PUBLIC CONSULTATION PAPER NO. 04/2024:

PERSONAL DATA PROTECTION STANDARDS

Start Date : 1 October 2024

End Date : 18 October 2024

PART 1: INTRODUCTION AND BACKGROUND

[A] Introduction

1.1 The Personal Data Protection Regulations 2013 ("**Regulations**") which were issued pursuant to the Personal Data Protection Act 2010 ("PDPA"), provides that Data Controllers (and where the security standard is concerned, Data Processors as well[1]) must carry out the following[2]:

(a) develop a security policy in accordance with the **security standard**;

(b) retain personal data in accordance with the **retention standard**; and

(c) process personal data in accordance with the **data integrity standard**,

based on standards as determined by the Personal Data Protection Commissioner ("**Commissioner**") from time to time.

1.2 On 23 December 2015, the Commissioner issued the Personal Data Protection Standards 2015 ("**Standards**") pursuant to the Regulations, which introduced a set of **security, retention and data integrity standards** which outline minimum compliance standards / requirements for the Security, Retention and Data Integrity Principles set out under the PDPA.[3] The language of the current Regulations only allows the Commissioner to prescribe standards in relation to **these three (3) Personal Data Protection Principles**. As such, the focus of this PCP will be limited to proposed amendments to requirements for the **Security, Retention and Data Integrity Principles *only***.

1.3 In order to comply with the Standards prescribed, Data Controllers (and in the case of the security standard, Data Processors as well) shall take all reasonable steps to ensure that personal data is:

(a) protected from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard to requirements of the **security standard**;

(b) destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed by having regard to the requirements of the **retention standard**; and

(c) accurate, complete, not misleading and kept updated by having regard to the purpose, including any directly related purpose, for which the personal data was collected and processed further, by adopting the measures under the **data integrity standard**.

---

[1] The latest amendments to the PDPA impose direct obligations on Data Processors to comply with the Security Principle. As such, the Regulations and the Standards relating to the Security Principle to similarly apply to Data Processors as well.

[2] Reg. 6,7 and 8 of the Regulations.

[3] A brief explanation of these principles are as follows: Security Principle (Section 9 of the PDPA) requires Data Controllers and Data Processors to take practical steps to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction; Retention Principle (Section 10 of the PDPA) requires Data Controllers to take reasonable steps to destroy or permanently delete personal data once the personal data is no longer required for the purpose for which it was collected; and Data Integrity Principle (Section 11 of the PDPA) requires Data Controllers to take reasonable steps to ensure that personal data collected and processed is accurate, complete, not misleading and updated.

1.4 For ease of reference, the full text of the requirements prescribed under the Standards has been appended in **Appendix 1**.

1.5 To update the Standards and bring them in line with international best practices, a **revised** set of security, retention and data integrity standards is being developed by the Commissioner.

1.6 Pursuant to the above, this Public Consultation Paper ("**PCP**") seeks to gather public views and feedback regarding aspects that will be or should be addressed in the proposed revised Standards.

PART 2: PROPOSED AMENDMENTS TO THE STANDARDS

2.1 As an overview, Part 2 of this PCP on proposed amendments to the Standards is segmented into the following aspects:

(a) outcome-based Standards;

(b) areas to be addressed under the security standard;

(c) areas to be addressed under the retention standard;

(d) areas to be addressed under the data integrity standard; and

(e) role of certification schemes to demonstrate compliance with the Standards;

[A] Outcome-based Standards

2.2 Background: The minimum standards prescribed by the current Standards (as appended in **Appendix 1**) primarily consist of "black and white" rules, i.e., prescriptive and specific instructions or measures that Data Controllers must comply with.

2.3 Examples of such "black and white" rules within the Standards include:

(a) the requirement to register all employees involved in the processing of personal data;

(b) the requirement to terminate an employee's access rights to personal data after their resignation / termination of employment with the Data Controller;

(c) the requirement to provide user IDs and passwords for authorised employees to access personal data;

(d) the requirement to dispose of personal data collection forms used in commercial transactions within a period not exceeding fourteen (14) days, except if / unless the forms carry legal values in relation to the commercial transaction; and

(e) the requirement to record personal data transferred conventionally such as through mail, delivery, fax and etc.

