OFFICE OF THE DATA PROTECTION COMMISSIONER

GUIDANCE NOTES ON DATA PROTECTION POLICY

Table of Contents

Definition.

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

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

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

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

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

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

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

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

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

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

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

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

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

"Privacy Notice (or Privacy Statement)" is an *outward-facing* document intended for data subjects/users generally. It explains how an organisation processes personal data (e.g. collects,

uses, stores etc), in compliance the duty to notify under Section 29 of the Data Protection Act, 2019.

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

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

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

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

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

1. Introduction

Regulations 23 of the Data Protection (General Regulations), 2021 provides that a data controller or data processor (data handlers) shall develop, publish and regularly update a data protection policy reflecting their personal data handling practices.

The Data Protection Policy is the internal governance document designed for use within the organization to guide and inform employees, management and internal stakeholders about the organisations' data handling practices fostering accountability and a culture of privacy within the organisation.

The guidance note outlines the essential elements of a data protection policy, offering step-by-step instructions and best practices for compliance. It assists institutions in understanding their responsibilities and provides practical guidance on how to communicate their data-handling practices to employees, customers, and other stakeholders.

By following this guidance, institutions can develop data protection policies that reflect their commitment to data protection, minimize data privacy risks, and ensure they meet the regulatory requirements set forth in the Act. The guidance note is applicable across all sectors irrespective of the size or establishment of the organization.

2. Obligations of the Office

The Office will periodically audit data controllers or data processors' processes and systems to ensure compliance with the Act and its Regulations.

Audit will include a review of the data protection policy to confirm that the organization's data protection governance aligns with the Act and Regulations requirements and is fully implemented.

To fulfil its oversight function, the Office does not draft or develop policies for or on behalf of any institution.

3. Legislative framework

i. **The Constitution of Kenya** - **Article 31 (c) and (d)** guarantee the right to privacy regarding to information relating to their family or private affairs unnecessarily required or revealed, or that of their communication infringed. **Article 35** states that every citizen has the right to access information the State holds and information another person holds necessary to exercise or protect any right or fundamental freedom.

ii. **The Data Protection Act, 2019** - Establishes the Office of the Data Protection Commissioner and provides various frameworks that guide the processing of personal data in Kenya. The attendant regulations to the Data Protection Act, 2019 include the *Data Protection (General) Regulations 2021, Data Protection (Complaints and Enforcement) Regulations 2021 and Data*

Protection (registration of Data Controllers and Data Processors) Regulations 2021. These Regulations outline how personal data should be handled in Kenya.

iii. **The Computer Misuse and Cyber Crime Act,2018** - This Act provides for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation, and prosecution of computer and cybercrimes; to facilitate international cooperation in dealing with computer and cybercrime matters, and for connected purposes.

4. Institutional Data Protection Policy

A data protection policy should include:

i. Principles of data protection;
ii. Lawful basis of processing personal data;
iii. Personal data management;
iv. Roles and responsibilities for data management;
v. Data subject rights management;
vi. Measures for protection of personal data;
vii. Data breach management;
viii. Vendor management;
ix. Commercial use of personal/sensitive personal data
x. Data sharing
xi. Data transfer
xii. The vulnerable group/Exercise of rights by others
xiii. Training and awareness;
xiv. Data protection impact assessments and audits; and
xv. Policy implementation monitoring.

The above domain areas can be regarded as minimum requirements which can be supplemented by additional provisions in the development of a data protection policy. Organisations should customize the development of the policy to cover its data protection needs.

4.1. Principles of Data Protection

The Act provides for core principles guiding processing of personal data by data handlers and as such the data protection policy should reflect adherence to:

- **Lawfulness, fairness, and transparency**: Personal data must be processed in a lawful, fair, and transparent manner, with clear communication to data subjects about how their data is being used.
- **Purpose limitation**: Personal data should only be collected for specific, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes.
- **Data minimization**: The collection of personal data should be limited to what is necessary for the intended purpose. Data collection should not be excessive.
- **Accuracy**: Personal data must be accurate and~~, where necessary,~~ kept up to date.
- **Storage limitation:** Personal data should not be stored for longer than necessary for the intended purpose.
- **Integrity and confidentiality**: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.
- **Accountability**: Data controllers must be able to demonstrate compliance with the principles, including having appropriate policies and procedures in place to hold processors and third parties accountable.

