Data Protection Authority of Sri Lanka

Draft Guidelines on Data Protection Management Programme

This document provides the draft outline of the Data Protection Management Programme intended to be issued as guidelines by the Authority under section 12 (2) of the Personal Data Protection Act No.9 of 2022.

Contents

DPMP GUIDELINES WORKING DRAFT VERSION 1.0

1. Introduction

These Guidelines are made pursuant to Section 12(2) of the Personal Data Protection Act, No. 9 of 2022 (the Act). They describe how a controller should prepare and implement internal controls and procedures for the purpose of complying with its obligations under the Act. Such internal controls and procedures are referred to as a Data Protection Management Programme (DPMP).

All "controllers" under the Act are required to implement a DPMP.[1] Controllers comprise a broad range of entities and natural persons that determine the purposes and means of processing personal data to which the Act applies.

The Act establishes various obligations that apply to controllers when they collect, store, safeguard and otherwise process data about people, i.e., personal data of "data subjects."[2] The Act also gives data subjects rights that controllers must honour.

Coming into and maintaining compliance with obligations under the Act will require many controllers to make important changes to how they manage information, do business and interact with customers, employees and other people. To be effective and endure, these changes need to be built into their business processes.

Controllers often engage "processors" to process personal data on their behalf and processors often in turn engage sub-processors. Processors and sub-processors that are not controllers are not required to prepare a DPMP.[3] However, controllers remain responsible under the Act for how such processors and sub-processors treat the personal data. Controllers must consider and plan for how to ensure that all of their obligations described in sections 2 and 3 will be met in such processing. This includes ensuring that the necessary contractual obligations are in place, along with allocating responsibility and reporting.

In Section 2 of these Guidelines key obligations of a controller under the Act are summarized and Section 3 describes the internal controls and procedures that would enable a controller to comply with those obligations.

Disclaimer: These guidelines are only meant to provide a general guidance on DPMPs. Controllers are required to design their respective DPMPs on the basis of structure, scale, volume and sensitivity of processing activities of the controller and may use this guideline as a baseline.

[1] Section 12 of the Act provides, "It shall be the duty of every controller to implement internal controls and procedures, (hereinafter referred to as the "Data Protection Management Programme") […] for the purpose of complying with the obligations referred to in sections 5, 6, 7, 8, 9, 10 and 11."
[2] See section 6 of these Guidelines for the Act's definitions of "personal data" and "data subjects."
[3] The Act's definitions of "controller" and "processor" are set out in section 4.1 of these Guidelines. Under Section 2 of the Act, the Act applies to processing of personal data taking place in Sri Lanka or where the controller, the processing or the data subjects have certain links to Sri Lanka, as set out in more detail in that Section 2.

2. Summary of controllers' obligations

Note: This section summarises key obligations of controllers under the Act. Being a summary, it is not a complete description of the Act's provisions. Merely following this summary will not provide any assurance that a controller complies with the Act. Controllers must study the Act itself to understand their respective obligations and process personal data in accordance with the Act.

2.1. Process personal data in a lawful manner

Controllers must ensure that their processing of personal data is "lawful." The conditions that make processing lawful are set out in Section 5 and Schedules I to IV of the Act. These are summarized in section 4.2 of these Guidelines.

There are several conditions that can make processing lawful, such as where the data subject has consented, or the processing is necessary to enter into or perform a contract with the data subject or for the controller to comply with a legal obligation. Processing is also lawful to protect the address an emergency that poses a threat to someone's life, health or safety, or to carry out a task in the public interest or exercise of official authority. Various "legitimate interests" can also be a lawful basis for processing.

Some kinds of personal data are more sensitive than others. The Act has tighter controls for "special categories of personal data", such as data relating to an individual's race, ethnicity, political opinion, religious and philosophical belief, genetic data used for identification, health, sex life, sexual orientation, and personal data relating to a child.[4] Such data may be lawfully processed where the subject has consented to the processing, where the processing is necessary in connection with employment, social security, public health and related areas, emergency situations, where the data subject has made the data public already, where the data is necessary for legal claims or court proceedings, public interest, medical purposes, and public interest research and archiving.[5]

Whether the personal data being processed are within the "special categories" or not, controllers must analyse the kind of processing they are planning, and ensure that this is within one of the lawful bases. They should keep a record of this analysis and if the nature of the processing changes, check again that there is a lawful basis.

Where the lawful basis of the processing is that the data subject has consented, then controllers should establish procedures for dealing with their customers and other individuals that ensure that their consent is freely given, specific, informed and unambiguous.[6] Controllers should keep records to enable them to demonstrate that consent is valid, including the circumstances in which data subjects are giving consent, what information is provided to them in the process, how their consent

[4] Section 4.1 of these Guidelines sets out the full definition in the Act of "special categories of personal data."
[5] See section 4.2.2 of these Guidelines.
[6] See section 4.2.3 of these Guidelines for further information on the meaning of "consent."

is conveyed, and a record of the consent itself.

2.2. Define a purpose for the processing

Controllers must ensure that they collect and process personal data for specified, explicit, and legitimate purposes.[7] Controllers should analyse the purpose for which they need to process the personal data, and record that purpose.