2.4 Such "black and white" rules, while providing prescriptive and specific instructions to Data Controllers to demonstrate compliance with the requirements of the Security, Data Integrity and Retention Principle, have their drawbacks, as follows:

(a) a prescriptive set of Standards is not capable of providing a comprehensive listing of all measures that Data Controllers / Data Processors should implement in order to safeguard personal data or comply with the requirements of the Security Principle, due to the constantly evolving data and security landscape, emerging threats and evolving best practices;

(b) "black and white" rules fail to account for the different levels of measures that should be implemented by Data Controllers / Data Processors, which should depend on the risks presented by the personal data processing activities carried

out by them. Instead, these rules risk imposing a uniform set of standards / requirements regardless of the levels of risk presented by the Data Controller's / Data Processor's personal data processing activities;

(c) enforcing the Standards becomes challenging as the current Standards only set out basic / baseline security measures for Data Controllers to comply with, which do not match the scale or complexity of processing carried out by certain Data Controllers / Data Processors. Further, "black and white" rules have led to difficulties in enforcing the Standards against Data Controllers for failure to take sufficient or adequate security measures to prevent a personal data breach, as the security measures required or ought to have been taken do not correspond with the prescriptive / specific rules outlined in the Standards.

2.5 It is noted that other jurisdictions are generally less prescriptive compared to the requirements outlined in the Standards and generally refrain from prescribing "black and white" requirements as to the measures that Data Controllers should implement to demonstrate compliance with their equivalent of the security, data integrity and retention standards.

2.6 For instance, the UK does not provide an exhaustive list of minimum security measures that organisations must implement to meet the security requirements under the EU GDPR / UK Data Protection Act. Instead, the UK's data protection authority outlines a set of security outcomes for organisations to comply with, and the measures taken by organisations to comply with these security outcomes will vary depending on the risks presented by the scope and nature of the data processing activities carried out by the organisation.

2.7 Proposal: It is proposed that the "black and white" rules under the Standards be replaced with requirements that are drafted based on a more outcome-based approach.

2.8 An outcome-based approach will focus on defining the Commissioner's expectations and the outcomes that Data Controllers should aim to achieve, and move away from prescribing specific processes that Data Controllers / Data Processors should put in place.

2.9 Examples of measures based on an outcome-based approach are as follows and may include the prescribed measures under the existing Standards:

(a) in respect of the security standard, that there is an appropriate level of internal processes in place to manage, track and limit access to personal data on a strictly need-to-know basis

Example: maintaining an inventory list of users/user accounts with access to personal data, and ensuring that access rights held by employees are promptly removed or disabled if no longer required; and

(b) in respect of the security standard, that the Data Controller has implemented legally enforceable measures to manage and mitigate security risks that may arise as a result of using third party Data Processors (e.g. third party service providers who process Data Controllers' personal data for the Data Controller)

Example: ensuring that Data Controllers have in place an agreement with Data Processors which require the Data Processors to employ appropriate security measures to protect personal data.

2.10 Notwithstanding the above, the Commissioner recognise that small businesses and organisations may lack the resources to determine how to comply with the measures of the Standards and may prefer clear directives on specific actions needed. In such cases, the Commissioner will provide examples of practical measures that small businesses and organisations can implement to meet the prescribed outcomes and expectations outlined in the Standards.

2.11 For instance, in relation to the requirement to implement appropriate measures to prevent unauthorised or accidental disclosure or leakage of personal data by personnel, the Standards will provide examples such as disabling USB ports to restrict any transfers of personal data through removable devices or recording / logging printing of personal data records, as measures that can be taken to comply with the requirement. Further examples of measures that Data Controllers / Data Processors may adopt, can be found in Appendix 2 below.

2.12 In order to ensure the Standards are applied based on the risks associated with the personal data processing, the amended Standards will stipulate that a risk-based approach must be taken, and the measures implemented to meet the "outcomes" stipulated must be proportionate with the level of risk faced by the organisation, depending on factors such as:

(a) the nature, scope and volume of personal data processing activities; and

(b) the potential harm and impact that would result should there be loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction of the personal data.