4.2 Lawful basis for Data Processing

A data protection policy should specify the lawful bases relied upon in processing personal data by the institution. An institution can only rely on one lawful basis per processing activity at a time which shall be established before the processing.

The lawful bases include:

Lawful basis	Description	Mechanism to exercise

Consent	It is the manifestation of an express indication of the data subjects' agreement to the processing of their personal data. When relying on consent as a lawful basis, an institution should ensure it obtains valid consent which should be specific, informed, and freely given. A data subject shall have the right to withdraw consent to the processing of their personal data at any time.	In order to rely on Consent as a lawful basis, data controllers and data processor should develop and implement a Data Protection Policy which speaks on Consent. In addition to that, have Data Subjects Right Requests (DSR) Forms tied to a particular processing activity. The Consent and DSR forms should be in simple, plain language for easy understanding by data subjects. DSRs are to be used when a data subject wishes to exercise their rights, including withdrawing consent. It is important to note that oral consent should be put in writing.
Compliance with a legal obligation	To rely on legal obligation as a lawful basis for processing personal information, an institution shall demonstrate that the processing is necessary for compliance with a legal obligation to which they are subject.	Data controllers and data processors can demonstrate reliance on this lawful basis by documenting, in their data protection policy, the specific basis relied upon for each processing activity tied to the relevant legal provision. Where multiple lawful basis apply to a single activity, the entity must specify the circumstances under which each basis (or if multiple legal obligation, each individual legal obligation) governs each processing detail.

Performance of a contract	This lawful basis applies where a contract exists between the controller/processor and the data subject. The contract must explicitly agree to the processing of the data subject's personal data for a defined purpose and duration. Processing is then lawful to enable the institution to fulfil its contractual obligations.	It allows data controllers and data processors to process personal data needed to execute contractual obligations to a data subject, or pre-contractual steps. Demonstration on how this lawful basis can be relied upon when executing either a written or unwritten contract should as well be captured in the organisation's data protection policy.
Vital interest of a data subject	Vital interest applies to processing personal data where it is strictly necessary to protect a data subject's life or physical safety. May be applicable in emergencies where the data subject cannot give consent or consciously rely on the other lawful bases.	May be applicable where processing personal data is necessary to protect someone's life or well-being, particularly in emergencies where the data subject is incapable or may not be rely on the other lawful bases.
Public interest	This applies where the processing of personal data 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.	Aimed at balancing individual privacy with societal needs. The public interest test must be satisfied to apply. Not a blanket rule to infringe/violate individual's privacy rights. The data protection policy must clearly show under what circumstances this lawful basis can be relied upon, taking into account its very limited applicability.

Public authority	Applies where the processing of personal data is necessary for the performance of any task carried out by a public authority.	Public authority is exercised when processing is necessary for a task exercised by an official authority vested in the data controller or data processor, usually by a legal instrument. Public bodies must still comply with principles of data protection, such as lawfulness, fairness, accountability, data security, and data minimisation as they process personal data; organisations therefore need to have a data protection policy as a guiding tool when performing any tasks as a public authority.
Legitimate interest	Legitimate interest can be a lawful basis for processing personal data if in the processing of personal data, the institution's interests do not override the data subject's rights and freedoms. Where an institution relies on legitimate interest as the legal basis for processing personal data, it must conduct a Legitimate Interest Assessment (LIA) to ensure the processing is justified, necessary, and balanced against the rights and freedoms of data subjects.	Legitimate interest can be relied upon by organisations to process personal data if it is necessary for their interests, provided it does not override the fundamental rights and freedoms of the data subject. It requires a balanced approach, balancing the controller's goals against the individual's rights, and is commonly used for fraud prevention, network security among many other processing activities as captured in the

		organisation's data protection policy.
Historical, statistical, journalistic, literary, artistic, or scientific research	An institution may rely on this lawful basis where the processing of personal data is necessary for historical, statistical, journalistic, literary, artistic, or scientific research purposes. When relying on this basis, the institution should ensure that appropriate safeguards are in place to protect the rights and freedoms of data subjects, such as data anonymization or limiting the use of personal data only to the historical, statistical, journalistic, literature and art or scientific research purpose.	This lawful basis provides data controllers and data processors a legal basis for processing personal data for the named purposes without sourcing any other lawful basis. These activities are generally considered compatible with the original purpose of data collection, provided appropriate safeguards are implemented. Where this is the lawful basis, it should be well documented in the Policy, ensure the minimum requirements provided by the Act are in place.

