MINISTRY OF DIGITAL

PERSONAL DATA PROTECTION

GUIDELINE

# DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Version 1.0

Date of Issuance: 30 April 2026

DEPARTMENT OF PERSONAL DATA PROTECTION

Address:

DEPARTMENT OF PERSONAL DATA PROTECTION
Level 8, Galeria PjH, Jalan P4W, Persiaran Perdana
Precinct 4, Federal Government Administration Centre
62100 Putrajaya, Malaysia

## TABLE OF CONTENTS

## PART A: INTRODUCTION

### 1. Background

1.1 Section 12A of the Personal Data Protection Act 2010 ("**Act 709**") sets out the requirement for both the data controller and the data processor to appoint one or more Data Protection Officers ("**DPO**") to oversee their compliance with Act 709.

1.2 Pursuant to the Circular of Personal Data Protection Commissioner No. 1/2025 (Appointment of Data Protection Officer) and the Appointment of Data Protection Officer Guideline, one of the core responsibilities of a DPO is to support and advise on the carrying out of a Data Protection Impact Assessment ("**DPIA**").

1.3 This DPIA Guideline ("**Guideline**") provides practical guidance in relation to the carrying out of DPIA. Through this process, the organisations can systematically identify and manage risks associated with their personal data processing activities, ensuring that such activities comply with the requirements of Act 709.

1.4 Please note that examples provided in this Guideline are not intended to be exhaustive and are included solely for context illustration purposes.

1.5 This Guideline supplements and is to be read together with Act 709 and any other relevant legislative instrument(s) issued under Act 709, as may be amended from time to time. It This Guideline shall not be considered to override any other personal data protection-related laws and regulations in force.

### 2. Legal Provisions

2.1 This Guideline is issued by the Personal Data Protection Commissioner ("**Commissioner**") pursuant to the functions of the Commissioner under subsection 48(g) of Act 709. In accordance with subparagraph 5(1)(d) of the Circular of Commissioner of Data Protection No. 1/2025 (Appointment of Data Protection Officer), the Commissioner in this Guideline sets out the requirements in relation to the carrying out of DPIA.

## 3. Interpretation

3.1 Unless otherwise defined in this Guideline, the terms and expressions used herein shall have the same meanings assigned to them under Act 709 and any other relevant legislative instrument(s) issued under Act 709.

# PART B: PRE-DPIA

## 4. What is a DPIA

4.1 A DPIA is an assessment of the impact of a planned processing operation on personal data protection. It involves identifying, assessing, and managing personal data protection risks based on the organisation's functions, requirements, and processes of an organisation.

4.2 In essence, DPIA is a process designed to analyse and mitigate personal data protection risks.

## 5. Why Carry Out a DPIA

5.1 DPIA serves as a useful mechanism to assist organisations in ascertaining the risks associated with a processing operation. It enables the organisation to evaluate whether such risks are acceptable in the circumstances, when weighed against the purpose and nature of the processing operation. By identifying risks at an early stage, organisations can determine and implement appropriate risk treatment measures, including preventive and mitigative measures to manage these risks and to ensure compliance with the Act 709. This proactive approach ensures effective risk management and full compliance with Act 709.

5.2 The implementation of a DPIA assists organisations in fulfilling the adequacy requirements prevalent in the international personal data protection landscape. For instance, the European Union, the United Kingdom, Indonesia, the Philippines, and South Korea have established the DPIA as a mandatory legal obligation under specific circumstances. Furthermore, DPIAs are expressly recommended as best practices in numerous other jurisdictions, including Singapore, Japan, Australia, and New Zealand.

5.3 Carrying out a DPIA will enhances an organisation's accountability and transparency. By demonstrating a steadfast commitment to safeguarding personal data, organisations can significantly bolster public confidence and foster long-term trust in their data processing activities.

## 6. Who Is Responsible for Carrying Out a DPIA

6.1 The obligation to carry out a DPIA falls on the data controller. This is because, by definition, the data processor does not process personal data for its own purposes and the data controller shall be responsible in deciding whether to proceed with a processing operation and ensure that all risks are addressed.

6.2 Nevertheless, the data processor who is involved in the processing operation is expected to provide all reasonable and necessary assistance to the data controller in carrying out the DPIA. The data controller shall reinforce this expectation through clear contractual clauses or other appropriate methods.

### *Duty to carry out DPIA*

6.3 The ultimate responsibility for carrying out the DPIA and for any resulting decisions rests with the senior management of the data controller.

### *DPO vs DPIA Lead*

6.4 One of the core responsibilities of a DPO is to support the carrying out of DPIA. In this regard, the DPO shall provide the following support:

(a) identifying whether a DPIA needs to be carried out;

(b) providing advice in relation to the carrying out of DPIA and the implementation of risk mitigation measures; and

(c) developing DPIA templates or checklists customised for the data controller.

6.5 The DPO may not necessarily be the individual leading the carrying out of a DPIA. A DPIA Lead may either be the DPO, the project manager, or other personnel deemed appropriate by the data controller ("**DPIA Lead**").

6.6 The DPIA Lead is the key personnel in charge of planning and executing the DPIA. This includes consulting and gathering input from relevant stakeholders on matters such as details of the processing operation, identified risks or challenges, and appropriate risk treatment solutions and mitigation measures to address those risks.

***Stakeholder Engagement***

6.7 To ensure a DPIA is comprehensive and effective, it shall involve all relevant stakeholders from various functions of the organisation connected with the processing operation. These include, but are not limited to:

(a) project manager;
(b) IT department;
(c) legal department;
(d) any other subject matter experts;
(e) data processor; and
(f) relevant third parties as defined under the Act 709.