Where a controller will process personal data for purposes beyond the initial purpose, they must not do so in a manner that is "incompatible" with the initial purposes. The Act provides a safe harbour for further processing of personal data where it is for archiving purposes in the public interest, scientific research, historical research or statistical purposes: these cases are not incompatible with the original purpose.[8] There may be other ways of further processing that would not be incompatible with the initial purpose of processing. Again, controllers should analyse such further processing with a view to its compatibility, and keep a record of their conclusions.

2.3. Limit processing to the defined purpose

Controllers must ensure that personal data processed is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.[9] This principle aims to reduce the risk of unnecessary data processing and the potential for data breaches.

Controllers should review the types and volumes of personal data collected and processed in light of the purpose of processing. Without compromising the adequacy of such data, they should ensure that only data that is relevant and necessary for the purpose is processed. They should keep a record of the purpose of the processing and an explanation of why such data are relevant and necessary for that purpose.

2.4. Ensure accuracy

Controllers must take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date. Data that are inaccurate or out of date should be corrected or deleted without delay.[10]

This require controllers to consider the nature of the personal data processed, and its likelihood of changing. While a person's name may be less likely to change, his or her address, employment, health condition and many other things may change with time. Where such data are processed about a person and the purpose of processing requires such data to be kept up to date, controllers should establish processes to ensure that the data will be verified from time to time. They should keep a

[7] Section 6(1) of the Act.
[8] Section 6(2) of the Act.
[9] Section 7 of the Act.
[10] Section 8 of the Act.

record of why it is necessary to keep personal data accurate and up to date, how such processes are expected to achieve this. They should also monitor the effectiveness of such processes, tightening them if necessary to meet the requirement.

2.5. Limit the period of retention

Controllers must keep personal data in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

"Personal data" are data about an identifiable person. If it is not possible to identify the person to whom the data relate, the Act does not apply. Controllers should analyse the data they process and determine how much of the data that is linked to an identifiable person they need to retain or for how long they need to retain that data in that form. Controllers should then establish clear retention policies and procedures to ensure data are deleted or anonymized when they are no longer needed in that form. Personal data that are only de-identified such that they could, if combined with other data, be linked back to individuals, remain subject to the Act. However, controllers may store personal data for a longer duration if the data is being further processed for archiving purposes in the public interest, scientific research, historical research or statistical purposes.[11]

2.6. Maintain integrity and confidentiality of the personal data

The Act requires controllers to ensure integrity and confidentiality of personal data that they collect and otherwise process. They must use appropriate technical and organizational measures to prevent unauthorised or unlawful processing and against loss, destruction or damage. Such measures include encryption, pseudonymisation, anonymisation, access controls, or other measures that may be prescribed in the future.[12]

Controllers should consider the risks from within and outside their organisations to data, whether due to weak organisation, poor controls on authorised access, lack of training, malicious attack or otherwise. They should consider the potential value to those who may wish to steal, manipulate, delete or corrupt data. They should also consider the risks to the systems they operate and to data subjects if the personal data is breached. Risks could range from reputational to emotional to financial to inconvenience. They should consider also vulnerabilities that may arise from the nature of the systems. For instance, systems that are accessible online or to the public may be more vulnerable than those that are accessible only by the organisation. In light of these considerations, controllers should adopt measures appropriate to address the risks. They may have to incur cost to procure security technologies, or to house data on more secure servers.

Controllers should record their assessments of these various factors and their choices so that they can demonstrate the appropriateness of their decisions about what measures to adopt. They should also review these from time to time as the nature of the data changes or the risks change. If they

[11] Section 9 of the Act.
[12] Section 10 of the Act.

experience any incident that could affect the integrity and confidentiality of the data, they should assess how it occurred, points of weakness, how it might occur in the future, and adapt the measures accordingly.

2.7. Provide required information to data subjects

The Act requires controllers to provide certain information to data subjects. The information is summarised in section 4.3 of these Guidelines. The information includes information about the controller and the purpose and legal basis of processing. It also includes the categories of data being collected, who the data may be shared with, information about any transfer of the data abroad, and how long the data will be retained. In addition, the controller must inform the data subject of his or her right to withdraw consent to processing, and how the data subject can exercise his or her other rights, including complaints to the Authority.[13]

Controllers should consider carefully the information they must provide, prepare the content in a manner that will be easily understood by data subjects, ensure that it is delivered to them in a way and at a time that allows them to consider it, and keep a record of having done so. They should check from time to time with data subjects that the information is readily understood.

3. Components of the DPMP

This section provides guidance on the controls and procedures that controllers should adopt in their DPMP. It offers examples and is not intended to be the only way to approach the DPMP, and is certainly not intended to be exhaustive. Each controller is responsible to approach the DPMP in a thoughtful and careful manner tailored to its situation with a view to ensuring compliance with the obligations in the Act and summarised in section 2 of these Guidelines.

3.1. Duly catalogued records

Under the Act, controllers must establish and maintain duly catalogued records to demonstrate how they carry out implementation of the obligations described in section 2 of these Guidelines.[14] The table below illustrates the minimum requirements for duly catalogued records and provides some examples.