4.3. Roles and Responsibilities of stakeholders

The data privacy policy should define the roles of stakeholders involved in data processing including but not limited to data controllers, data processors, data protection officer, data protection committee, and specific department(s). Key roles and their responsibilities may include:

4.3.1. Data Controllers

Determine the purposes and means of processing personal data.

Responsibilities may include:

- Ensure data processing is lawful, fair, and transparent.
- Collect and process only the data necessary for the specified purposes.
- Keep data accurate and up to date.

- Store data only for as long as necessary.
- Implement appropriate security measures to protect data.
- Uphold the rights of individuals, including the right to access, rectify, and erase their data.
- Notify the Data Commissioner of any data breaches within 72 hours.
- Develop data processing agreements when engaging data processors and third parties.

4.3.2. Data Processors

Process personal data on behalf of the data controller.

Responsibilities may include:

- Act only on the instructions of the data controller.
- Implement appropriate technical and organisational measures to protect data.
- Assist the data controller in meeting their data protection obligations.
- Ensure all personnel handling data are subject to confidentiality.
- Assist the data controller in ensuring compliance with data subject rights.
- Notify the data controller of any data breaches within 48 hours.

4.3.3. Data Protection Officer (DPO)/ Data Protection Committee

Serves as a focal person in ensuring compliance with the Act and attendant regulations in proper processing of personal data.

Responsibilities may include:

- Inform and advise the institution and employees about their obligations under data protection laws.
- Monitor compliance with data protection laws and internal policies.
- Provide advice regarding Data Protection Impact Assessments (DPIAs).
- Cooperate with the Office and act as a contact point.
- Facilitate capacity building of staff involved in data processing operations.
- Conduct internal audits and reports on data protection activities within the institution.

4.3.4 Employees

Responsibilities:

i. Comply with the institutional Data Privacy Policy
ii. Demonstrate understanding of their obligations in the processing of personal data
iii. Ensure personal data is kept securely in accordance with institutional information security policy;
iv. Maintain confidentiality and integrity in processing personal data.
v. Collaborate with stakeholders in compliance with the policy.

4.3.5 Senior Management/Board Management.

Offer strategic and operational leadership in ensuring effective implementation of the institutional data protection policy**.**

Responsibilities may include:

- Oversee the overall management of the institutional data privacy program.
- Approval and review of the institutional data protection policy
- Resource allocation for effective implementation of the data privacy program
- Ensure independence of the Office of the Data Protection Officer, including having adequate resources to operationalize the data protection obligations of the controller/processor.
- Develop and maintain a data privacy risk management strategy that aligns with the overall business strategy.
- Oversee audits and reviews to ensure the effectiveness of data privacy programs.
- Ensure that staff receive appropriate training and understand their responsibilities regarding Data Privacy risks.

4.4 Data Subject Rights Management / Rights of a Data Subject

The Act provides certain rights and fundamental freedoms to individuals in relation to their personal data. The data protection policy should outline how the following rights will be exercised:

