PUBLIC CONSULTATION PAPER NO. 1/2025

DATA PROTECTION IMPACT ASSESSMENT GUIDELINE

Start Date: 20 March 2025

End Date: 19 May 2025

PART 1: INTRODUCTION AND BACKGROUND

1.1 The Personal Data Protection (Amendment) Act 2024 introduces a new section 12A to the Personal Data Protection Act 2010 ("**Act 709**") which provides the mandatory requirement for data controllers and data processors to appoint Data Protection Officer ("**DPO**").

1.2 The full text of Section 12A of the Act 709 is as follows:

> ***Appointment of data protection officer***
>
> ***12A.*** *(1) A data controller shall appoint one or more data protection officers who shall be accountable to the data controller for the compliance with this Act.*
>
> *(2) Where the processing of personal data is carried out by a data processor on behalf of the data controller, the data processor shall appoint one or more data protection officers who shall be accountable to the data processor for the compliance with this Act.*
>
> *(3) The data controller shall notify the Commissioner on the appointment of data protection officer in the manner and form as determined by the Commissioner.*
>
> *(4) The appointment of data protection officer under subsections (1) and (2) shall not discharge the data controller or data processor from all duties and functions under this Act.*

1.3 One of the proposed responsibilities of a DPO is to provide support and advice on the implementation of data protection impact assessments ("**DPIA**").

1.4 To guide DPOs on how to conduct a DPIA, the Data Protection Impact Guideline ("**DPIA Guideline**") is being developed by the Personal Data Protection Commissioner ("**Commissioner**") to set the minimum requirements and practical steps in managing and protecting personal data controlled by an organisation.

1.5 DPIA can help organisations to systematically identify potential risks associated with their data processing activities. By identifying risks early, organisations can introduce preventive measures to manage these risks. DPIA can also help to enhance public confidence in the organisation while promoting accountability and transparency.

1.6 Carrying out DPIA would also be in line with the data protection regulatory landscape around the world. For examples, the European Union ("**EU**"), the United Kingdom, Indonesia and the Philippines have made DPIA a general legal obligation in certain circumstances. DPIA has also been expressly recommended by the regulators in many other jurisdictions such as Japan, South Korea, Singapore, New Zealand and Australia.

1.7 In view of the above, this Public Consultation Paper on DPIA Guideline ("**PCP**") seeks to gather public views and feedback regarding aspects that will be or should be addressed in the proposed DPIA Guideline.

PART 2: PROPOSED REQUIREMENTS FOR DPIA UNDER THE ACT 709

2.1 As an overview, Part 2 of this PCP is categorised as follows:

(a) Definition;
(b) Who to conduct DPIA;
(c) When to conduct DPIA;
(d) How to conduct DPIA;
(e) Notification to the Commissioner; and
(f) What to do after DPIA.

[A] Definition

2.2 **Background:** DPIA is not expressly referred to in the Act 709. It would be helpful to provide a definition of DPIA. However, the definition is only provided for illustrative purposes, rather than to set the scope of DPIA.

2.3 **Proposal:** DPIA is proposed to be defined as below, which is based on the definitions of DPIA in the UK and Singapore. The definition is proposed to accommodate evolving international standards on DPIA and similar exercises.

Definition

A Data Protection Impact Assessment (DPIA) is an assessment of the impact of planned processing operations on personal data protection, which may involve identifying, assessing and managing personal data protection risks based on the organisation's functions, requirements and processes.

Question 1

What are your views on the proposed scope of definition for DPIA? Would the definition be too broad, or should it be further restricted?

[B] Who to conduct DPIA

2.4 **Background:** The EU, the UK, Singapore and Indonesia legally requires data controllers to conduct DPIA in certain circumstances while the Philippines provides a wider approach requiring both data controllers and data processors to carry out DPIA.

2.5 For Malaysia, notwithstanding that the new section 12A of the Act 709 requires data processors to appoint DPO, it may not be necessary to mandate them to carry out DPIA. This is because by definition, data processors do not process personal data for their own purposes

and data controllers should be responsible to decide whether to proceed with a data processing operation. It may also be too difficult to require data processors to carry out DPIA in view of their limited legal obligations under the Act 709.

2.6 **Proposal:** It is proposed that **only data controllers** are subject to the DPIA requirement under the Act 709.