Reference in the Act	Record-keeping requirements	Examples
§5	The lawful basis for the processing	Consent, contractual necessity, medical emergency
§6	The purpose of the processing	Customer relationship management, marketing and advertising, human resources, legal compliance,

[13] Section 11 and Schedule V of the Act.
[14] Section 12(1)(a) of the Act.

		providing public services such as healthcare or education
§7	Data minimisation; personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed	The records should show data minimisation efforts. For example, a website requesting just the name and email address for newsletter sign-ups, rather than asking for additional information like phone numbers or addresses. If role-based access controls are implemented, these should be recorded. For example, in a hospital, administrative staff may only access patient contact details, while medical staff can view medical histories.
§8	Accuracy	Conducting periodic reviews and audits of personal data to ensure its accuracy; sending out annual reminders to customers to update their contact information; establishing and enforcing data accuracy policies; having a policy that requires data to be checked for accuracy at regular intervals and sets out procedures for correcting inaccuracies
§9	Storage limitation	Conducting periodic reviews of data to determine whether it is still necessary to keep. For example, a healthcare provider might review patient records annually to ensure outdated or irrelevant data is removed. Restricting access to data that is nearing the end of its retention period to minimize the risk of unauthorised use. For example, access to old employee records might be limited to HR personnel only. Adhering to legal and regulatory requirements for data retention and deletion. For instance, financial institutions might retain transaction records for a specific period as mandated by financial regulations. Keeping detailed records of data retention and deletion practices, including who approved the retention period and the reasons for retaining or deleting data.
§10	Data security	Encrypting sensitive customer data such as payment information during online transactions; role-based access controls to limit data access based on job roles; using data centres with advanced security features like biometric access and surveillance; conducting regular security audits and vulnerability assessments; implementing regular data backup procedures to ensure data can be recovered in the event of a loss or disaster; providing ongoing

		training to employees on data security best practices and recognising phishing attempts or other cyber threats; developing and maintaining an incident response plan
§11	Transparency	Privacy notices; using simple language in consent forms and privacy notices; obtaining explicit consent before collecting email addresses for marketing purposes; offering clear and easy-to-use mechanisms for data subjects to opt out of data processing activities or marketing communications

3.2. Design Based on Processing Activities

The DPMP must be designed on the basis of the structure, scale, volume, and sensitivity of the controller's processing activities.[15]

- **Structure** may relate to the information systems architecture, such as whether data are held on proprietary servers or on data centres or in the cloud, whether data are processed internally or by third parties (e.g., outsourcing), whether systems are accessible to third parties (e.g., online), whether data are exchanged with third parties (e.g., suppliers and customers). Each of these scenarios may merit different controls and procedures to ensure compliance with the obligations described in section 2.

- **Scale and volume** relates to the number of data subjects whose data are processed, the number of data points for each, how much of the data are stored or actively processed, the scale of data requiring to be transmitted or regularly updated, and similar aspects.

- **Sensitivity** of processing relates to the nature of the data and whether they include special categories of personal data (see section 2.1 of these Guidelines), including whether the combination of data that are not themselves special categories of personal data might reveal such sensitive data (e.g., geo-location data showing attendance at religious or political meetings or particular type of health clinic).

Controllers may find it useful to document their data processing activities using a record of processing activities, and mapping data flows to understand how data is collected, used, shared, and stored. These will help organisations understand and document how personal data flows through their systems, ensuring they can manage and protect it effectively. By maintaining a comprehensive record of data processing activities, organisations can better ensure transparency, security, and compliance with legal obligations.

Controllers may take a tiered approach to controls and procedures where appropriate. For example,

[15] Section 12(1)(b) of the Act.

a controller might classify data into different tiers based on sensitivity (e.g., public, internal, confidential, and highly confidential) and determine the level of protection required for each type of data. Based on the classification of data, access controls, data handling procedures and audit frequencies could be subject to different standards. Below is an example of a tiered approach to internal data protection policies.

Internal controls and procedures	Examples of tiered approaches
Access controls	• **Public data**: Limited controls, accessible to a broad audience with minimal restrictions • **Internal data**: Access restricted to employees within the company who require it for their job functions • **Confidential data**: Access limited to specific departments or roles, with additional authentication measures • **Highly confidential data**: Access tightly controlled with additional security measures such as encryption, multi-factor authentication, and regular audits
Data handling procedures	• **High-volume processing**: Automated data handling and processing systems are implemented to manage large volumes efficiently, with regular monitoring and system updates • **Sensitive data**: Strict protocols for data storage, encryption, and transmission to protect sensitive information, including secure disposal methods for outdated or unnecessary data
Regular audits and reviews	• **Public data**: Less frequent audits and reviews are conducted • **Highly confidential data**: More frequent and regular audits are conducted to ensure compliance with internal policies and external regulations, and procedures are updated based on audit findings, changes in the regulatory environment, or modifications in processing activities
Training and awareness	Employees receive training tailored to their roles and the sensitivity of the data they handle, ensuring they understand and comply with the relevant internal controls and procedures

3.3. Safeguards and Impact Assessments

The Act requires controllers to have a DPMP that provides for appropriate safeguards based on certain personal data protection impact assessments (PDPIAs).[16] However, this only applies where controllers are required to conduct a PDPIA. The Act requires a DPIA where the controller intends to carry out processing which involves:[17]

[16] Section 12(1)(c) of the Act.
[17] Section 24 of the Act.