Right	Description	Mechanism to exercise	Absolute/ Conditional	Timeline

Right to be Informed	Transparent information on processing (purpose, legal basis, recipients, retention, rights) at, before & post collection (entire data cycle).	Privacy notices, consent forms, just-in-time notices	Absolute	Before, at and post collection (entire data cycle)
Right of Access	Obtain confirmation of processing and access to personal data and related information.	Formal request (email, portal), identity verification	Absolute	7 days
Right to Rectification	Correction of inaccurate or incomplete personal data.	Formal request with supporting evidence	Conditional on provision of evidence	14 days
Right to Erasure	Erase where data is no longer necessary, consent withdrawn, or unlawful processing.	Formal erasure request	Conditional	Within 14 days
Right to Restriction	Limit processing while issues (accuracy/lawfulness) are resolved.	Formal request specifying grounds	Conditional *(Absolute for direct marketing)*	Within 14 days
Right to Data Portability	Receive data in structured, machine-readable format and transfer to another controller.	Request specifying format/recipient	Conditional	Within 30 days
Right to Object	Object to processing based on violation of lawful basis, data protection principle(s) etc or direct marketing.	Opt-out/unsubscribe or formal objection	Conditional *(Absolute for direct marketing)*	7 days for marketing; other instances: within 14 days

Automated Decision-Making	Not to be subject to decisions based solely on automated processing with significant effects.	Request human review/intervention	Conditional	Promptly upon request

4.5 Complaints Handling Mechanisms

The data protection policy should include an internal complaint handling procedure addressing complaints by data subjects regarding their personal data. The data protection complaints handling procedure should handle complaints based on the processing of personal data by the data controller or processor.

The complaints handling procedure should also address complaints made by third parties in relation to the data controllers or processors' use of personal data.

The policy should inform that a data subject who is dissatisfied with the outcome of an internal complaint handling may escalate the matter by lodging a complaint with the Data Commissioner. The policy should also prescribe a centralized log to keep track of all complaints, including date, type of complaint, and actions taken.

4.6. Measures for the protection of personal data.

The data protection policy should detail the technical and organisational measures designed to safeguard and ensure protection of personal data.

The policy should also detail elements necessary to implement a robust data security including;

a) Having an operative means of managing policies and procedures for information security;
b) Assessing the risks against the security of personal data and putting in place measures to counter identified risks;
c) Processing that is robust to withstand changes, regulatory demands, incidents, and cyber-attacks;
d) Ensuring only authorised personnel have access to the data necessary for their processing tasks;
e) Secure data sharing and transfers against unauthorised access and changes;

f) Secure data management;
g) Regular backups and disaster recovery procedures to ensure availability of personal data;
h) Monitoring and logging of access to personal data to detect and respond to security incidents;
i) Protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data;
j) Routine measures and procedures to detect, handle, report, and learn from data breaches; and
k) Regular review and testing of software to uncover vulnerabilities of the systems supporting the processing.

Furthermore, the data protection policy should also outline record-keeping requirements, such as documenting the lawful bases for processing personal data, data subject consent, and data protection impact assessments.

4.7 Data Protection Impact Assessment (DPIA)

Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, an institution shall, prior to the processing, carry out a data protection impact assessment.

The data protection policy should detail a description of the envisaged processing operations that are considered high risk, the purposes and the need to conduct a DPIA for processing activities considered to have high risk to the rights and freedoms of data subject.

The DPIA should originate from the user department, where applicable, to allow for a comprehensive outline of what's required, the privacy concerns and mitigations measures without compromising the necessity of the project.

The Office has published a Guidance Note on Data Protection Impact Assessments on www.odpc.go.ke The Guidance Note includes the form in which a Data Protection Impact Assessment should be submitted.

4.8 Data Breach Management.

A data breach occurs when personal data is accessed, acquired, or exposed by an unauthorised person, potentially leading to harm to the affected data subjects. Such harm may include identity theft, financial loss, reputational damage, or emotional distress.

An effective Data Protection Policy should clearly outline the procedures to be followed in the event of a data breach. This can be effected through the Incidence Response Procedure. These procedures should enable the institution to promptly detect potential breaches through appropriate monitoring and reporting mechanisms, contain the breach to prevent further exposure or escalation, assess its nature, scope, and impact, and notify all relevant parties, including the Data Commissioner and, where applicable, the affected data subjects.

Where sensitive personal data is compromised, the institution is obligated to notify the Office of the Data Protection Commissioner (ODPC) without undue delay. Where there is a significant risk to the rights and freedoms of individuals, the institution must also inform the affected data subjects to enable them to take appropriate protective measures.

