PUBLIC CONSULTATION PAPER NO. 02/2024:

THE APPOINTMENT OF DATA PROTECTION OFFICER

PART 1: INTRODUCTION AND BACKGROUND

[A] Introduction

1.1 The Personal Data Protection (Amendment) Bill 2024 ("**Amendment Bill**"), which introduces amendments to the Personal Data Protection Act 2010 ("**PDPA**"), was passed without amendments by the House of Representatives on 16 July 2024, and by the Senate on 31 July 2024. The Amendment Bill is currently pending assent by the Yang di-Pertuan Agong.

1.2 Clause 6 of the Amendment Bill seeks to introduce a new mandatory data protection officer obligation for data controllers (previously known as data users)[1] and data processors by inserting a new Section 12A under Part II of the PDPA.

1.3 For ease of reference, the full text of Section 12A of the PDPA which provides for the new mandatory data protection officer appointment requirement states 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.*

1.4 To supplement the data protection officer obligation that will be introduced by the new Section 12A of the PDPA, a proposed Personal Data Protection (Data Protection Officer) Regulations ("DPO Regulations") and Data Protection Officer Guideline ("**DPO Guideline**") are being developed by the Personal Data Protection Commissioner ("**Commissioner**"). The DPO Regulations and the DPO Guideline will provide additional guidance on implementation requirements for the data protection officer appointment obligation and supplement Section 12A of the PDPA.

1.5 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 DPO Regulations and DPO Guideline.

[1] Clause 2 of the Amendment Bill substitutes the term "data user(s)" with "data controller(s)" throughout the Amendment Bill.

PART 2: PROPOSED REQUIREMENTS FOR DATA PROTECTION OFFICER APPOINTMENT REQUIREMENT UNDER THE PDPA

2.1 As an overview, Part 2 of this PCP on proposed requirements that will be addressed in the DPO Regulations and DPO Guideline is categorised as follows:

(a) Threshold requirement for mandatory appointment of Data Protection Officer ("**DPO**");

(b) Consistency with other legal requirements to a role similar to a DPO;

(c) Sector-specific risks for DPOs to be aware of when carrying out its functions;

(d) Reporting line for DPOs;

(e) Regional DPO appointment and DPO local residency requirement;

(f) Minimum expertise and qualifications of DPO and certification of DPOs; and

(g) Factors the Commissioner may consider in exercising its discretion to mandate appointment of a DPO.

[A] Threshold requirement for mandatory appointment of DPO

2.2 Background: Prior to the latest amendments to the PDPA, there was no mandatory requirement under the PDPA for data controllers or for data processors to appoint DPOs. As such, DPOs (or their equivalents) were only appointed pursuant to additional legal requirements that they were subject to under other laws or regulations, contractual provisions or on a voluntary basis.

2.3 In order to align with practices of data protection authorities in other jurisdictions (including the European Union or "EU") and to prevent the DPO appointment requirement from being overly burdensome on smaller data controllers / data processors, it is proposed that the mandatory DPO appointment requirement under Section 12A of the PDPA be restricted to only certain types of data controllers / data processors. The risk posed to data subjects, the nature of personal data being processed, and the volume of data subjects whose personal data is being processed would need to be taken into consideration as well.

2.4 Proposal: It is proposed that the mandatory DPO appointment requirement applies only to data controllers / data processors that carry out data processing activities of a "large scale". In determining whether or not the data processing activities are of a "large scale", the following factors will need to be considered:

(a) the number of data subjects concerned;

(b) the volume of data and/or the range of different data items being processed;

(c) the nature of the data being processed (e.g., whether sensitive personal data is involved);

(d) the risk posed to the data subject as a result of the data processing activity carried out by the data controller / data processor;

(e) the duration, or permanence, of the data processing activity; and/or

Examples:

This may include data processing activity requiring "regular and systematic monitoring".

"Regular monitoring" refers to processing requiring ongoing or constant processing, whereas "systematic monitoring" refers processing which is organised and pre-arranged.

(a) Example of processing activity requiring regular and systematic monitoring: A business analytics service provider processes personal data by tracking and profiling data subjects offline and online for the purpose of behavioural advertising services offered to its clients. This processing is likely to be regular as it is carried out continuously.