Question 1

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you agree with the proposed approach of moving towards an outcome-based approach based on the examples set out in paragraph 2.9(a) and (b) above that moves away from prescribing specific processes that Data Controllers / Data Processors should put in place?

(b) Do you foresee any potential challenges / difficulties that may be faced by the Commissioner in enforcing standards that are based on an outcome-based approach? Would outcome-based standards be too subjective for the Commissioner to enforce?

(c) Are there any existing sector-specific security, data integrity or retention standards prescribed for your industry / sector? If yes, please specify.

[B] Areas to be addressed under the security standard

2.13 Background: Based on the latest amendments to the PDPA, the Security Principle is now directly applicable to Data Controllers and Data Processors. Based on the existing Standards, the minimum security standards prescribed are categorised according to whether personal data is processed electronically or physically, which may be unnecessarily duplicative.

2.14 Proposal: Commissioner propose to remove the differentiation between personal data processed electronically or physically and provide security standards which applies to personal data generally, whether it is processed electronically and/or physically. To avoid any potential confusion about whether a measure is applicable to personal data processed electronically, physically, or both, the measures specified in the amended Standards will, by default, apply to both electronic and physical processing of personal data. Extra emphasis or clarification will be provided if a measure is specifically applicable only to personal data processed electronically or physically.

2.15 In order to provide a more comprehensive listing of security outcomes Data Controllers / Data Processors should meet, Commissioner propose to broadly address the following key elements pertaining to security controls:

(a) governance structure;

(b) access control;

(c) asset and data inventory management;

(d) digital threats (e.g. protection against viruses, malware and other threats);

(e) network security and software updates;

(f) third-party risk management (e.g. managing risks of sharing personal data with Data Processors); and

(g) training / awareness.

2.16 Please refer to **Appendix 2** below for examples of the types of security elements, as well as the relevant security measures, identified by other jurisdictions.

Question 2

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you agree with the proposed removal of the differentiation between security measures that are applicable to personal data processed electronically or physically?

(b) Besides the key elements referred in paragraph 2.15 above, are there any additional key elements you believe should be included in the list to cover all necessary security outcomes comprehensively?

(c) Do you think Data Controllers and Data Processors are ready to implement security measures which include the implementation of anonymisation and pseudonymisation of personal data?

[C] Areas to be addressed under the retention standard

2.17 Background: Under the PDPA, the Retention Principle is only applicable to Data Controllers and as such, the minimum retention standards discussed herein do not directly apply to Data Processors. The current retention standards primarily cover

measures for the planning of retention periods and the preparation of records of disposal for personal data.

2.18 Proposal: In order to make the retention measures more comprehensive, it is proposed to further expand on the measures of the retention standard by referencing the following key elements:

(a) duration of retention period;

(b) documentation and records for retention and disposal of personal data;

(c) methods of destruction or deletion of personal data; and

(d) third-party retention of personal data.

2.19 Please refer to **Appendix 2** below for examples of the types of retention outcomes, as well as the relevant retention measures, deployed by other jurisdictions.

Question 3

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you agree with the proposed expansion of retention standards to include the key elements stated in paragraph 2.18 in order to provide clearer and more comprehensive guidelines?

(b) Other than those stated in paragraph 2.18, are there any additional key elements or specific measures you believe should be included in order to better address data retention?

[D] Areas to be addressed under the data integrity standard

2.20 Background: Under the PDPA, the Data Integrity Principle is only applicable to Data Controllers and does not directly apply to Data Processors. The current listing of minimum data integrity standards is brief and does not address the key elements pertaining to maintaining the integrity of personal data. Further, it is not sufficiently comprehensive in terms of the measures that should be taken by Data Controllers to ensure that personal data is accurate, complete, not misleading, and kept up to date.

2.21 Proposal: To ensure more comprehensive data integrity standards, it is proposed to address key elements pertaining to maintaining the integrity of personal data as well as indicate relevant data integrity measures that may be deployed by Data Controllers. This approach will provide a clear and detailed framework for Data Controllers to follow, ensuring the accuracy, consistency, and reliability of personal data throughout its lifecycle.