The data protection policy should clearly outline procedures on each of the following when a breach occurs:

4.8.1 Obligation to Notify the Data Commissioner

When a data breach occurs, the data controller is required to notify the Data Commissioner without undue delay and within 72 hours of becoming aware of the breach. The notification must include:

- A description of the nature of the breach;
- The personal data involved and the extent of the breach;
- The potential consequences of the breach;
- The measures the data controller has taken or intends to take to address the breach; and prevent further incidents.

Delayed Notification: If notification to the Data Commissioner cannot be made within 72 hours, the data controller must provide reasons for the delay. This should accompany the breach notification and detail the circumstances causing the delay.

4.8.2 Notification from Data Processors to Data Controllers

In accordance with Regulation 38(2) of the Data Protection (General) Regulations, 2021, where a data processor becomes aware of a personal data breach, it is their responsibility to notify the data controller without undue delay, and, within 48 hours of becoming aware of the breach.

This obligation is critical to ensure that the data controller can meet their statutory requirement to notify the Office of the Data Protection Commissioner (ODPC) within 72 hours, as stipulated under Section 43 of the Act,

4.8.3 Communicating the Breach to Data Subjects

Once a breach has been identified and reported to the Data Commissioner, the data controller also communicates the breach to the affected data subjects. This communication should be done within a reasonable period and must allow the data subjects to take protective action.

The communication should include:

- A description of the nature of the breach;
- Steps taken or to be taken by the data controller to address and mitigate the breach;
- Recommendations for the data subject to minimize the impact of the breach (e.g., changing passwords, monitoring accounts);
- Where applicable, the identity of the unauthorized person who accessed or acquired the personal data; and
- Contact information from the Data Protection Officer or another point of contact for further inquiries.

4.8.4 Circumstances for Delaying or Restricting Communication

A data controller may delay or limit communication to affected data subjects if it is deemed necessary and proportionate for the prevention, detection, or investigation of an offense by relevant authorities. This must be carefully assessed, and such delays must not unnecessarily endanger the data subjects' ability to protect themselves. The policy must clearly address the requirements and limitations allowed (only as per the Act).

4.8.5 Exemptions from Communicating to Data Subjects

Communication to data subjects is not required if the data controller or processor has implemented appropriate security safeguards such as encryption that ensure the data breach is unlikely to result in harm to the data subjects.

4.8.6 Providing Additional Information in Phases

If all relevant information cannot be provided at the time of the initial notification, the data controller may provide the information in phases, provided this is done without undue delay. The phased communication must still prioritize giving the data subject sufficient information to take immediate protective measures.

4.8.7 Record Keeping and Documentation

The data controller must keep detailed records of all data breaches, including the following:

- The facts surrounding the breach, including how it was discovered, its scale, and the affected data;
- The effects or consequences of the breach, including any harm caused to individuals; and
- The remedial actions taken to address and contain the breach, as well as measures implemented to prevent future occurrences.

These records must be maintained securely and made available to the Data Commissioner upon request.

4.8.8 Ensuring Compliance

Breach detection, notification, and response procedures is crucial to maintaining a strong data protection culture within the organisation.

4.9 Data Management

4.9.1 Data life cycle

Data handlers are required to maintain detailed records of processing activities, demonstrating how personal data is managed and processed, ensuring compliance with the Act and the Regulations at each stage of the lifecycle.

A data protection policy should provide details on data life cycle management; a clear approach to managing personal data throughout its entire lifecycle, covering collection, storage, lawful basis relied upon, use, sharing, transfer, archiving, and disposal. Data controllers and processors should perform thorough data mapping to identify optimal processing activities.

4.9.2 Records of processing Activities/Data map

To manage data through its life cycle, data handlers should conduct comprehensive data mapping and develop a Data Map or simply a Record of Processing Activities (RoPA). A Data Map/RoPA is an essential aspect of data management that helps data handlers to maintain a detailed account of how personal data is processed within the organisation.