Question 2

What are your views on requiring only data controllers (and not data processors) to carry out DPIA?

[C] When to conduct DPIA

2.7 **Background:** A DPIA is generally conducted by a data controller to determine whether a processing[1] is **likely to result in a high risk to the protection of personal data for data subjects**.

2.8 From the identified jurisdictions, there are generally 2 approaches for data controllers to determine the likelihood of risk when assessing whether DPIA is required:

(a) qualitative factors (EU and the UK); and

(b) quantitative threshold (South Korea).

2.9 **Proposal:** Given that the DPIA concept is new in Malaysia, it is proposed that data controllers will be required to conduct a DPIA after adopting a 2-tier approach by considering quantitative thresholds and qualitative factors as below:

(i) First, the data controller will need to determine if the quantitative threshold is met. If the quantitative threshold is met, a DPIA will need to be conducted.

(ii) Second, even if the quantitative threshold is not met, the DPO will need to use his/her best judgment to consider the qualitative factors to determine whether a DPIA is required.

2.10 In assessing the quantitative threshold, **each** of the following circumstances **is deemed likely to result in a high risk** to the protection of personal data for data subjects:

[1] Note that "processing" is defined widely under the PDPA to mean "collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including *(a)* the organization, adaptation or alteration of personal data; *(b)* the retrieval, consultation or use of personal data; *(c)* the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or *(d)* the alignment, combination, correction, erasure or destruction of personal data".

(a) processing of **sensitive personal data**[2] is expected to involve more than **10,000 data subjects**;

(b) processing of **personal data for automated decision-making purposes** (to be defined by the Commissioner) is expected to involve more than **10,000 data subjects**; or

(c) processing of **personal data** is expected to involve more than **20,000 data subjects,**

(collectively referred to as the "**Quantitative Threshold**").

2.11 Note that, even if a processing does not meet any of the Quantitative Threshold, the **DPO is required to use his/her best judgment** to consider other qualitative factors in assessing whether a DPIA needs to be conducted, such as:

(a) potential legal or significant effects on data subjects (e.g., noticeable impact on individuals' legal status/rights or their financial status, health, reputation, access to services or other economic or social opportunities);

(b) systematic monitoring of publicly accessible area (e.g., CCTV with profiling capability);

(c) use of innovative technology (e.g., combining the use of fingerprint and face recognition for enhanced access control);

(d) denial or restriction of right of data subjects (e.g., using automated decision-making to approve and reject loan/insurance applications);