- a systematic and extensive evaluation of personal data or special categories of personal data including profiling; or
- a systematic monitoring of publicly accessible areas or telecommunication networks.

Additionally, the Authority may make rules to determine processing activities requiring PDPIA taking into consideration the scope and associated risks of that processing.

"Systematic" would reasonably mean:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

Systematic and extensive evaluation of personal data might include: a hospital implementing a new health information database with patients' health data; providing telecommunications services; email retargeting/remarketing; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices.

Systematic monitoring of publicly accessible areas would include closed circuit television cameras used by security or police services or commercial premises and depending on scale could include monitoring of entrance to and exit from buildings using electronic security systems. Systematic monitoring of telecommunication networks would include recording or interception of phone calls, text messages, email, mobile apps and internet browsing.

These are only examples. Each controller should consider whether it is engaged in systematic and extensive processing of personal data requiring a PDPIA. They should implement the controls and procedures identified in the PDPIA to protect rights and freedoms of data subjects. They should regularly review and update safeguards to address emerging risks and threats.

Controllers should refer to the Regulations on Personal Data Protection Impact Assessments for the preparation of PDPIAs. Below are some examples of how controllers might plan a DPIA and policies that they might adopt.

DPIA policy framework	Examples
Purpose and Scope	• Define the purpose of the DPIA policy and the scope of its application within the organization.
Responsibility and accountability	• Assign roles and responsibilities for conducting DPIAs, including appointing a Data Protection Officer (DPO). • Establish a DPIA review board or committee.
DPIA triggers	• Define specific scenarios that trigger the need for a DPIA

DPIA process	• Outline the step-by-step process for conducting a DPIA, including:
	  ○ Identifying the need for a DPIA
	  ○ Describing the processing activity
	  ○ Identifying measures to mitigate risks
	  ○ Documenting the DPIA and its outcomes

Checklists and tools	• Provide checklists, tools, and software solutions to facilitate the DPIA process and ensure consistency and thoroughness
Mitigation measures	• List potential measures for mitigating identified risks, such as data minimization, pseudonymization, encryption, access controls, and regular audits
Documentation and reporting	• Establish guidelines for documenting the DPIA process and outcomes, including templates and reporting structures • Specify the frequency and method of reporting DPIA findings to senior management and, if necessary, to the Authority
Review and update	• Set procedures for regular review and updating of DPIAs, especially when there are changes in processing activities or risks

3.4. Updates Based on Monitoring and Assessments

Controllers must monitor and assess their systems regularly and make updates as required to ensure continuous improvement.[18] Below are examples of monitoring and assessment tools that may serve this purpose.

Monitoring	**Examples of tools**
Data inventory and mapping	• Maintain an up-to-date inventory of data processing activities, including data flows, data storage locations, and access controls • Regularly review and update this inventory to reflect any changes
Regular audits and assessments	• Conduct regular audits and reviews of data processing activities, controls and procedures to ensure compliance with internal policies and legislation, and identify areas for improvement • Both internal audits and, where appropriate, third-party assessments are recommended
Compliance monitoring	• Establish a compliance monitoring program to ensure ongoing adherence to data protection regulations • This includes tracking changes in laws and regulations and updating internal policies accordingly
Feedback mechanisms	• Implement mechanisms to collect feedback from employees, customers, and other stakeholders about data protection practices • Use this feedback to make continuous improvements
Vendor and other	• Select and periodically assess third-party vendors and service

[18] Section 12(1)(g) of the Act.

third-party arrangements	providers to ensure they comply with data protection requirements

3.5. Governance and Oversight

Controllers must ensure that their DPMP is integrated into their governance structures and must establish internal oversight mechanisms to monitor compliance with data protection policies and procedures.[19]

Below are some examples of governance and monitoring tools that controllers may use to achieve this.

Governance and oversight tools	Examples
Comprehensive policies	• Develop and implement comprehensive data protection policies that outline the controller's commitment to data protection, roles and responsibilities, and specific procedures for data handling
Procedural documentation	• Document procedures for data collection, storage, access, sharing, and deletion to ensure consistency and compliance
Data Protection Committee	• Establish a Data Protection Committee responsible for overseeing data protection activities, ensuring compliance with regulations, and addressing privacy issues. This committee should include senior management, the Data Protection Officer (DPO), IT, legal, and other relevant departments.
Data Protection Officer (DPO)	• Appoint a DPO with a defined role within the governance structure, reporting directly to the highest level of management to ensure independence and authority
Regular reporting to management	• Provide regular reports to senior management on data protection activities, risks, incidents, and compliance status, as well as audits
Vendor and other third-party arrangements	• Establish legal responsibilities for compliance by and procedures for reporting from third parties

Compliance requires assigning responsibilities for oversight and ensure accountability at all levels. Ideally, the person who is in charge of the DPMP should be a high-level person in the organisation, sometimes even a direct report of a C-level executive, to ensure that data protection is a key consideration in strategic decision-making processes.