(b) Example of processing activity that does not require regular and systematic monitoring: A school organises a parent-teacher conference and asks attending parents to pre-register online ahead of the conference. However, the school realises on the day of the conference that the parent that pre-registered was not necessarily the parent that ended up attending the conference. The school collects personal data of parents who have physically attended a parent-teacher conference in order to register and verify the identity of the parent in attendance. This processing is done on an ad hoc basis in response to the situation and not regular and systematic monitoring.

(f) the geographical extent of the data processing activity.

2.5 Please note that when assessing whether data processing activities will be deemed to be "large scale", each of the above thresholds should be considered in turn. Once established, each individual threshold may be sufficient to establish that a data controller / data processor carries out "large scale" processing.

2.6 However, each individual threshold need not necessarily be established for data processing to be considered large scale. In other words, each individual threshold is sufficient but not necessary for the purposes of determining whether the data processing activities are "large scale". That said, a data controller / data processor that satisfies more than one (1) of the above thresholds is more likely than not to be considered as processing personal data on a large scale.

2.7 For the avoidance of doubt, a data controller / data processor will not be precluded from carrying out "large scale" processing purely for the reason that it does not fall within any one of the given thresholds.

2.8 Please also note that a data controller / data processor that meets the threshold of large scale processing of personal data is required to, at the very least, appoint one (1) DPO for its organisation, who may be appointed from an external provider or appointed internally among the data controller / data processor's employees.

2.9 The data controller / data processor may consider whether additional DPOs or supporting team of personnel for the DPO should also be appointed for the purposes of facilitating the DPO in carrying out their responsibilities, depending on the data controller / data processor's circumstances, such as the size of its organisation or the nature of data processing activities being carried out by the data controller / data processor.

Question 1

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

(a) Do you think data controllers / data processors are reasonably capable of applying the factors above to determine whether they satisfy the "large scale" threshold to comply with the DPO appointment requirement under the PDPA?

(b) Do you think "large scale" should be defined based purely on an express quantitative threshold (e.g. a data controllers / data processor must appoint a DPO if it processes personal data of 20,000 data subjects), or should it be based on a list of factors, such as the list of factors outlined in Paragraph 2.4 above?

(c) If your response in (b) is the latter, is the list of factors above sufficient or does it omit threshold requirements that may be helpful to determine whether a data controller / data processor may be processing personal data on a "large scale"? If so, please specify what these specific requirements are.

(d) Do you think factor 2.4(e) listed above should include data processing activities that would require "regular and systematic monitoring"? If so, is there merit in including the criteria of "regular and systematic monitoring" for the appointment of DPOs, to cover data processing activities by data controllers / data processors that occur frequently, over extended periods, and continuously e.g. for behavioural analytics purposes?

[B] Consistency with other legal requirements to a role similar to a DPO

2.10 Background: Some data controllers / data processors may already have designated / appointed officers within their operations who carry out a role similar or overlapping role to a DPO (e.g. a compliance officer or chief information officer or chief technology officer).

2.11 This may be the result of factors such as the data controller / data processor's own unique human resource structure, or due to other data-related requirements that have otherwise imposed a requirement for a person-in-charge or officer to be responsible for data compliance within the organisation.

2.12 Proposal: In order to prevent the DPO role being a redundant or a duplicative role and in line with the practice of other jurisdictions (including the EU), it is proposed that DPOs are allowed to carry out additional job functions aside from their data-specific roles as a DPO. As such, a person may be designated to be a DPO in addition to carrying out their existing job scope, provided that this person is still able to carry out their role as a DPO effectively.

Question 2

Does the DPO appointment requirement overlap, duplicate, or otherwise relate to other existing legal requirements that your organisation is subject to under Malaysian laws? If so, please describe or refer to these other applicable legal requirements.

[C] Sector-specific risks for DPOs to be aware of when carrying out its functions

2.13 Background: Data protection authorities in other jurisdictions (including the EU), set out a minimum scope of statutory responsibilities that DPOs must carry out, which is intended to promote consistency and accountability in the DPO's role of overseeing and monitoring a data controller / data processor's data protection practices.