6.8 All relevant stakeholders are expected to assist the DPO and the DPIA Lead and provide appropriate input in completing the DPIA.

## 7. When to Carry Out DPIA

7.1 A data controller shall carry out a DPIA if the data controller foresees that a processing operation is likely to result in a high risk to the protection of personal data for the data subject.

7.2 In this regard, the data controller is required to follow a two-tier approach to determine the level of risk and assess whether a DPIA is required:

(a) First, the data controller shall determine if the **quantitative threshold** (as explained in paragraph 7.5) is met. If the quantitative threshold is met, a DPIA shall be carried out.

(b) Second, if the quantitative threshold is not met, the DPO shall exercise best judgment in considering the **qualitative factors** (as explained in paragraph 7.6) to determine whether a DPIA is required.

7.3 This Guideline does not derogate from the requirements set out under any other legal or regulatory instruments regarding the circumstances in which a DPIA needs to be carried out. Where there is an overriding obligation imposed by those other instruments, that broader requirement shall apply.

7.4 In cases where it is not obvious whether a DPIA is required, it is prudent for the data controller to carry out a DPIA nonetheless as a best practice, as it remains a useful tool for building trust with the data subject, managing personal data protection risks, and facilitating compliance with the Act 709.

***Quantitative Threshold***

7.5 The following circumstances are deemed likely to result in a high risk to the protection of personal data for the data subject, thereby triggering the requirement to carry out a DPIA:

(a) processing of personal data expected to involve more than 20,000 data subjects; or

(b) processing of sensitive personal data, including financial information data, expected to involve more than 10,000 data subjects.

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

***Qualitative Factors***

7.6 If the processing does not meet any of the Quantitative Thresholds, the DPO is required to exercise best judgment in considering other qualitative factors that are likely to result in a high risk to the protection of personal data for the data subject, such that a DPIA is required to be carried out. It is emphasised that these qualitative factors are neither exhaustive nor exclusive and include but are not limited to, the following:

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

**Examples:**

**(1) Example 1: Processing of sensitive personal data that may significantly affect a data subject's access to insurance**

**Situation:** An insurance company collects and processes health-related information, such as medical history or data obtained from fitness tracking applications, to determine a data subject's insurance eligibility, set premium rates or coverage approval.

**Why DPIA is required:** The data controller shall conduct a DPIA because the processing involves sensitive personal data and potentially involves automated decision-making that has a significant impact on the data subject's access to insurance services.

**(2) Example 2: Processing of personal financial data that may significantly affect a data subject's access to loan facilities**

**Situation:** A financial institution uses an automated credit scoring system to assess loan or credit applications. The system automatically approves or rejects an application without human review, resulting in an immediate impact on the data subject's credit score, financial standing, and access to financial services.

**Why DPIA is required:** The processing involves automated decision-making based on personal and financial data, which may have a direct and significant effect on the data subject's economic rights and opportunities. Therefore, the data controller is required to carry out a DPIA.

(b) systematic monitoring of the data subject;

**Examples:**

**(1) Example 1: Systematic monitoring of individuals in a commercial setting**

**Situation:** A retail chain uses facial recognition technology in all its stores to identify repeat customers enrolled in its loyalty programme. When the data subject enters an outlet, the system automatically matches the data subject's facial image against stored records to provide personalised discounts based on shopping history.

**Why DPIA is required:** Although the purpose is to enhance customer experience and marketing efficiency, the processing involves systematic monitoring of the data subject in a commercial setting and the use of biometric data (facial features) for identification. Such processing may pose a high risk of misidentification, profiling or intrusion into the privacy of the data subject. Accordingly, prior to the implementation of the facial recognition technology, the data controller is required to carry out a DPIA.

**(2) Example 2: Continuous tracking of the data subject's location and behaviour linked to commercial transactions**

**Situation:** A food delivery company offers an in-app loyalty feature that tracks the data subject's geolocation data when the app is opened or when orders are placed. The system logs the delivery address, frequently patronised food vendors, time spent on the application and browsing behaviour. The system cross-references this information with past purchase records to identify behavioural patterns such as spending habits, meal timing and preferred food vendors. The company uses these insights to deliver targeted advertisements, and location-based promotions, thereby influencing the data subject's purchasing decisions and marketing outcomes.

**Why DPIA is required:** The processing involves continuous tracking of the data subject's location and behaviour linked to commercial transactions. Such systematic monitoring and profiling activities are likely to result in a high risk to the protection of personal data. Therefore, the data controller is required to carry out a DPIA.

(c) use of innovative technologies, namely technologies that involve a new or significantly improved product (goods or services), a new process, a new marketing method, a new organisational method in business practices, or a new workplace organisation or external relations;

**Examples:**

**(1) Example 1: Enhancing Business Processes via Innovative Technology**

**Situation:** A financial institution operates a mobile banking application that enables customers to perform commercial transactions such as fund transfers, bill payments and online purchases using biometric fingerprint authentication. The data controller subsequently decides to enhance this process by incorporating Artificial Intelligence-driven biometric authentication features, such as facial recognition to provide an additional layer of security.

**Why DPIA is required:** The processing involves technology that is new to the organisation. The transition to facial recognition increases the volume and complexity of sensitive personal data being processed. This change may pose a significant risk to the privacy of the data subject due to the increased use of sensitive personal data. Therefore, the data controller is required to carry out a DPIA.

