are procedures in place to ensure you have complied with your duty to notify?			
If personal data are not collected from the subject but from a third party (e.g. shared due to legal obligation) are procedures in place to provide a data protection policy to the individuals?			
When engaging with individuals, such as when providing a service or CCTV monitoring, are procedures in place to proactively inform individuals of their data protection rights?			
Is the information on how the organisation facilitates individuals exercising their data protection rights published in an easily accessible and readable format?			
Data Processor Agreements			
We have agreements with data processors (such as suppliers and other third parties) processing personal data on your behalf been reviewed to ensure all appropriate data protection requirements are included.			
Data Protection Impact Assessments (DPIAs)			
If your data processing is considered high risk, do you have a process for identifying the need for, and conducting of, DPIAs? Are these procedures documented?			
Appropriate technical and organisational security measures			
Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?			
Is there a documented process for resolving security related complaints and issues that specifies the technical, administrative, and physical safeguards for personal data?			

Is there a designated individual who is responsible for preventing and investigating security breaches?			
Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?			
Are personal data systematically destroyed, erased, or anonymised when they are no longer legally required to be retained.			
Can access to personal data be restored in a timely manner in the event of a physical or technical incident?			
Data Breach Response Obligations			
Does the organisation have a documented privacy and security incident response plan?			
Are there procedures in place to notify the Office of the Data Protection Commissioner of a data breach?			
Are there procedures in place to notify data subjects of a data breach?			
Are the plans and procedures regularly reviewed?			
Are all data breaches fully documented?			
Are there cooperation procedures in place between data controllers, data processors, and other partners to deal with data breaches?			
Compliance Reporting			
Is there compliance assessment carried out to ensure compliance with the data protection Act and its attendant Regulations?			
The organisation prepares compliance report regularly and undertakes to address any non-compliance finding			
The organisation considers submitting compliance report to the Data Commissioner			