2.14 For the avoidance of doubt, the DPO is not expected to directly carry out the individual tasks proposed below. Instead, the DPO may exercise an oversight function by ensuring that their team of data specialists / personnel carries out the responsibilities below.

2.15 Proposal: It is proposed that a DPO has the following responsibilities (briefly summarised), at minimum:

(a) advise the data controller / data processor on the processing of personal data and application of PDPA and related data protection laws;

(b) support the data controller / data processor in complying with the requirements of the PDPA and other applicable data protection laws;

(c) carry out data protection impact assessments;

(d) monitor the personal data compliance of the data controller / data processor;

(e) ensure that internal training is provided to the data controller / data processor's staff on data protection current and updated practices;

(f) act as a facilitator and liaison point between data subjects and the data controller / data processor with respect to the processing of the data subjects' personal data;

(g) act as the liaison and main contact point of the data controller / data processor with the Commissioner; and

(h) such additional minimum responsibilities that the Commissioner or the data controller / data processor may include from time to time (e.g. as a result of technology developments).

Question 3

Are there any specific personal data processing activities or risks you foresee that DPOs should be aware of when carrying out their functions, which are not already covered or should be specified in the minimum responsibilities above? If yes, please detail what these specific activities or risks are and provide clear justifications to support your views.

[D] Reporting line for DPOs

2.16 Background: Several jurisdictions (including the EU) specifically require DPOs to have direct reporting access to the top senior management of the data controller / data processor. This is in order to ensure the independence of DPOs and to provide them with the authority needed to perform their duties effectively, as well as to grant them influence over the data controller / data processor's data protection strategy.

2.17 DPOs may face potential conflicts of interest if they hold a position in the senior management of the data controller / data processor, or if a member of senior management "double-hats" or holds dual responsibilities within the organisation (e.g. as DPO and Chief Finance Officer). This conflict may arise due to differing interests and priorities of their job scopes, i.e. between the role of promoting strategic and business-friendly goals and prioritising due compliance with data protection laws.

2.18 Proposal: It is proposed that DPOs must have a direct reporting line / access to the senior management team of the data controller / data processor, or to the personnel of an equivalent position depending on the nature of the data controller / data processor's organisation structure (e.g. personnel who can direct the highest-level of decision-making within that data controller / data processor in that jurisdiction).

2.19 A direct reporting line means that the DPO must have access to the senior management team (or equivalent) to provide their advice and recommendations, or be able to draft reports which are submitted directly to the top senior management team, ensuring that the senior management team is aware of the DPO's advice and recommendations. In practice, this may require the DPO to be appointed to a role that does not sit too low within the hierarchy of the organisational structure.

Question 4

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

(a) Do you think it is important the DPO has a direct reporting line / access to the data controller / data processor's senior management (or an equivalent)?

(b) Do you foresee any potential compliance challenges that may arise which might prevent a data controller / data processor from implementing the requirement for direct reporting line / access effectively?

[E] Regional DPO appointment and DPO local residency requirement

2.20 Background: As alluded to above, some data controllers / data processor may already be subject to a legal requirement to appoint a DPO or equivalent position which may be based on data protection laws of other jurisdictions.

2.21 The requirements in some of these countries (including the EU) expressly allow a group of companies to appoint a single DPO for the purposes of ensuring compliance with personal data laws applicable in the respective jurisdictions that the group operate in. As such, a single shared DPO may be appointed to oversee and manage data compliance activities across a group of companies operating across multiple jurisdictions, including the obligations under the PDPA.

2.22 As mentioned above as well, the role of a DPO may also be an external (as opposed to an internal role) and DPO services may be outsourced from third parties depending on the needs of the data controller / data processor.

2.23 In order to ensure accessibility and responsiveness, particularly towards the Commissioner (e.g. to enable quicker responses to any inquiries or concerns of the Commissioner due to time and language differences), a DPO should be appointed and should be ordinarily resident in Malaysia.

2.24 Proposal: It is proposed that a single DPO may be appointed to serve multiple entities within the same group of companies for data controllers / data processor.

2.25 Additionally, for the purposes of accessibility and responsiveness to the Commissioner, it is also proposed that the DPO appointed is also ordinarily resident in Malaysia.