**(2) Example 2: Innovative Technology in Workplace Practices**

**Situation:** An organisation currently uses manual methods to monitor employee performance. The data controller has decided to adopt an Artificial Intelligence (AI) system to automate performance monitoring. The AI system generates performance scores and behavioural summaries, which are subsequently used as the primary basis for decisions regarding promotion, reward or disciplinary decisions.

**Why DPIA is required:** The processing involves the implementation of technology that is new to the organisation's operational environment. The transition to automated monitoring may significantly affect the data subject's employment rights, professional reputation and privacy. Therefore, the data controller is required to carry out a DPIA.

(d) denial or restriction of rights of the data subject;

**Examples:**

**(1) Example 1: Denial or restriction of access to services**

**Situation:** An e-hailing service provider requires the data subject to consent to continuous behavioural tracking, such as real-time location monitoring, trip patterns and in-app interactions, as a mandatory condition for accessing its services. A data subject who declines to consent may be denied access to the services entirely (for example, unable to book a ride) or may face specific restrictions (such as being ineligible for discounts or promotional offers).

**Why DPIA is required:** This practice involves the denial or restriction of the data subject's rights, particularly the freedom to withhold or withdraw consent without detriment. Accordingly, the data controller is required to carry out a DPIA.

**(2) Example 2: Systemic restriction the right of access**

**Situation:** An e-commerce company enables the data subject to make purchases via its mobile application. However, when the data subject requests access to his personal data, such as purchase history or account details, the application does not provide a direct mechanism for submitting such a request. Instead, the data subject is redirected to an external e-mail address or a telephone number to submit the request.

**Why DPIA is required:** This practice creates administrative hurdles that deter the data subject from exercising his right to access personal data. Since this involves a systemic restriction on the fundamental rights of the data subject, the data controller is required to carry out a DPIA.

(e) tracking of the data subject's location or behaviour;

**Examples:**

**(1) Example 1: Continuous tracking through a retail app**

**Situation:** A retail company uses a mobile application to continuously tracks the data subject's geolocation, store movement paths and dwell time at specific aisles. The personal data is used to analyse the data subject's behaviour, optimise store layout and deliver targeted advertisements or promotions based on real-time movement patterns.

**Why DPIA is required:** Since the processing involves regular and systematic tracking of the data subject's location and behaviour, the data controller is required to carry out a DPIA.

**(2) Example 2: Online click-path analytics**

**Situation:** An e-commerce platform tracks the data subject's online behaviour such as browsing history, clicks, time spent on pages and purchase activity, to predict buying intent, personalise prices and deliver targeted advertisements.

**Why DPIA is required:** The processing involves systematic and continuous monitoring of data subject's behaviour for commercial and profiling purposes. This may significantly affect data subject's rights and accordingly, the data controller is required to carry out a DPIA.

(f) targeting of children or vulnerable individuals; and

**Example:**

**Processing of children's personal data for advertising purposes**

**Situation:** An educational institution through its technology platform, collects children's personal data and intends to publish advertisements within the platform.

**Why DPIA is required:** The processing involves children's personal data and profiling activities, particularly for advertising purposes. This may give rise to risks regarding the protection of children's rights and the potential commercial targeting of minors. Therefore, the data controller is required to carry out a DPIA.

(g) automated decision-making and profiling that pose a high risk to the data subject.

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

7.7 DPOs shall exercise their best judgment in considering the Qualitative Factors, which may include factors that are not expressly set out above, to determine whether a processing operation is likely to result in a high risk to the protection of personal data for the data subject.

**Illustration: Determining the Necessity of Carrying Out a DPIA**

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

***Quantitative Threshold***

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

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

b) Is the processing operation of sensitive personal data, including financial information, expected to involve more than 10,000 data subjects?

If **either** of the above is answered '**Yes**', the DPIA Lead is required to carry out DPIA on the processing operation.

(iii) If **both** of the above are answered '**No**', the DPO, upon consultation with the DPIA Lead, shall exercise best judgement in considering the **Qualitative Factors** to determine whether the processing operation is likely to result in a high risk to the protection of personal data for the data subject.

***Qualitative Factors***

(iv) The relevant Qualitative Factors may include, for example:

a) the types of personal data involved (e.g., whether the processing may lead to potential legal or significant effects on the data subject); and

b) the location of cloud service provider (e.g., if the provider is located outside of Malaysia, whether such place has data protection laws equivalent to the Act 709 to safeguard the personal data).

(v) If, in the DPO's best judgment, the processing operation is likely to result in a high risk to the protection of personal data for the data subject, the DPIA Lead is required to carry out a DPIA.

(vi) If the DPO is of the view that the processing operation is unlikely to result in a high risk to the protection of personal data for the data subject, the DPO may advise that carrying out a DPIA to be done as a best practice.

## PART C: CARRYING OUT A DPIA

### 8. How to Carry Out a DPIA

8.1 A data controller is expected to adopt a five-step approach, which are Describe, Evaluate, Identify, Consider and Assess or better known as its abbreviation, DEICA ("**DEICA**"), to analyse a processing operation in relation to its purposes, the specific risks and the measures to be taken:

(a) **Step 1: Describe** – Describe the processing operations (including the extent of personal data involved and the data flow) and the purposes of the processing;

**Explanation:**

This step involves describing the processing in terms of the following aspects:

(i) **Nature:** What is planned with the personal data. (e.g., how the personal data will be collected, stored, used, accessed and disclosed with relevant parties);

(ii) **Scope:** 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 and whether there is cross border transfer);

(iii) **Context:** The wider picture that may affect expectations and impact. (e.g., the nature of the relationship with the data subject and any current issues of public concern); and

(iv) **Purposes:** The reason why the organisation wants to process the personal data, which may include the intended outcome for the data subject and the expected benefits for the organisation.