2.22 The proposed key elements to be addressed in relation to the data integrity standard are as follows:

(a) data validation and verification;

(b) data quality monitoring;

(c) data consistency (e.g., implementing internal practices and procedures to ensure personal data is collected and recorded in a standardised and compatible format); and

(d) data lifecycle management (e.g., promptly update or add new personal data to relevant existing records).

2.23 Please refer to **Appendix 2** below for examples of the types of data integrity outcomes, as well as the relevant data integrity measures, deployed by other jurisdictions.

Question 4

In providing your responses to the question below, please provide clear justifications to support your views:

(a) Do you agree with the proposed expansion of data integrity standards to include the key elements stated in paragraph 2.22 above in order to provide clearer and more comprehensive guidelines?

(b) Are there any additional key elements or specific measures that you believe should be included in order to address data integrity other than those referred in paragraph 2.22 above?

[E] Role of certification schemes to demonstrate compliance with the Standards

2.24 Background: The current Standards do not expressly recognise the use of certification schemes, marks or seals to demonstrate compliance with the requirements of the Standards. In practice, proactive Data Controllers may have already obtained data privacy certification etc. to demonstrate a level of data privacy compliance which meets or exceeds the requirements in the Standards. As such, requiring compliance with the Standards on top of the certification requirements may be an unnecessarily duplicative requirement for such Data Controllers.

2.25 The Commissioner note that other jurisdictions recognise, encourage or otherwise adopt the use of certification schemes, marks or seals as one of the methods that Data Controllers / Data Processors can utilise to demonstrate compliance with their respective data protection regulatory frameworks.

2.26 Proposal: It is proposed that industry certifications be recognised as a method that Data Controllers / Data Processors can utilise to demonstrate compliance with the Standards.

2.27 Industry certifications will be voluntary but encouraged as a means of showing compliance with the Standards. While obtaining an industry certification does not automatically imply blanket compliance or immunity from sanctions or liabilities under the Standards, it will be considered by the Commissioner as a mitigating factor when assessing a Data Controller / Data Processor's compliance with the PDPA and the Standards.

2.28 Examples of industry certification include ISO 27001 certification for Information Security Management System (ISMS), ISO 27017 certification on information security controls for the provision and use of cloud services, and ISO 27701 certification for Privacy Information Management System (PIMS).

Question 5

In providing your responses to the question below, please provide clear justifications to support your views:

(a) Are there specific industry certifications that are mandated or recommended for organisations in your sector? Is there a list of approved or recognised certifications applicable to your industry? If yes, please specify.

(b) Please specify what industry certifications the Commissioner should recognise for Data Controllers / Data Processors to utilise as evidence of compliance with the Standards?

(c) What potential challenges might arise from recognising industry certifications for both Data Controllers / Data Processors, and how might these challenges be addressed?

Appendix 1

Security Standard

Data Security for Personal Data Processed Electronically	
No.	**Descriptions**
1	Register all employees involved in the processing of personal data.
2	Terminate an employee's access rights to personal data after his/her resignation, termination, termination of contract or agreement, or adjustment in accordance with changes in the organisation.
3	Control and limit employees' access to personal data system for the purpose of collecting, processing and storing of personal data.
4	Provide user ID and password for authorized employees to access personal data.
5	Terminate user ID and password immediately when an employee who is authorized access to personal data is no longer handling the data.
6	Establish physical security procedures as follow: i. control the movement in and out of the data storage site; ii. store personal data in an appropriate location which is unexposed and safe from physical or natural threats; iii. provide a closed-circuit camera at the data storage site (if necessary); and iv. provide a 24-hour security monitoring (if necessary).
7	Update the Back up/ Recovery System and anti-virus to prevent personal data intrusion and such.
8	Safeguard the computer systems from malware threats to prevent attacks on personal data.
9	The transfer of personal data through removable media devices and cloud computing services is not permitted unless with written consent by an officer authorized by the top management of the Data Controller / Data Processor organisation.
10	Record any transfer of data through removable media devices and cloud computing services.
11	Personal data transfer through cloud computing services must comply with the personal data protection principles in Malaysia, as well as with the personal data protection laws of other countries.
12	Maintain a proper record of access to personal data periodically and make such record available for submission when directed by the Commissioner.
13	Ensure that all employees involved in processing personal data always protect the confidentiality of the Data Subject's personal data.
14	Bind an appointed third party by the Data Controller with a contract for operating and carrying out personal data processing activities. This is to ensure the safety of personal data from loss, misuse, modification, unauthorized access and disclosure.