Controllers should consider how these governance structures cover processing by third party processors to which they outsource any processing of personal data, including not only the alteration and carrying out of logical operations, but also the mere collection, transmission and

[19] Section 12(1)(d) and (e) of the Act.

storage.

3.6. Complaints and Breach Management

A controller's DPMP must include a mechanism to receive complaints, conduct inquiries and identify personal data breaches.[20]

Data subjects, whether customers, employees, the public at large or otherwise, should know where and how to lodge a complaint relating to the processing of personal data about them. Effective and efficient complaints processes are essential to safeguarding data subjects' rights under the Act (see section 3.7 of these Guidelines). They can also be crucial in ensuring an efficient approach to handling breaches that are subject to tight deadlines.

Examples of complaint management mechanisms are included in section 3.7 of these Guidelines. Below are some examples of tools that might be helpful for data breach management.

Breach management mechanism	**Recommendations**
Incident response team	• A dedicated incident response team that includes members from IT, legal, compliance, and communications to handle data breaches
Incident response plan	• A detailed incident response plan that outlines the steps to be taken in the event of a data breach, including detection, containment, investigation, notification, and remediation
Breach detection tools	• Implementation of tools and technologies for real-time monitoring and detection of data breaches, such as intrusion detection systems and data loss prevention solutions
Immediate containment measures	• Procedures for quickly containing the breach to prevent further data loss or unauthorized access • This may include isolating affected systems, revoking access, and applying patches
Root cause analysis	• Conducting a thorough investigation to determine the root cause of the breach and implementing corrective actions to prevent recurrence
Notification procedures	• Establishing procedures for notifying affected data subjects and relevant regulatory authorities in a timely manner in accordance with the Act • Notifications should include details of the breach, potential impact, and steps being taken to mitigate harm
Remediation	• Implementing measures to remediate the breach, such as restoring

[20] Section 12(1)(f) of the Act.

measures	affected systems, recovering lost data, and enhancing security controls
Documentation	• Keeping detailed records of the breach, including the nature of the breach, affected data, steps taken to address the breach, and communications with affected parties and authorities
Post-incident review	• Conducting a post-incident review to evaluate the response to the breach, identify lessons learned, and improve the incident response plan
Training and awareness	• Regular training for employees on recognizing and responding to data breaches, including simulated breach exercises to test the effectiveness of the incident response plan

3.7. Facilitation of Data Subject Rights

A controller's DPMP must facilitate the exercise of rights of data subjects,[21] including the rights to:

- access to personal data[22]
- withdrawal of consent[23]
- object to processing[24]
- rectification or completion[25]
- erasure[26]
- request a review of a decision based solely on automated processing[27]

Below are some recommendations for request and complaint management mechanisms that would ensure clear and accessible procedures for data subjects to exercise their rights.

Data subject request and complaint management mechanism	**Recommendations**
Dedicated Data Protection Officer (DPO) or team	• A designated DPO or a specialised team should handle data protection complaints • This person or team should be easily accessible to data subjects
Request / complaint	• An online portal where data subjects can submit data subject

[21] Section 12(1)(h) of the Act.
[22] Section 13 of the Act.
[23] Section 14(1) of the Act.
[24] Section 14(2) of the Act.
[25] Section 15 of the Act.
[26] Section 16 of the Act.
[27] Section 18 of the Act.

submission portal	requests and complaints related to data protection • The portal should provide clear instructions on how to file a request / complaint and what information is needed
Contact information	• Clear and accessible contact information (email, phone number, mailing address) for submitting complaints • This information should be readily available on the controller's website and privacy notices
Request / complaint acknowledgment	• A system to acknowledge receipt of requests / complaints promptly, typically within 24-48 hours • This ensures that the data subject knows their issue is being addressed
Request / complaint tracking system	• An internal tracking system to log and monitor the status of each request and complaint • This system should record details of the request / complaint, actions taken, and outcomes
Timely resolution	• Established timelines for responding to data subject requests, investigating and resolving complaints • Inform data subjects of the expected timeline and provide updates on the progress
Internal review process	• A structured process for internally reviewing complaints, involving relevant departments (e.g., legal, compliance, IT) to ensure a thorough investigation and appropriate resolution
Escalation procedures	• Clear procedures for escalating unresolved complaints to a higher level within the organisation or to external bodies, such as the Authority, if necessary
Feedback mechanism	• A mechanism to solicit feedback from complainants on the handling of their data subject requests and complaints, which can be used to improve the request / complaint management process

4. Selected provisions of the Act

4.1. Definitions

In these Guidelines, unless the context otherwise requires—

"Act" means the Personal Data Protection Act, No. 9 of 2022;

"Authority" means the Data Protection Authority of Sri Lanka;

"biometric data" means, personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, including facial images, dactyloscopic data or iris related data;

"child" means, a natural person who is below the age of sixteen years;