(b) **Step 2: Evaluate** – Evaluate the compliance, necessity, and proportionality of the processing operation in relation to its purposes;

**Explanation:**

This may involve considering:

(i) whether the organisation's plans actually help to achieve the intended purposes; and

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

(c) **Step 3: Identify** – Identify and analyse the specific risks to the protection of personal data of the data subject;

**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 the data subject and any harm that the processing may cause, for example:

(i) security risks (including sources of risk and the potential impact for each type of breach);
(ii) inability to exercise data subject's rights;
(iii) loss of control over the use of personal data;
(iv) identity theft or fraud;
(v) financial loss;
(vi) physical harm;
(vii) loss of confidentiality; and

(viii) inadequate privacy and data protection laws in the country to which the personal data is transferred.

The analysis of the specific risks identified shall consider both the **Likelihood** and **Impact** of the possible harm. A **3 x 3 Risk Matrix** (as shown below) is used to determine the risk level for each specific risk. The risk score is derived by multiplying the Likelihood score by the Impact score.

1. **Risk Matrix (3 x 3)**

   The table below is a sample 3 x 3 Risk Matrix for the calculation of risk levels. Each possible harm's risk is calculated by multiplying the Likelihood with the Impact of the possible harm.

| **Risk Matrix** | | **Likelihood** | | |
|---|---|---|---|---|
| | | **Low (1)** | **Medium (2)** | **High (3)** |
| **Impact** | **High (3)** | Medium (3) | High (6) | High (9) |
| | **Medium (2)** | Low (2) | Medium (4) | High (6) |
| | **Low (1)** | Low (1) | Low (2) | Medium (3) |

2. **Definition of Criteria**

   a) **Likelihood**

   Likelihood assesses the probability or chance of a risk event (e.g., data breach, accidental disclosure, unauthorised access, or loss of personal data) occurring within a given timeframe or operational context.

| **Likelihood** | **Criteria** |
|---|---|
| **Low (1)** | The event is unlikely or has a remote chance of occurring. Existing controls or systems are in place and are adequate to protect the data subject. |

| | |
|---|---|
| **Medium (2)** | The event is possible or is known to occur in the specific industry. Controls or systems are in place but may have limitations or weaknesses. |
| **High (3)** | The event is highly likely to occur or has occurred previously. Controls or systems have limitations or weaknesses and have significant vulnerabilities. |

**b) Impact**

Impact refers to the seriousness of the potential harm to the data subject if the risk materialises. It focuses on whether the processing is likely to result in a high risk to the protection of personal data for the data subject.

| Impact | Criteria |
|---|---|
| **Low (1)** | Unlikely to result in a material risk. The data involved is non-sensitive, and any breach would cause minimal inconvenience with no significant impact on the data subject's rights or interests. |
| **Medium (2)** | Likely to result in a risk. The processing may cause material but not irreversible harm, such as social embarrassment, minor financial loss, emotional distress, or limited loss of control. |
| **High (3)** | Likely to result in a high risk to the protection of personal data for the data subject. The harm may be significant or irreversible, including substantial financial loss, identity theft, discrimination, or reputational damage. |

**3. Risk Response and Risk Treatment**

| Risk Score | Level | Action Required |
|---|---|---|
| **1-2** | **Low** | **Monitor** – Risk is manageable. Continue monitoring through existing controls and standard operating procedures. |
| **3-4** | **Medium** | **Mitigate** – Strengthen mitigation measures. Implement additional technical and/or organisational controls to reduce the likelihood or impact. |
| **6-9** | **High** | **Mandatory Action** – Likely to result in a high risk to the data subject. A DPIA is required. Robust risk treatment measures shall be implemented. |

**Illustration: Risk Assessment for Identity Theft**

The following example demonstrates how a specific risk is identified and analysed.

As an illustration, if a processing operation poses a specific risk of identity theft, the data controller shall consider:

(i) **The likelihood** (e.g., whether identity theft has previously occurred within the organisation, among its competitors in the same industry, or in similar processing operations);

(ii) **The impact** (e.g., taking into account the extent of the harm that may be caused, based on the types of personal data involved such as bank account numbers and the profile of the data subject);

(iii) **Assigning a risk level** (e.g., if the specific risk of identity theft is assessed as "Medium"(2) in likelihood and "High"(3) in impact severity, such risk would be considered "High Risk"(6).

In such circumstances, more robust mitigation measures shall be implemented in Step 4 (Consider), which may subsequently affect the overall residual risk level in Step 5 (Assess)).

(d) **Step 4: Consider** – Consider measures to be taken to address the specific risks identified to safeguard the protection of personal data; and

**Explanation:**

This may involve any of the following:

(i) not to collect certain types of data;

(ii) reduce the frequency of processing or shorten retention periods;

(iii) implement additional security measures;

(iv) anonymise or pseudonymise certain personal data;

(v) use a different technology;

(vi) incorporate additional contractual safeguards with the third party involved in the processing; and

(vii) conduct a Transfer Impact Assessment (TIA) to determine whether the transfer is permitted under Act 709 and/or the receiving country has adequate data protection and privacy laws.

(e) **Step 5: Assess** – 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 those specific risks, to determine the overall residual risk level.

8.2 To illustrate how the DEICA procedure may be applied, a DPIA Template is provided under **Annex A** as a reference. The suggested DPIA Template is intended for guidance, and usage of its contents is discretionary. The data controller may adapt this Template to suit its specific

needs or circumstances, develop its own template (adapted from this Template), or develop any accompanying checklist, so long as it is aligned with this Guideline.