Data Security for Personal Data Processed Non-Electronically	
No.	**Description**
1	Register employees handling personal data into a system/registration book before being allowed access to personal data.
2	Terminate an employee's access rights to personal data after his/her resignation, termination, termination of contract or agreement, or adjustment in accordance with changes in the organisation.
3	Control and limit employees' access to personal data system for the purpose of collecting, processing and storing of personal data.
4	Establish physical security procedures as follows: i. store all personal data orderly in files; ii. store all files containing personal data in a locked place; iii. keep all the related keys in a safe place; iv. provide record for keys storage; and v. store personal data in an appropriate location which is unexposed and safe from physical or natural threats.
5	Maintain a proper record of access to personal data periodically and make such record available for submission when directed by the Commissioner.

6	Ensure that all employees involved in processing personal data always protect the confidentiality of the Data Subject's personal data.
7	Record personal data transferred conventionally such as through mail, delivery, fax and etc.
8	Ensure that all used papers, printed documents or other documents exhibiting personal data are destroyed thoroughly and efficiently by using shredding machine or other appropriate methods.
9	Conduct awareness programmes to all employees (if necessary) on the responsibility to protect personal data.

Retention Standard

No.	Descriptions
1	Determine the retention period in all legislation relating to the processing and retention of personal data are fulfilled before destroying the data.
2	Keep personal data no longer than necessary unless there are requirements by other legal provisions.
3	Maintain a proper record of personal data disposal periodically and make such record available for submission when directed by the Commissioner.
4	Dispose of personal data collection forms used in commercial transactions within the period not exceeding fourteen (14) days, except if/unless the forms carry legal values in relation to the commercial transaction.
5	Review and dispose of all unwanted personal data that in the database.
6	Prepare a personal data disposal schedule for inactive data within a 24-month period. The personal data disposal schedule should be maintained properly
7	The use of removable media devices for storing personal data is not permitted without written approval from the top management of the organisation.

Data Integrity Standard

No.	Descriptions
1	Provide personal data update form for Data Subjects, either via online or conventional.
2	Update personal data immediately once data correction notice is received from Data Subject.
3	Ensure that all relevant legislation is fulfilled in determining the type of documents required to support the validity of the Data Subject's personal data.
4	Notify on personal data updates either through the portal or notice at premises or by other appropriate methods.

[the remainder of this page is intentionally left blank]

Appendix 2

*Note: For avoidance of doubt, the examples provided under this Appendix 2 are not intended to be the draft revised Standards. These are **EXAMPLES** of security, retention, data integrity measures that Data Controllers / Data Processors may adopt to demonstrate compliance.*

[A] Examples of Security Measures

Key elements	Examples
Governance	• There are appropriate data protection and information security policies and processes in place, and if required the organisation shall ensure that records of processing activities are maintained. • There are appropriate steps to identify, assess and understand security risks to personal data and the systems that process this data. • The Data Controller / Data Processor defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems involved in the processing of personal data.
Access Control	• The Data Controller / Data Processor understands, documents, and manages access to personal data and systems that process this data. • Access rights granted to specific users must be understood, and limited to those users who reasonably need such access to perform their functions, and removed when no longer needed. • The Data Controller / Data Processor undertakes activities to check or validate that the technical system permissions are consistent with the documented user access rights. • The Data Controller / Data Processor should ensure that users (or any automated functions) accessing personal data are appropriately authenticated and authorised. • The Data Controller / Data Processor should prevent users from downloading, transferring, altering, or deleting personal data where there is no legitimate organisational reason to do so. Legitimate access should be appropriately constrained, and there should be an appropriate audit trail. • The Data Controller / Data Processor should have a robust password policy that avoids users having weak passwords, such as those trivially guessable.
Asset and data inventory management	• The Data Controller / Data Processor understands and catalogues the personal data it processes and can describe the purpose for processing it. The Data Controller / Data Processor also understands the risks posed to Data Subjects of any unauthorised or unlawful processing, accidental loss, destruction or damage to that data. • An up-to-date asset inventory of the organisation's assets is maintained in the organisation. • Hardware and software assets that are unauthorised or have reached their respective end-of-support (EOS) term shall be replaced • There are measures in place to prevent unauthorised / accidental leakage of personal data from the Data Controller / Data Processor (e.g. anonymisation or pseudonymisation measures).
Digital threats	• Solutions to protect against digital threats such as viruses and malware shall be used and installed to protect the organisation's systems and networks. • Updates and patches for systems and applications should be applied as soon as possible.
Third-party risks	• The Data Controller / Data Processor understands and manages security risks to its processing operations that may arise as a result of using third parties as Data Processors. This includes ensuring that they employ appropriate security measures.