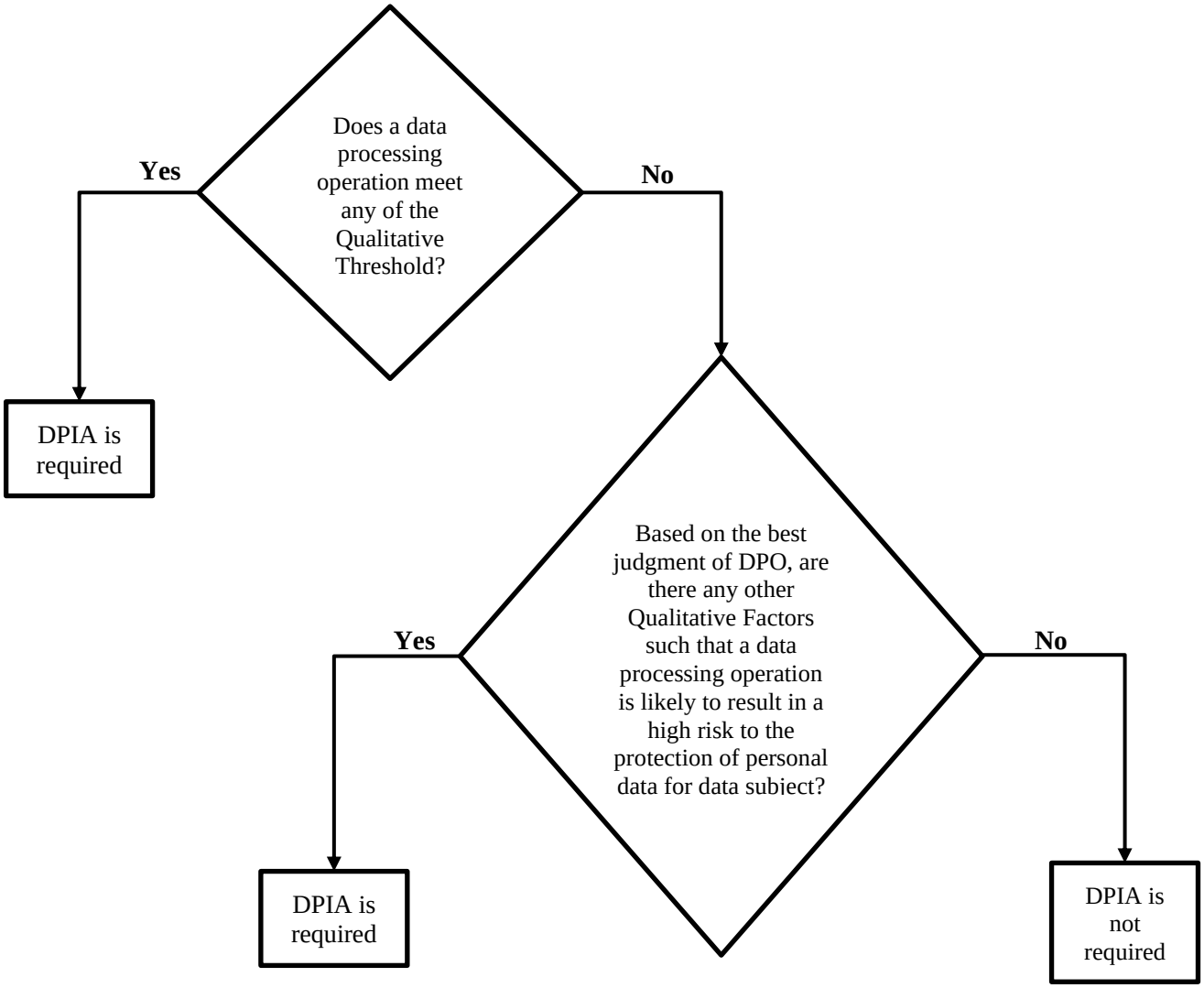
(e) tracking of data subjects' location or behaviour (e.g., eye-tracking to generate data to provide more tailored direct marketing); or

(f) targeting of children or other vulnerable individuals (e.g., processing their personal data to offer services to them).

(collectively referred to as the "**Qualitative Factors**").

[2] Under the PDPA, "sensitive personal data" includes "any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence". This definition will also include biometric data, which is defined as "any personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a person".

2.12 The thought process behind the proposal above can be illustrated below:



Example

(i) An organisation intends to store its customers' personal data with an external cloud service provider. Such proposed storage is a type of processing operation.

Quantitative Threshold

(ii) The DPO of the organisation should first consider whether such processing operation meets the Quantitative Threshold (i.e., it is deemed likely to result in a high risk to the protection of personal data for data subjects), by asking the following questions:

- Does the processing operation involve any sensitive personal data with more than 10,000 data subjects expected to be impacted?

- Is the processing operation for automated decision-making purposes and expected to involve more than 10,000 data subjects?

- Is the processing operation expected to involve more than 20,000 data subjects?

(iii) If **any** of the above 3 questions is responded with a '**yes**', the DPO will need to carry out DPIA on the processing operation.

(iv) If all of the above 3 questions are responded with a '**no**', the DPO should use his/her best judgment to consider the Qualitative Factors, in order to determine whether the processing operation is likely to result in a high risk to the protection of personal data for data subjects.

Qualitative Factors

(v) The relevant Qualitative Factors may include, for examples, the types of personal data involved (e.g., whether there may be potential legal or significant effects on data subjects) and the location of cloud service provider (e.g., if located outside of Malaysia, whether such place has data protection laws equivalent to the Act 709 to safeguard the personal data).

(vi) If the intended processing operation is likely to result in a high risk to the protection of personal data for data subjects in the DPO's best judgment, the DPO will need to conduct a DPIA.

(vii) On the contrary, if the DPO is of the view that the intended processing operation is unlikely to result in a high risk to the protection of personal data for data subjects, there is no need for the DPO to conduct a DPIA.