## PART D: POST-DPIA

### 9. Report to Senior Management

9.1 Upon completion of the DPIA, where the overall residual risk level is assessed as “High”, the findings shall be reported to the senior management of the organisation. Unless otherwise determined by the organisation, all risks, regardless of their level, shall also be reported to senior management to ensure that it remains fully informed of all identified risks.

9.2 The senior management shall consider the DPIA findings and provide input in connection with the processing operation. This may include:

(a) accepting the overall residual risk level arising from the processing operation;

(b) deciding on any additional mitigation measures to manage the risks; and

(c) allocating appropriate resources for implementing the risk mitigation measures.

### 10. Implementation of Risk Mitigation Measures

10.1 Once a decision has been made to proceed with the processing operation, the identified risk mitigation measures shall be implemented accordingly to address and manage the specific risks identified in the DPIA.

10.2 The DPIA Lead is the key personnel responsible for overseeing the implementation of the risk mitigation measures. The DPO shall provide support and advice on such implementation in line with the organisation's data protection policies, industry best practices, and Act 709. The ultimate responsibility for implementing the risk mitigation measures, however, rests with the senior management of the data controller.

## 11. Publication, Validity and Monitoring

11.1 To promote transparency and accountability, the data controller may consider publishing its DPIA to foster trust in its personal data processing activities. To protect commercially sensitive information or manage other data security risks (including those involving personal data), the published DPIA may be redacted. Alternatively, a summary of the DPIA may be published.

11.2 A completed DPIA is **valid for a period of two (2) years** from its date of completion. Upon **expiry of that period**, **a refreshed DPIA** shall be carried out.

11.3 In any event, a DPIA is not a one-off activity but requires continuous monitoring and periodic review. Notwithstanding the validity period, and throughout the duration of the processing operation, the DPIA Lead shall monitor developments that may affect the processing operation, the risks identified and the risk mitigation measures adopted (e.g., changes to the purposes of processing or newly identified vulnerabilities in the technology used). The DPIA Lead shall address such developments accordingly to ensure the ongoing protection of the data subject.

## 12. Record-Keeping

12.1 In any event, the DPIA shall be carried and all relevant documentation shall be properly maintained for at least two (2) years from the cessation of the processing operation. For example, if the processing operation lasts for five (5) years, the DPIA and its relevant records shall be retained for two (2) years from the cessation of processing operation. Accordingly, the record-keeping period will be at least seven (7) years.