Audit and testing	• The Data Controller / Data Processor undertakes regular testing to evaluate the effectiveness of its security measures, including virus and malware scanning, vulnerability scanning, and penetration testing as appropriate. The results of any testing should be recorded, along with any remediation action plans.
Training and awareness	• The Data Controller / Data Processor puts in place training for all employees to ensure that employees are aware of the data protection practices of the Data Controller / Data Processor and what is expected of them when handling personal data.
Incident response	• There should be an incident response plan to guide the Data Controller / Data Processor on how to respond to personal data breaches.

[B] Examples of Retention Measures

Key elements	Examples
Duration of retention period	• The Data Controller must take reasonable steps to destroy personal data or ensure it is de-identified if it no longer needs the data for any purpose for which it may be used or disclosed. This obligation is contingent on there being no other applicable legal requirements regarding retention.
Documentation and records of retention and disposals of personal data	• The Data Controller should have practices, procedures, and systems in place to identify personal data that needs to be destroyed or de-identified. • The Data Controller should maintain documentation and records of the retention periods and the methods of disposal of personal data.
Methods of destruction or deletion of personal data	• Disposal through garbage or recycling collection would not ordinarily constitute taking reasonable steps to destroy the personal data unless the data has been destroyed through processes such as pulping, burning, pulverising, disintegrating, or shredding. • The methods will vary depending on the type of hardware used to store the data. In some cases, it may be possible to 'sanitise' the hardware to completely remove stored personal data. Where irretrievable destruction is not possible, the Data Controller should take reasonable steps to de-identify the data. • Where it is not possible to irretrievably destroy personal data held in electronic format, reasonable steps to destroy it would include putting the data 'beyond use'. This means: (a) the data cannot be used or disclosed; (b) the Data Controller cannot grant access to the data to any other entity; (c) the data is surrounded with appropriate technical, physical, and organisational security measures, including access controls, logs, and audit trails; and (d) the Data Controller commits to taking reasonable steps to irretrievably destroy the data if or when it becomes possible.
Third-party retention of personal data	• On a third party's hardware, such as cloud storage, where the Data Controller has instructed the third party to irretrievably destroy the personal data, reasonable steps would include verifying that this destruction has occurred.

[C] Examples of Data Integrity Measures

Key elements	Examples
Data validation and verification	• If personal data is to be used or disclosed for a new purpose that is not the primary purpose of collection, assess the quality of the personal data with regard to that new purpose before use or disclosure.

	• Contact Data Subjects to verify the quality of personal data when it is used or disclosed, particularly if there has been a lengthy period since its collection.
Data quality monitoring	• Conduct regular reviews of the quality of personal data held by the organisation to ensure it is accurate, up-to-date, complete, and relevant at the time of use or disclosure. • Implement internal practices, procedures, and systems to audit, monitor, identify, and correct poor-quality personal data, including training staff in these practices, procedures, and systems
Data consistency	• Implement protocols to ensure personal data is collected and recorded in a consistent format.
Data lifecycle management	• Ensure updated or new personal data is promptly added to relevant existing records. • Provide Data Subjects with a simple means to review and update their personal data on an ongoing basis. • Remind Data Subjects to update their personal data each time the organisation engages with them. • Check that a third party from whom personal data is collected has implemented appropriate practices, procedures, and systems to ensure data quality.

[the remainder of this page is intentionally left blank]