RoPA/ Data Map should include;

1. Contact Information on the data controller or the data processor;
2. Purposes of Processing: A clear description of why personal data is being processed;
3. Classes of Personal data processed;
4. Categories of personal data/groups of individuals whose data is being processed (e.g., customers, employees);
5. Details on any transfers of personal data to other countries or international organisations, including safeguards in place when transferring personal data to third-party service providers or to entities located outside Kenya. Such transfers must be documented and carried out in accordance with the Act. Transfers to third parties are permitted only where a valid legal basis exists, and appropriate safeguards - such as contractual agreements and security measures are in place;
6. The duration for which the personal data will be retained, or the criteria used to determine this period;
7. An overview of the technical and organisational measures in place to protect personal data;
8. The justification for processing personal data under relevant data protection laws;
9. A summary of how data is collected, used, stored, and deleted; and
10. Lawful basis for each processing activity undertaken by the organisation.

Maintaining accurate and comprehensive RoPA is crucial for compliance and can help demonstrate accountability in data processing activities.

4.10 Data retention & disposal schedule

To implement the storage limitation principle, data handlers are required to develop data retention and disposal schedules as guided under Section 39(1) of the Act and Regulation 19 and 35 of the General Regulation. The Act and the Regulations state that data controllers and processors may retain personal data only for as long as it is reasonably necessary to achieve the purpose for which it was collected. Section 39(2) further mandates that once the retention period has ended, the data controller or processor must delete, erase, anonymize, or pseudonymize any personal data that is no longer required, in accordance with established guidelines. To ensure compliance, Regulation 19 and 35 outlines specific instructions for data controllers and processors to implement a personal data retention schedule, including, but not limited to, specifying retention durations for all personal data and ensuring its complete deletion or anonymization after the expiration of the designated retention periods.

Regulation 23(2)(f) of the General Regulations outlines that data retention schedule may be part of the data protection policy. Where the data retention and disposal schedules are not part of the Policy, the data handler should refer to the relevant policies and procedures that guide data retention in the institution.

Record Category	**Type of Data**	**Retention Period**	**Purpose of processing**	**Lawful basis of processing**	**Disposal Method**	**Responsible Office**
Tenant Application Files	Application forms, ID copies, references	6 years after decision	Dispute resolution, fraud prevention	Performance of a contact	Shredding / secure deletion	Letting Office / Compliance
Employee HR Files	Contracts, performance, payroll	7 years after exit	Labour & tax law	Legal obligation	Shredding / secure deletion	HR
CCTV Footage	Surveillance footage	30 days	Security	Legitimate interest	Auto-overwrite	Security

4.11 Vendor Management.

Data protection policy should outline mechanisms of ensuring that all third-party relationships comply with the Data Protection Act, 2019 and the Data Protection (General) Regulations, 2021. Where a data controller or processor outsources processing activities, appropriate due diligence, contractual safeguards, and oversight mechanisms must be established to guarantee secure and lawful handling of personal data.

The Policy should indicate that where a data controller engages in the services of a data processor, this engagement should be done through a written Data Processing Agreement between data controller and processors as per Regulation 24 of the General Regulations. In addition, the Policy should indicate that where a data processor engages the services of a third-party, the engagement should be done with prior authorization by the data controller, and the engagement should be done through a written contract as outlined in Regulation 25 of the General regulations.

Entities should maintain an updated vendor register, documenting all processors, sub-processors, and the nature of data they handle. Regular reviews and compliance confirmations should be part of the institutional risk management framework.

4.12 Commercial Use of Personal/Sensitive Personal Data

Data protection policy should outline clear prohibition on use of personal and/or sensitive personal data for commercial purposes. In the event the institutional policy allows specific circumstances where personal data may be use for commercial purposes, the circumstances must be clearly stated; which must only be on either one or both requirements below:

a. The express and unequivocal consent of the data subject was obtained prior to the processing; or
b. The commercial use is authorized under any written law, and the data subject has been informed of such when collecting the data from the data subject.

The policy should call for use of anonymization techniques, where possible to ensure the data subject is no longer identifiable, where the use for commercial purposes is mandated by law.

4.13 Data Sharing

Data sharing is the exchange of personal data between two or more controllers or joint controllers or third parties within the country. Regulation 21 of the General Regulation requires that data sharing must always be through a legally binding documents (a data sharing agreement) that regulates how personal data is shared between the named persons.