12.2 Such records shall be made available for inspection upon request by the Commissioner.

## ANNEX A: DPIA TEMPLATE

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| **<u>Pre-DPIA</u>: Determine whether a DPIA is required** | | | |
| **Planned processing** | | | |
| 1. | What is the planned processing operation of personal data about? | *Please provide a brief explanation*<br><br>("**Planned Processing**") | <u>Response example</u>: *Engaging a human resource service provider, Z, to analyse customers' survey responses and store their personal data in Singapore.* |
| **Determinants** | | | |
| 2. | Does the Planned Processing involve personal data expected to exceed 20,000 data subjects? | ☐ Yes ☐ No<br><br>Elaboration: *Please provide* | Please tick the applicable checkbox for each question.<br><br><u>Response examples for the elaboration</u>:<br><br>i. The Planned Processing involves the processing of personal data exceeding 20,000 data subjects; or<br><br>ii. The Planned Processing involves the processing of sensitive personal data, including financial information, exceeding 10,000 data subjects. |
| 3. | Does the Planned Processing involve sensitive personal data including financial data, expected to exceed 10,000 data subjects? | ☐ Yes ☐ No<br><br>Elaboration: *Please provide* | |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| 4. | Does the Planned Processing involve **any Qualitative Factors** that will likely result in a high risk to the protection of personal data for the data subject, such that, in the DPO's judgment **a DPIA shall be carried out to further assess the risks?** | ☐ Potential legal or significant effects on the data subject<br><br>☐ Systematic monitoring of the data subject<br><br>☐ Use of innovative technology<br><br>☐ Denial or restriction of the rights of data subject<br><br>☐ Tracking of the data subject's location or behaviour<br><br>☐ Targeting of children or other vulnerable individuals<br><br>☐ Automated decision-making and profiling that pose a high risk to the data subject<br><br>☐ Any other factors necessitating the carrying out of a DPIA: *Please elaborate*<br><br>☐ None of the above applies. | Please tick all applicable checkbox(es).<br><br>Examples:<br><br>(i) Potential legal or significant effects on the data subject (e.g., noticeable impact on the data subject's legal status or rights, financial status, health, reputation, access to services or other economic or social opportunities).<br><br>(ii) Systematic monitoring of the data subject (*e.g., systematic monitoring of individuals in a commercial setting).*<br><br>(iii) Use of innovative technology (*e.g., significantly improved business process through innovative technology).*<br><br>(iv) Denial or restriction of the right of the data subject (*e.g., systemic restriction to the right of access).*<br><br>(v) Tracking of data subject's location or behaviour *(e.g., online click-path analytics).*<br><br>(vi) Targeting of children or other vulnerable individuals (*e.g., processing their personal data to offer services to them).*<br><br>(vii) Automated decision-making and profiling that pose a high risk to the data subject. |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | | | (viii) Any other factors necessitating the carrying out of a DPIA (*e.g., risk of physical harm to the data subject in the event of data breach).* |
| **Outcome** | | | |
| 5. | Does the Planned Processing require a DPIA? | ☐ Yes ☐ No | Please tick "No", if:<br>(i) questions 2 and 3 are responded with "No"; **AND**<br>(ii) question 4 is responded with "None of the above applies".<br>Otherwise, please tick "Yes" and proceed to answer the questions below. |
| **DPIA: Carry out the five steps under DEICA** | | | |
| **D – Describe the Planned Processing** | | | |
| 6. | What is the **nature** of the Planned Processing? | *Please describe* | Illustration and examples: The description shall address what is planned to be done with the personal data:<br>(iii) How the data will be collected;<br>(iv) How the data will be stored;<br>(v) How the data will be used;<br>(vi) Who will have access to the data;<br>(vii) To whom the data will be disclosed; |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | | | (viii) Whether any data processor will be engaged;<br>(ix) The applicable retention period(s);<br>(x) Security measures to be implemented. |
| 7. | What is the **scope** of the Planned Processing? | *Please describe* | Illustration and examples: The description shall address what the processing covers, for example:<br>(i) Volume and variety of the data;<br>(ii) Extent, frequency, and duration of the processing;<br>(iii) Number of data subjects involved;<br>(iv) Countries or jurisdictions outside Malaysia involved in the processing. |
| 8. | What is the **context** of the Planned Processing? | *Please describe* | Illustration and examples: The wider picture, including internal and external circumstances that may affect expectations and impact. Consider the following, where applicable:<br>(i) Source of the personal data;<br>(ii) Nature of the relationship with the data subject;<br>(iii) The extent of control the data subject retains over the personal data; |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | | | (iv) Likely expectations the data subject has of the processing;<br>(v) Previous experience with this type of processing;<br>(vi) Current issues of public concern or sensitivity relevant to the processing. |
| 9. | What are the **purposes** behind the Planned Processing? | *Please describe*<br>("**Purposes**") | Illustration: The underlying reason(s) for the processing and the intended outcome(s) for the organisation. |
| **E – Evaluate compliance, necessity and proportionality** | | | |
| 10. | What is the applicable legal basis under Section 6 of the Act 709 for **processing personal data** under the Planned Processing? | ☐ Consent of the data subject<br>☐ Another legal basis under subsection 6(2) of the Act 709: *Please state the applicable legal basis*<br>☐ Exempted under Section 45 of the Act 709: *Please state which exemption* | Please tick the applicable checkbox.<br>Examples of legal basis under subsection 6(2) of the Act 709:<br>(i) Necessary for the performance of a contract to which the data subject is a party;<br>(ii) Necessary for compliance with any legal obligation to which the data controller is the subject (other than an obligation imposed by a contract);<br>(iii) Necessary in order to protect the vital interests (i.e., matters relating to life, death or security) of the data subject;<br>(iv) Necessary for the administration of justice. |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| 11. | If the Planned Processing involves **processing sensitive personal data**, what is the applicable legal basis under Section 40 of the Act 709? | ☐ Not applicable<br><br>☐ Explicit consent of the data subject<br><br>☐ Another legal basis under subsection 40(1) of the Act 709: *Please state the applicable legal basis*<br><br>☐ Exempted under Section 45 of the Act 709: *Please state the applicable exemption* | Please tick the applicable checkbox.<br><br>Examples of legal basis under subsection 40(1) of the Act 709:<br><br>(i) Necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;<br><br>(ii) Necessary for the purpose of obtaining legal advice. |
| 12. | If the Planned Processing involves **disclosing personal data to any third party**, what is the applicable legal basis under Section 39 of the Act 709? | ☐ Not applicable<br><br>☐ Consent of the data subject<br><br>☐ Another legal basis under Section 39 of the Act 709: *Please state the applicable legal basis*<br><br>☐ Exempted under Section 45 of the Act 709: *Please state the applicable exemption* | Please tick the applicable checkbox.<br><br>Examples of legal basis under Section 39 of the Act 709:<br><br>(i) Necessary for the purpose of preventing or detecting a crime or for the purpose of investigations;<br><br>(ii) Required or authorised by or under any law or by the order of a court. |
| 13. | If the Planned Processing involves **transferring personal data to a place outside Malaysia**, what is the applicable legal basis under Section 129 of the Act 709? | ☐ Not applicable<br><br>☐ The recipient country has a law substantially similar to the Act 709 | Please tick the applicable checkbox.<br><br>Examples of legal basis under subsection 129(3) of the Act 709:<br><br>(i) Necessary for the performance of a contract between the data subject and the data controller; |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | | ☐ The recipient country or jurisdiction ensures an adequate level of protection equivalent to the Act 709.<br><br>☐ Consent of the data subject to the transfer<br><br>☐ Another legal basis under subsection 129(3) of the Act 709: *Please state the applicable legal basis* | (ii) For the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;<br><br>(iii) Necessary in order to protect the vital interests (i.e., matters relating to life, death or security) of the data subject. |
| 14. | Does the data controller belong to a class of data controllers required to be registered under Act 709? | ☐ Yes ☐ No | Please tick the applicable checkbox.<br><br>If "No", please refer to the General Code of Practice, where applicable.<br><br>If "Yes", proceed to Question 15. |
| 15. | Is the Planned Processing subject to compliance with any applicable **Code of Practice** issued by the Commissioner? | ☐ Yes ☐ No<br><br>*Please specify the applicable Code of Practice*<br><br>("**Code of Practice**") | Please tick the applicable checkbox.<br><br>Examples of Codes of Practice issued by the Commissioner include:<br><br>(i) Personal Data Protection Code of Practice for the Malaysia Aviation Sector;<br><br>(ii) Personal Data Protection Code of Practice for the Banking and Financial Institutions Sector;<br><br>(iii) Personal Data Protection Code of Practices for the Insurance and Takaful Industry in Malaysia; |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | | | (iv) Personal Data Protection Code of Practice for the Communications Sector;<br><br>(v) Personal Data Protection Code of Practice for the Utilities Sector (Electricity);<br><br>(vi) Personal Data Protection Code of Practice for the Utilities Sector (Water);<br><br>(vii) Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry. |
| 16. | What are the **requirements** under the applicable Code of Practice which governs the Planned Processing, and how is compliance ensured? | Elaboration: *Please provide* | Illustration:<br><br>The data controller shall identify the specific requirements set out in the Code of Practice with regards to the Planned Processing. This includes any standards, safeguards and sector-specific obligations. Next, the data controller shall assess and document how the Planned Processing complies with said requirements. |
| 17. | Is it **necessary** to adopt the Planned Processing in order to achieve the Purposes? | ☐ Yes ☐ No<br><br>Elaboration: *Please provide* | Please tick the applicable checkbox.<br><br>Illustration and examples: Consider whether there is any other reasonable way to achieve the Purposes **without** adopting the Planned Processing. For example:<br><br>(i) Leveraging on existing means to achieve the Purposes; |