"consent" means, any freely given, specific, informed and unambiguous indication by way of a written declaration or an affirmative action signifying a data subject's agreement to the processing of his personal data;

"controller" means, any natural or legal person, public authority, public corporation, non-governmental organization, agency or any other body or entity which alone or jointly with others determines the purposes and means of the processing of personal data;

"data concerning health" means, personal data related to the physical or psychological health of a natural person, which includes any information that indicates his health situation or status;

"data subject" means, an identified or identifiable natural person, alive or deceased, to whom the personal data relates;

"financial data" means, any alpha-numeric identifier or other personal data which can identify an account opened by a data subject, or card or payment instrument issued by a financial institution to a data subject or any personal data regarding the relationship between a financial institution and a data subject, financial status and credit history relating to such data subjects, including data relating to remuneration;

"genetic data" means, personal data relating to the genetic characteristics of a natural person which gives unique information about the physiology or the health of that natural person which results from an analysis of a biological sample or bodily fluid of that natural person;

"identifiable natural person" is a natural person who can be identified, directly or indirectly, by reference to any personal data;

"local authority" means, a Municipal Council, Urban Council or a Pradeshiya Sabha and includes any authority created or established by or under any law to exercise, perform and discharge

powers, duties and functions corresponding or similar to the powers, duties and functions exercised, performed or discharged by any such Council or Sabha;

"personal data" means, any information that can identify a data subject directly or indirectly, by reference to—

(a) an identifier such as a name, an identification number, financial data, location data or an online identifier; or

(b) one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or natural person;

"personal data breach" means, any act or omission that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"processing" means, any operation performed on personal data including but not limited to collection, storage, preservation, alteration, retrieval, disclosure, transmission, making available, erasure, destruction of, consultation, alignment, combination, or the carrying out of logical or arithmetical operations on personal data;

"processor" means, a natural or legal person, public authority or other entity established by or under any written law, which processes personal data on behalf of a controller;

"public authority" means, a Ministry, any Department or Provincial Council, local authority, statutory body or any institution established by any written law, or a Ministry, any Department or other authority or institution established or created by a Provincial Council;

"relevant regulatory or statutory body" means the regulatory or statutory body established by or under any written law which regulates, authorizes or supervises a public authority and includes a Ministry which carries out any such supervisory functions;

"special categories of personal data" means, the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, personal data relating to offences, criminal proceedings and convictions, or personal data relating to a child;

"Sri Lanka" means, the territorial limits of Sri Lanka as stipulated by Article 5 of the Constitution and includes the territorial waters or air space of Sri Lanka, any ship or aircraft registered in Sri Lanka, any location within the premises of a Sri Lankan mission or the residence of the Head of such mission, diplomatic agent or any other member of such mission, situated outside Sri Lanka, or within any premises occupied on behalf of, or under the control of, the Government of Sri Lanka or any statutory body established in Sri Lanka and situated outside Sri Lanka; and

"sub processor" means, in accordance with section 22(3) of the Act, a processor engaged by

another processor for carrying out specific processing activities.

4.2. Lawful bases of processing under the Act

Section 5 of the Act defines the conditions for processing to be lawful as follows:

> *The processing of personal data shall be lawful if a controller is in compliance with—*
>
> *(a) any condition specified in Schedule I hereto;*
>
> *(b) any condition specified in Schedule II hereto in the case of processing special categories of personal data;*
>
> *(c) all the conditions specified in Schedule III hereto in the case of processing personal data based on the consent of the data subject under item (a) of Schedule I or under item (a) of Schedule II hereto; or*
>
> *(d) all the conditions specified in Schedule IV hereto in the case of processing personal data in respect of criminal investigations.*

This section sets out the rules that apply to lawful processing personal data. Schedule I of the Act is a general list of lawful bases that apply to processing of personal data. Schedule II of the Act applies heightened requirements when the data being processed is one of the special categories of personal data. There are overlaps between Schedule I and Schedule II of the Act, which are explained below in sections 4.2.1 and 4.2.2.

On of the lawful bases of processing is where the data subject has given consent to the processing. Schedule III of the Act defines the conditions that make consent lawful under Sri Lankan law.

Finally, Schedule IV of the Act provides for the special rules that apply to processing personal data within the context of criminal investigations.

4.2.1.Conditions for lawful processing

Schedule 1 of the Act sets out the legal bases for lawful processing in accordance with Section 5(a) of the Act. These are:

- **Consent:** The data subject has consented to the processing of their personal data.
- **Contract:** This legal basis applies where the data subject is a party to a contract or wishes to enter into a contract with the controller. Processing personal data would be legal if it is necessary for the performance of the contract or to take steps at the request of the data subject prior to entering into the contract. For example, a seller would need to process a buyer's address to ship the purchased goods. Similarly, a person buying a car would provide their personal details (such as name and address) to the vendor so that the vendor can prepare the sale agreement.
- **Legal Obligation:** Processing is necessary for compliance with a legal obligation to which the controller is subject. For example, a financial institution may be subject to anti-money

laundering requirements. Accordingly, the financial institution would be legally required to collect and process personal data, such as identification documents and transaction histories, to verify the identities of their customers and monitor transactions for suspicious activities.