The data protection policy must clearly specify how data handlers engage with other third parties, controllers, and joint controllers in accordance with Regulations 21 (General Regulations) provisions.

4.14 Data Transfer

The data protection policy must satisfy the provision of Section 48 and 49 of the Act regarding transfers of personal data to another country.

It must specify the requirement for proof of appropriate safeguards ensuring the security and protection of the personal data before any transfers, including jurisdictions with commensurate data protection laws.

The transfer must be of necessity. For sensitive personal data, the controller or processer must additionally obtain the data subjects' express and unequivocal consent prior to transfer, alongside all other abovementioned safeguards.

The proof of safeguard, necessity, and consent to be communicated to the Data Commissioner before the transfer.

4.15 The Vulnerable Group/Exercise of Rights by Others

A data protection policy should emphasize inclusive practices, including the vulnerable groups like the minors, persons with disabilities, the elderly, low-literacy communities, the minorities and the marginalized. This ensures processing upholds fairness, transparency and non-discrimination with special safeguards for the vulnerable to mitigate risks like bias or exploitation.

For processing the vulnerable groups, the Act requires prioritizing accessibility in notices, explicit consent and conduct of DPIA assessing impacts and the privacy risks for the vulnerable groups. Provide how rights on the vulnerable data subjects group will be exercised and ensure the imbalances have been addressed.

Practical example may be: Institutions providing mechanisms how parents and guardian can exercise rights on behalf of minors; how the mentally incapacitated, low literacy, disabled

(incapacitated) in other ways are allowed to exercise rights just like other data subjects, in line with principle of fairness; mitigate biases, imbalances and inequities.

4.16 Training and Awareness

The data protection policy should outline measures in place to promote compliance with the Act and the Regulations. The policy should guide on how the institution should implement robust training and awareness programs on data protection to ensure that employees, contractors, and other relevant parties understand their responsibilities regarding personal data handling, breach-management and confidentiality.

The data protection policy should indicate how an institution can develop and implement a well-structured training program that enhances the organisation's ability to protect personal data and minimizes the risk of data breaches. The policy should guide documentation of all training activities and assessment results to maintain records of compliance with training requirements under the Act.

4.17 Data Protection Policy Review

Periodic reviews are vital parts of a strong data protection policy as it guides the frequency of data protection reviews and checks to align with changes in laws, regulations and circumstances/activities of the organization.

This involves checking current policies against legal requirements, gathering feedback from staff and stakeholders, and spotting any gaps or areas that need improvement. The data protection policy should clearly outline the review process, including documentation of reports and implementation of recommendations. The review period may be within 3-5 years or on a need basis which cannot go beyond 3-5 years.

4.18 Implementation and Enforcement of Data Protection Policy

The Data Privacy Policy should be communicated to all employees, including new hires, during their onboarding process. This ensures that every staff member is fully informed of their responsibilities regarding data protection from the outset. Integrating the policy into the staff

handbook and providing it as part of the induction program ensures that new employees understand its importance and how it applies to their daily tasks. Continuous training and updates should also be provided to all employees to keep them informed of any changes to the policy.

Key third parties, like data processors and service providers, should also be informed to ensure they comply with the organisation's data protection standards. In case of policy violations, clear disciplinary actions should be outlined.

4.19 Monitoring and Evaluation

As part of the organizations' data protection management framework, compliance with the Data Protection Policy should be continuously monitored and evaluated.

a) Frequency of Internal Audit

- Internal data protection compliance audits should be conducted at least every year.
- Where necessary, internal audits may be initiated in response to:
  - Data breaches or incidents
  - Significant changes in processing activities
  - Amendments to applicable laws or regulatory guidance

This will inform the need for timely review of the Data Protection Policy

b) Key Performance Indicators (KPIs) for Compliance

The following indicators should/may be used to assess compliance effectiveness:

- Data Subject Rights Compliance Rate: Percentage of requests (access, rectification, erasure, objection) responded to within statutory timelines
- Breach Response Time: Time taken to detect, report, and respond to personal data breaches (target: within 72 hours where applicable)
- Training and Awareness Coverage: Percentage of staff trained on data protection and privacy obligations annually
- Audit Findings Resolution Rate: Percentage of audit issues resolved within prescribed timelines