<table>
<tr><th>No.</th><th>Questions</th><th>Responses</th><th>Guidance Notes</th></tr>
<tr><td></td><td></td><td></td><td>(ii) Determining whether anonymising personal data would still enable the Purposes to be achieved.</td></tr>
<tr><td>18.</td><td>Is it proportionate to adopt the Planned Processing to achieve the Purposes?</td><td>☐ Yes ☐ No<br><br>Elaboration: Please provide</td><td>Please tick the applicable checkbox.<br><br><u>Illustration and examples</u>: Consider whether there is any other reasonable way to achieve the Purposes through the Planned Processing, but via a lesser extent of processing. For example:<br><br>(i) Collecting fewer types of personal data from the data subject;<br><br>(ii) Reducing the duration of processing or retention;<br><br>(iii) Reducing the extent of or removing disclosure of personal data to a third party.</td></tr>
<tr><td colspan="4">I – Identify and analyse risks</td></tr>
<tr><td colspan="4">Please use this risk matrix to determine the risk level for each of Questions 19 to 29.<br><br>
<table>
<tr><th colspan="2" rowspan="2">Risk Matrix</th><th colspan="3">Likelihood</th></tr>
<tr><th>Low (1)</th><th>Medium (2)</th><th>High (3)</th></tr>
<tr><td>I<br>m</td><td>High (3)</td><td>Medium (3)</td><td>High (6)</td><td>High (9)</td></tr>
</table>
</td></tr>
</table>

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | **p a c t** | **Medium (2)** | Low (2) | Medium (4) | High (6) |
| | | **Low (1)** | Low (1) | Low (2) | Medium (3) |