Question 3

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

(a) Based on the proposal in Paragraph 2.9, do you agree on adopting a 2-tier approach: Quantitative Threshold and Qualitative Factors in Malaysia? Please specify the reason and suggestion.

(b) What are your views on the use of a Quantitative Threshold to guide the assessment (instead of a purely Qualitative Factors) to determine the need to carry out DPIA?

(c) Do you consider the proposed figures in Paragraph 2.10 for the Quantitative Threshold to be appropriate figures to be considered likely to result in high risk for

the protection of personal data for data subjects? If your answer is no, please specify the reason.
For reference, South Korea requires government entities to carry out DPIA if e.g., it involves sensitive information or personally identifiable information of at least 50,000 data subjects for processing.

(d) What are your views on DPOs using their best judgment to assess whether to carry out DPIA based on the Qualitative Factors?

(e) Beside assessing the DPIA based on the Qualitative Factors in Paragraph 2.11, what other factors that can be considered / suggested?

[D] How to conduct DPIA

2.13 **Background**: The approach on how to conduct DPIA is more or less similar across many jurisdictions. It involves identifying, evaluating and addressing personal data protection risks, with proper documentation.

2.14 As an illustration, the EU requires DPIA to contain at least:

(a) a systematic description of the processing operations and the purposes of the processing including, where applicable, the legitimate interest pursued by the data controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the EU regulations taking into account the rights and legitimate interests of data subjects and other persons concerned.

2.15 **Proposal:** After considering the varying but broadly similar approaches across the identified jurisdictions, it is proposed for Malaysia to adopt a **5-step approach**, abbreviated as "DEICA", to analyse a data processing operation regarding the purposes, the specific risks and the measures to be taken.

(a) **Describe** the processing operations (including for examples the extent of personal data involved and the data flow) and the purposes of the processing;

Explanation

This may involve explaining the processing's:

- nature (i.e., what is planned with the personal data e.g., how to collect, store and use the data, who has access, to whom the data is shared with etc.);

- scope (i.e., what the processing covers e.g., the volume and variety of the personal data, the extent, frequency and duration of the processing, the number of data subjects involved, the geographical area covered, whether there is cross-border transfer etc.);

- context (i.e., the wider picture which may affect expectations and impact e.g., the nature of the relationship with the data subjects, any current issues of public concern etc.); and

- purposes (i.e., the reason why the organisation wants to process the personal data, which may include the intended outcome for data subjects and the expected benefits for the organisation and others).

(b) **Evaluate** the necessity and proportionality of the processing operation in relation to the purposes;

Explanation

This may involve considering:

- whether the organisation's plans actually help to achieve the intended purposes; and

- whether there is any other reasonable way to achieve the same result without the proposed processing or with lesser extent of processing (e.g., is cross-border transfer really necessary in the processing operation to achieve the intended purposes).

(c) **Identify** and analyse the specific risks on the protection of personal data for data subjects;

Explanation

This may involve considering the risk of breaching any personal data protection principles or other requirements under the Act 709, as well as the potential impact on data subjects and any harm the processing may cause e.g.:

- security risks (including sources of risk and the potential impact for each type of breach);

- inability to exercise rights;
- loss of control over the use of personal data;
- identity theft or fraud;
- financial loss;
- physical harm;
- loss of confidentiality;
- the country to which the data is transferred may not have adequate data and privacy protection law.

Further, the analysis of the specific risks identified should involve both the likelihood and severity of the possible harm. A risk matrix (sample below) may be used to determine the risk level for each specific risk identified.

Sample Risk Matrix		**Likelihood**		
		Remote	**Reasonably possible**	**More likely than not**
Severity	**Minimal impact**	Low risk	Low risk	Low risk
	Some impact	Low risk	Medium risk	High risk
	Serious harm	Low risk	High risk	High risk

As an illustration, if a processing operation has a specific risk of identity theft, the organisation should consider:

- the likelihood (e.g., has identity theft happened before to the organisation, or to its competitors in the same industry, or to anyone adopting similar processing operation); and
- the severity (e.g., what is the extent of the harm that may cause, based on for instance, the types of personal data involved in the processing operation (e.g., bank account numbers), the profile of data subjects (e.g., adults vs children),

to then assign a risk level (e.g., if the specific risk of identity theft is reasonably possible to happen and it may cause serious harm to the data subjects, then such specific risk is considered high risk, in which case there should be more robust measures to address such risk in the step 4 and/or may affect the overall residual risk level in the step 5).