- Records of Processing Activities (ROPA) Accuracy: Completeness and periodic updating of data processing records
- Third-Party Compliance Rate: Percentage of data processors and partners with signed data protection agreements and due diligence completed
- Privacy by Design Implementation: Evidence of data protection impact assessments (DPIAs) conducted where required

c) Roles and Responsibilities in Compliance Monitoring, Audit and Review

- **Data Protection Officer (DPO)**
  - ♦ Prepare and consolidate compliance reports
  - ♦ Ensure implementation of corrective actions
  - ♦ Advise management on compliance risks and mitigation measures
- **Departmental Heads / Data Owners**
  - ♦ Ensure compliance within their respective units
  - ♦ Provide necessary documentation and responses during audits
  - ♦ Implement corrective actions within agreed timelines
- **ICT / Information Security Team**
  - ♦ Support monitoring through technical controls (e.g., access logs, security measures)
  - ♦ Report any vulnerabilities or incidents affecting personal data
- **Senior Management**
  - ♦ Review compliance reports submitted by the DPO
  - ♦ Provide oversight and approve necessary corrective or strategic actions
  - ♦ Allocate resources for compliance improvements

d) Reporting Structure

- Findings from monitoring and audits shall be documented and submitted quarterly to the DPO.

- The DPO shall prepare a consolidated compliance report annually, and where necessary, escalate critical issues to senior management and/or the Office of the Data Protection Commissioner in accordance with legal requirements.

5. Other Policies on Data Protection

5.1 Privacy Notice/Statement (Outward Facing Statement)

A privacy notice/statement communicates to data subjects how their personal data is collected, used, and protected. Transparency is a core requirement under Section 29 of the Data Protection Act

According to Section 29 of the Act, data controllers and data processors are obligated to notify data subjects of their rights specified in the Act, provide them with 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 security measures, and outline the consequences if data subjects fail to provide all or part of the requested data.

All this information should be contained in the privacy notice/statement (customer facing), 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 notice, it is important to use clear and plain language that is easy to understand, avoiding technical or legal jargon as much as possible. This policy should be comprehensive, covering 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 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, entities can utilize various methods to cater for the wide range of audiences. 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 utilized can assist data subjects in comprehending the policy and understanding the consequences of sharing their personal information.

5.2 Cookies Policy

A cookies policy ensures transparency regarding online data collection. Under Section 29 of the Act, data subjects have the right to be informed before their personal data is collected.

Data handlers must inform data subjects about the use of cookies when they visit their website, they must make sure that data subjects are provided with detailed information about the use of cookies on their websites.

5.2.1 Cookie Policy Requirements

It is imperative for the data controller or processor to have in place a cookie banner or pop-up displayed on their website to comply with the provisions set out in the data protection act.

Cookies policy should inform data subject:

1. Which information is being capturing about them,
2. How the organisation is handling, processing, storing and safeguarding the personal data,
3. What is the personal data used for,
4. The purpose for which personal data is collected,
5. The types of cookies i.e. Session Cookies, Persistent Cookies, First-party cookies or Third-Party Cookies,
6. Whether third parties are involved, and
7. How does the organisation seek to comply with data subject rights. The cookie policy should provide clear information on how individuals can manage their cookie settings and include instructions on how to opt out

5.2.2 ICT POLICY DISTINGUISHED FROM DATA PROTECTION POLICY

The ICT Policy aims to provide a framework for the safe and responsible use of organisations' technology and digital resources. It defines acceptable use of computers, networks, and software, sets standards for cybersecurity, outlines user responsibilities and access controls, and provides

procedures for monitoring, incident reporting, and password use/management within an organisation.

As a rule, therefore, data handlers must distinguish the ICT Policy and the Data Protection Policy as two distinct, separate and independent policy, addressing independent purposes, usage and compliance requirements. Whereas the former governs the use and management of an organizations' technology system and resources, the later governs responsible, legal and acceptable use of personal data as provided for in the Data Protection Laws and Regulations.