| | | | |
|---|---|---|---|
| 19. | What is the extent of risk of the Planned Processing violating the **General Principle** under Section 6 of the Act 709? | ☐ Low ☐ Medium ☐ High<br><br>Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | <u>Examples of consideration</u>:<br><br>(i) Whether the Planned Processing is for a lawful purpose directly related to an activity of the data controller.<br><br>(ii) Whether processing is necessary for or directly related to that purpose.<br><br>(iii) Whether the personal data is adequate but not excessive in relation to that purpose. |
| 20. | What is the extent of risk of the Planned Processing violating the **Notice and Choice Principle** under Section 7 of the Act 709? | ☐ Low ☐ Medium ☐ High<br><br>Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | <u>Examples of consideration</u>:<br><br>(i) Whether the existing written notice provided to the data subject is sufficient to cover the Planned Processing.<br><br>(ii) When was the written notice provided or when will the written notice be provided to the data subject? |
| 21. | What is the extent of risk of the Planned Processing violating the **Disclosure** | ☐ Low ☐ Medium ☐ High | <u>Example of consideration</u>:<br><br>Whether the disclosure of personal data is for any other purpose than the purpose for which the personal data was |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | **Principle** under Section 8 of the Act 709? | Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | to be disclosed at the time of collection or a purpose directly related to the purpose at the time of collection. |
| 22. | What is the extent of risk of the Planned Processing violating the **Security Principle** under Section 9 of the Act 709? | ☐ Low ☐ Medium ☐ High<br><br>Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | Examples of consideration:<br><br>(i) The risks of loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction of personal data.<br><br>(ii) The practical steps taken to protect personal data from those risks. |
| 23. | What is the extent of risk of the Planned Processing violating the **Retention Principle** under Section 10 of the Act 709? | ☐ Low ☐ Medium ☐ High<br><br>Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | Examples of consideration:<br><br>(i) Whether the personal data will be kept no longer than is necessary for the fulfilment of the Purposes.<br><br>(ii) Whether the personal data will be permanently deleted once it is no longer required for the Purposes. |
| 24. | What is the extent of risk of the Planned Processing violating the **Data Integrity Principle** under Section 11 of the Act 709? | ☐ Low ☐ Medium ☐ High<br><br>Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | Examples of consideration:<br><br>*Whether reasonable steps will be taken to ensure that the personal data is:*<br><br>(i) Accurate;<br><br>(ii) Complete;<br><br>(iii) Not misleading; and<br><br>(iv) Kept up-to-date. |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | | | |
| 25. | What is the extent of risk of the Planned Processing violating the **Access Principle** under Section 12 of the Act 709? | ☐ Low ☐ Medium ☐ High<br><br>Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | Examples of consideration:<br><br>(i) Whether the data subject will be able to access their personal data under the Planned Processing to enable any applicable correction.<br><br>(ii) Whether the Planned Processing will affect the ability to comply with the requirements under Sections 30 to 37 of the Act 709. |
| 26. | What is the extent of risk of the Planned Processing violating **other data subject rights** under the Act 709, particularly Sections 38, 42, 43 and 43A? | ☐ Low ☐ Medium ☐ High<br><br>Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | Examples of consideration:<br><br>Whether the data subject will be able to:<br><br>(i) Withdraw consent.<br><br>(ii) Prevent processing likely to cause damage or distress.<br><br>(iii) Prevent processing for direct marketing.<br><br>(iv) Exercise the right to personal data portability. |
| 27. | What is the extent of risk of the Planned Processing violating **other requirements** under the Act 709, particularly Sections 12A, 12B, 25(2) and 130? | ☐ Low ☐ Medium ☐ High<br><br>Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | Examples of consideration:<br><br>(i) Whether the Planned Processing necessitates the need to appoint additional DPOs (e.g., due to an increase in the processing of personal data or systematic monitoring). |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | | | (ii) Whether the Planned Processing affects the ability to comply with the mandatory data breach notification requirements.<br><br>(iii) Whether the Planned Processing results in a breach of any provisions under the applicable Code of Practice.<br><br>(iv) Whether the Planned Processing constitutes an unlawful collection of personal data. |
| 28. | What is the extent of risk of the Planned Processing breaching the **specific requirements** of the applicable Code of Practice? | ☐ Low ☐ Medium ☐ High<br><br>Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | <u>Examples of consideration</u>:<br><br>(i) Whether additional safeguards, technical measures, or organisational controls required under the applicable Code of Practice have been implemented (e.g., encryption, data security safeguards).<br><br>(ii) Whether there are any gaps between the Planned Processing and the standards or best practices prescribed under the applicable Code of Practice.<br><br>(iii) Whether appropriate processes are in place to enable the data subject to exercise rights in accordance with the specific requirements set out in the applicable Code of Practice. |
| 29. | What are the **potential impacts and harms** on the data subject that the Planned Processing may cause and their extent of | Potential impact/harm: *Please explain.*<br><br>☐ Low ☐ Medium ☐ High | <u>Examples of potential impact or harm</u>:<br><br>(i) Security risks;<br><br>(ii) Inability to exercise data subject's rights; |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | risk? (You may add additional rows for each potential impact and harm identified, e.g. 29(a), 29(b) and etc.) | Elaboration: *Please explain as appropriate and specify the likelihood and impact severity* | (iii) Loss of control over the use of personal data;<br>(iv) Identity theft or fraud;<br>(v) Financial loss;<br>(vi) Physical harm;<br>(vii) Loss of confidentiality; and<br>(viii) Inadequate data and privacy protection laws in the country to which the data is transferred. |
| **C – Consider measures to mitigate risks** | | | |
| 30. | What are the measures that can (and will) be adopted to mitigate the risks set out under questions 19 to 29? (You may add additional rows for each measure identified, e.g. 30(a), 30(b) and etc.) | Measure: *Please explain*<br>Which risk(s) does the measure mitigate: *Please state the question number(s)*<br>Degree of mitigating the risk(s): ☐ Some ☐ Material ☐ Significant<br>Responsible person to implement the measures: *Please state*<br>Expected completion date of the implementation: *Please state* | Examples of measures:<br>(i) Not to collect certain types of data;<br>(ii) Reduce the frequency of processing or shorten retention periods;<br>(iii) Implement additional security measures;<br>(iv) Anonymise or pseudonymise certain personal data<br>(v) Use a different technology;<br>(vi) Incorporate additional contractual safeguards with the third party involved in the processing; and<br>(vii) Conduct a Transfer Impact Assessment to determine whether the transfer is permitted under Act 709 and/or |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | | | the receiving country has adequate data protection and privacy laws. |
| **A – Assess overall residual risk level** | | | |
| 31. | What is the overall residual risk level (taking into account the measures to be implemented) of the Planned Processing? | ☐ Low ☐ Medium ☐ High | Evaluation of:<br>(i) the risk levels assigned under questions 19 to 29; and<br>(ii) how effective the proposed measures are realistically expected to mitigate these specific risks. |
| 32. | What is the date of completing the DPIA? | *Please state* | This will be the starting date of the two (2) year validity period of the DPIA. |
| **Post-DPIA**: Manage risks and accountability | | | |
| **Report to senior management** | | | |
| 33. | If the overall residual risk level is assessed as High, who is responsible for reporting the findings of the DPIA carried out on the Planned Processing to the senior management for its consideration and input? | ☐ Not applicable<br>☐ Responsible person: *Please state* | The responsible person can be the DPO, the DPIA Lead or another designated personnel. |
| 34. | Further to question 30, are there any additional risk | ☐ Yes ☐ No<br>Elaboration: *Please describe the measures and for each measure, identify the* | This is to set out any additional risk mitigation measures that are identified after the completion of the DPIA, which |

| No. | Questions | Responses | Guidance Notes |
|---|---|---|---|
| | mitigation measures that will be implemented? | *responsible person for implementation and the expected completion date of the implementation.* | may or may not be based on input from the senior management. |
| **Record keeping** | | | |
| 35. | Who is responsible for properly maintaining the DPIA and all relevant documents for at least two (2) years from the cessation of the processing operation? | *Please provide* | Please provide the name(s) of the personnel. If a team is responsible, please provide the names of the team members. |

## ANNEX B: FLOWCHART ON CARRYING OUT A DPIA