- **Vital Interests:** Processing is necessary to address an emergency that poses a threat to the life, health, or safety of the data subject or another person. An example could be a rescue team accessing personal data during a natural disaster. For instance, if there's a flood and people are trapped in their homes, emergency services might use personal information, such as addresses, to locate the individuals and prioritise their rescue efforts.

- **Public Task:** Processing is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller.

  "Public interest" includes the processing of personal data required for health-related purposes, including public health, social protection, management of healthcare services, controlling communicable deceases and other serious threats to health. It also includes the processing of personal data carried out by official authorities to achieve objectives or purposes established by law.

  For instance, public health officials might collect and analyse data on individuals who have tested positive for a contagious illness, such as their address, to track the spread of the disease, identify potential outbreaks, and implement containment measures. This processing would be necessary for protecting public health, preventing further transmission, and ensuring effective responses to an outbreak as per their statutory mandate under relevant legislation.

- **Legitimate Interests:** Processing is necessary to achieve the legitimate interests of the controller or a third party, unless these interests are outweighed by the data subject's rights, particularly when the data subject is a child, which require the protection of personal data.

  The term "legitimate interest" includes the legitimate interests of the controller when the data subject is a client of the controller or provides services to the controller. For instance, a company may collect and analyse performance metrics and feedback about its employees to manage their professional development and make decisions about promotions or salary increases. This processing is based on the company's legitimate interest in ensuring effective performance management and maintaining a productive workforce, while the data subjects are employees who provide services to the company.

  Another type of "legitimate interest" listed in Schedule 1 is in cases where the data subject would reasonably expect the processing at the time and in the context of the collection of the personal data. For example, if a customer enrols in a store's loyalty program and provides personal information such as their email address and purchase history, they would reasonably expect that their data will be processed to track their rewards, offer personalised discounts, and communicate program updates. The legitimate interest here is the store's

need to manage the loyalty program effectively and enhance the customer experience, which aligns with the data subject's expectations at the time of data collection.

Finally, processing that is necessary for preventing fraud and ensuring network and information security are listed as legitimate interests. A bank may analyse patterns in credit card transactions to detect potential fraudulent behaviour. Similarly, a company may use intrusion prevention systems to continuously monitor network traffic for suspicious activities or potential security threats. These systems analyse incoming and outgoing data to identify patterns that could indicate a cyberattack, such as unusual traffic spikes or unauthorised access attempts. By processing data this way, the company aims to protect its IT infrastructure and sensitive information from potential breaches, thus maintaining the security and integrity of its network.

4.2.2.Conditions for lawful processing of special categories of personal data

The Act defines special categories of personal data as:

> *the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, personal data relating to offences, criminal proceedings and convictions, or personal data relating to a child[.]*

Schedule 2 of the Act sets out the legal bases for lawful processing of special categories of personal data in accordance with Section 5(b) of the Act. Many of these overlap with the legal grounds in Schedule I, with certain differences.

- **Consent**: The data subject has given explicit consent for one or more specified purposes, unless prohibited by other laws. For children, consent must come from a parent or legal guardian.

- **Legal Obligations**: Processing is necessary for the controller's obligations and data subject's rights in employment, social security, public health, and related areas, as per any written law with appropriate safeguards. For example, a company might process data related to employees' health to ensure compliance with occupational health and safety laws. This could include processing data about vaccinations or health conditions to manage risks in the workplace, especially in industries where health and safety are critical, such as healthcare and manufacturing.

- **Emergency Situations:** Processing is necessary to respond to emergencies threatening life, health, or safety when the data subject cannot give consent. For instance, if a person is unconscious after an accident and is taken to the emergency room, healthcare professionals may need to access the person's medical history to provide the appropriate treatment.

- **Public Data:** This basis for processing applies when the data subject has manifestly made

the data public. An example is a social media post about the data subject's political opinions, religious or philosophical beliefs.

- **Legal Claims:** Processing is necessary for legal claims or when courts act in their judicial capacity. For instance, if law enforcement is investigating a case involving allegations of identity theft or financial fraud, they might process special categories of data such as bank account details of individuals involved in the alleged fraud. This data would be crucial for identifying perpetrators, understanding the extent of the fraud, and gathering evidence for prosecution.

- **Public Interest:** Processing is necessary for purposes provided in any written law or public interest, with suitable measures to safeguard the data subject's rights and freedoms.

  "Public interest" includes the processing of personal data required for health-related purposes, including public health, social protection, management of healthcare services, controlling communicable deceases and other serious threats to health. It also includes the processing of personal data carried out by official authorities to achieve objectives or purposes established by law.

  For example, public health officials might collect and analyse data on individuals who have tested positive for a contagious illness, such as their vaccination status and other medical conditions, to implement containment measures and develop a public health policy. Suitable measures to safeguard the data subject's rights could be anonymisation and data minimisation to process the minimum amount of data that is necessary for public health purposes.

- **Medical Purposes:** Processing is necessary for preventive or occupational medicine, diagnosis, treatment, or healthcare management, conducted by a licensed health professional. For example, when a patient undergoes a diagnostic test such as an MRI or a biopsy, the medical team collects and analyses the patient's health information to diagnose the condition accurately.