(d) **Consider** measures to be taken to address the specific risks identified in order to safeguard the protection of personal data; and

Explanation

This may involve one or more of the following:

- not to collect certain types of data;
- reduce the frequency of processing or retention periods;
- take additional security measures;
- anonymise/pseudonymise certain sensitive data;
- use a different technology;
- incorporate additional contractual safeguards with the third party involved in the processing;
- conduct a cross-border data transfer assessment to determine whether the transfer is permitted under the Act 709 and/or the receiving country has adequate data protection and privacy law.

(e) **Assess** the overall residual risk level (e.g., high, medium, low) of the processing operation.

Explanation

This may involve considering the risk level assigned for each specific risk identified and the proposed measures to address the specific risks in order to determine the overall residual risk level.

Question 4

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

(a) What are your views on the proposed 5-step approach "DEICA" to carry out DPIA? Is It sufficient or are there other aspects to be considered?

(b)	***What specific guidance in your view should be provided in the DPIA Guideline in order to better assist the DPOs to discharge their responsibility to carry out DPIA effectively and systematically?***
(c)	***Is there a need for practical examples or templates to be provided to assist with the implementation of DPIA? If yes, please specify.***

[E] Notification to the Commissioner

2.16 **Background**: Submission of DPIA to regulator is required in jurisdictions e.g.:

(a) the EU and the UK – in the event of high risk; and

(b) Japan and South Korea – in all circumstances (though only government entities in certain circumstances are legally required to do DPIA).

2.17 Further, in the EU and the UK, data controllers undertaking a DPIA and determining that it is of high risk will need to consult the regulator prior to the processing and provide the following to the regulator:

(a) where applicable, the respective responsibilities of the data controller, joint data controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the law;

(d) where applicable, the contact details of the DPO; and

(e) any other information requested by the regulator.

2.18 **Proposal:** It is proposed that, **if the overall residual risk is assessed as high**, the data controllers will need to **notify the Commissioner** regarding the DPIA conducted and provide such information and documents as may be required by the Commissioner. However, it is not necessary to consult or obtain approval of the Commissioner in order to proceed with the processing operation.

2.19 In terms of the medium of notification to the Commissioner, it is proposed that an online portal (e.g., https://daftar.pdp.gov.my/) be provided, where the DPO can provide relevant information and upload relevant documents onto the portal.

Question 5

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

(a) What are your views on the proposal in Paragraph 2.18 regarding notification to the Commissioner, if the overall residual risk is assessed as high?

(b) Do you agree that notification of DPIA is sufficient without the need to obtain approval or consult with the Commissioner?

(c) What are your views on the information and documents to be provided to the Commissioner as part of the notification?

(d) What type of documents should be included to ensure transparency and effective monitoring without placing unnecessary administrative burden on the data controllers?

(e) What are your views on the proposal in Paragraph 2.19 regarding the DPIA notification medium to the Commissioner through an online portal?

(f) Is the approach in Paragraph 2.19 practical and sufficient, or do you suggest an alternative channel to make the DPIA notification process more efficient and accessible?

[F] What to do after DPIA

2.20 **Background**: Apart from notification to the regulator, some jurisdictions have introduced certain post-DPIA obligations. For example, the Philippines requires maintenance of proper records pertaining to the DPIA.

2.21 **Proposal**: It is proposed that, if the data controllers proceed with the processing operation after conducting the DPIA, they must do **all** of the following:

(a) implement the measures proposed in the DPIA to manage the specific risks identified;

(b) monitor developments which may impact the processing operations and the risks (e.g., modified purposes for processing, new vulnerabilities in the technology used) from time to time and address them accordingly;

(c) keep all DPIAs conducted and relevant documents in proper record for at least two (2) years and make them available upon request by the Commissioner.

<u>Question 6</u>

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

(a) What are your views on the proposed obligations post-DPIA?

(b) What specific guidance in your view should be provided in the DPIA Guideline in order to better assist the DPOs to discharge their obligations post-DPIA?

(c) What are your views on the proposed retention period of at least two (2) years for keeping the documentation relating to DPIA?