- **Research and Archiving:** Processing is necessary for public interest archiving, scientific or historical research, or statistical purposes, with measures to protect the data subject's rights and freedoms. For example, a research institution may process personal data from historical records to study demographic changes over the past century. This may include archival data such as census records, old medical records, and immigration records. As safeguards, the institution could ensure that the data is anonymised or pseudonymised where possible to protect individual identities. Another safeguard could be to restrict the access to the data to only authorised researchers, and implement robust data security measures to prevent unauthorised access.

4.2.3.Conditions for consent of the data subject

The Act defines "consent" as

any freely given, specific, informed and unambiguous indication by way of a written declaration or an affirmative action signifying a data subject's agreement to the processing of his personal data.

Schedule III of the Act sets out the conditions for lawful consent when the legal basis for processing is consent in accordance with Section 5(c) of the Act. These apply whether the data being processed fall under one of the special categories of data or not. Accordingly, the following conditions must be met for consent to be lawful:

- **Demonstration of consent:** The controller must be able to demonstrate that the data subject has consented to the processing of their personal data.

- **Clarity in written declarations:** If consent is given as part of a written declaration that also includes other matters, the consent request must be clearly distinguishable, intelligible, and accessible, using clear and plain language. The declaration must comply with the Act's provisions.

  For example, if consent to process the data subject's financial data is requested as part of a loan agreement, the consent part should be clearly separate from the rest of the agreement and easily understood by a layperson.

- **Freely given consent:** When assessing if consent is freely given, special attention should be given to whether the performance of a contract or provision of a service is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. For example, collection and processing of a user's personal data for personalised advertising and marketing is not necessary for a step tracker app. Users should be able to use the app without providing additional consent beyond what is necessary for the app's core functionality.

- **Right to withdraw consent:** Before giving consent, the data subject must be informed that they can withdraw their consent at any time, subject to the provisions of the Act.

4.2.4. Processing of personal data relating to criminal investigations

Schedule IV of the Act governs the processing of personal data within the context of criminal investigations as required by Section 5(d) of the Act.

- **Lawful investigations and safeguards:** Processing personal data for lawful investigations on offenses or related security measures must be conducted in compliance with applicable laws, ensuring that appropriate safeguards are in place to protect the rights and freedoms of data subjects.

- **Legal basis:** Processing is lawful if conducted according to the Code of Criminal Procedure Act, No. 15 of 1979, or other relevant written laws.

- **Safeguards:** The Minister may prescribe the conditions for providing appropriate

safeguards for the rights and freedoms of data subjects.

4.3. Information that must be provided to data subjects

Section 11 of the Act provides:

> *A controller shall, provide data subjects—*
>
> *(a) the information referred to in Schedule V; and*
>
> *(b) the information regarding any decision taken pursuant to a request made under PART II of this Act,*
>
> *in writing or by electronic means and in a concise, transparent, intelligible and easily accessible form.*

Controllers must provide the following information to data subjects at the time of collection of their personal data:

- **Identity and Contact:** Identity and contact details of the controller and, if applicable, the controller's representative.
- **Data Protection Officer:** Contact details of the Data Protection Officer, if applicable.
- **Purpose and Legal Basis:** Purposes for which personal data is processed and the legal basis for the processing.
- **Legitimate Interests:** Legitimate interest pursued by the controller or a third party if processing is based on legitimate interests.
- **Categories of Data:** Categories of personal data being collected.
- **Consent Withdrawal:** Information about the right to withdraw consent and the procedure for doing so, without affecting the lawfulness of prior processing.
- **Data Sharing:** Recipients or third parties with whom the data may be shared, if applicable.
- **Cross-Border Transfer:** Information on any cross-border transfers of personal data, if applicable.
- **Data Retention:** Retention period or criteria for determining the retention period.
- **Data Subject Rights:** Procedure for exercising the rights of the data subject.
- **Complaints:** Information about the right to file complaints with the Authority.
- **Data Provision Requirements:** Explanation on whether providing personal data is a statutory or contractual requirement, and the consequences of not providing the data.

- **Automated Decision-Making:** Information about automated decision-making, including profiling, and its significance and consequences.

If the data is processed for a purpose other than originally collected, the controller must provide detailed information on this further processing.

When personal data is obtained indirectly, the controller must inform the data subject of the data's source and whether it came from publicly accessible sources. In this scenario, the controller shall provide the required information within a reasonable period, which shall not exceed one month. If the controller will use the personal data for communication with the data subject, then the data subject shall receive this information at the time of the first communication with the data subject. If the data is first disclosed to another recipient, then the data subject shall be informed when the personal data is disclosed.

Information requirements do not apply to cases where the data subject is already informed or if providing information is impossible or involves disproportionate effort, especially for archival, scientific, historical, or statistical purposes. In addition, if a statutory provision explicitly covers the disclosure, then the controller does not have to repeat it. Finally, if the personal data remains confidential due to professional privilege or statutory obligations, then no disclosure is required by virtue of the Act. There might be other necessary disclosures under other laws.