Question 5

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

(a) Do you foresee any issues if shared DPO(s) are appointed across all entities within the same group?

(b) Do you foresee any issues with introducing a requirement that DPO(s) are ordinarily resident in Malaysia?

[F] Minimum expertise and qualifications of a DPO and certification of DPOs

2.26 Background: A DPO should possess certain knowledge and abilities in order to ensure that they are able to fulfil the minimum tasks outlined for DPOs, as outlined in Paragraph 2.15 above.

2.27 The qualifications of the DPO must align with the responsibilities that they are expected to undertake in order that the DPO is able to carry out their responsibilities effectively. In other words, data controllers / data processor of larger size or those handling personal data on a larger scale (e.g., multinational corporations) are expected to appoint a DPO with higher qualifications compared to Small and Medium Enterprises of a smaller size.

2.28 Other jurisdictions (including the EU) generally require a DPO to possess minimum knowledge and abilities which are expected to be aligned with their responsibilities. While we have not observed specific or strict qualification requirements imposed for a DPO, some jurisdictions have recognised certain certification programs for DPOs, e.g., in Singapore and the Philippines:

(a) Singapore has a partnership with the International Association of Privacy Professionals ("**IAPP**") to train and issue Practitioner Certificates for Personal Data Protection (Singapore) to individuals who have passed the certification exam jointly conducted by Singapore's Personal Data Protection Commission and IAPP; and

(b) Philippines has implemented a data privacy competency programme to train and educate the public on the legal framework of privacy law and regulations in the Philippines. However, completion of the course is not equivalent to earning a professional certification.

2.29 Proposal: It is proposed that appointed DPOs meet a minimum set of prescribed expertise and qualifications to ensure that they are able to carry out their tasks effectively, namely:

(a) good knowledge about the requirements under the PDPA (including any other applicable data protection laws);

(b) good understanding of the data controllers / data processor's business operations, and the personal data processing operations that are carried out;

(c) good understanding of the IT systems and data safety/data security measures deployed by data controllers / data processor;

(d) personal qualities such as integrity and high professional ethics;

(e) the ability to promote data protection culture within the organisation; and

(f) good proficiency and understanding of the cultural and language requirements of the jurisdictions that data controllers / data processor operate in.

2.30 The Commissioner may also develop or prescribe training or certification programs for DPOs from time to time, which may be local or international, and require the individuals who wish to be appointed as a DPO under the PDPA to complete such training programs or obtain such certification before they can be appointed as a DPO.

Question 6

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

(a) What are your views about the use of "sound" versus "good" as a measure and yardstick to determine the minimum expertise and qualification for DPOs?

(b) What type(s) of certification / qualifications do you propose should be recognised by the Commissioner? For example, privacy certifications issued by IAPP?

(c) In your view, are the above set of proposed minimum expertise and qualification requirements adequate and sufficient to ensure that a DPO is equipped to carry out its obligations under the PDPA?

[G] Factors the Commissioner may consider in exercising its discretion to mandate appointment of a DPO

2.31 Background: In addition to the criteria for mandatory DPO appointment above, it is proposed that the Commissioner should have the authority to mandate data controllers / data processors who do not meet the prescribed criteria / threshold to comply with the DPO appointment obligation, as he sees fit on a case-by-case basis.

2.32 We have observed a similar catch-all requirement in other jurisdictions (including the EU) to allow data protection authorities to direct data controllers / data processor to appoint a DPO for their organisation.

2.33 Proposal: In view of the above, it is proposed that the Commissioner should have the flexibility to direct certain classes or specific data controllers / data processor to appoint a DPO as deemed necessary on a case-by-case basis. This is notwithstanding that the data controllers / data processor does not meet the prescribed criteria / threshold to be subjected to the mandatory DPO appointment obligation.

2.34 Examples of circumstances where the Commissioner may potentially exercise his/her powers to direct the appointment of a DPO include:

(a) where the nature of the personal data processed by the data controller / data processor is sensitive;

(b) where the data controller or data processor has previously experienced significant data breaches or has a history of non-compliance with data protection laws and regulations; or

(c) where the Commissioner identifies specific industries or sectors that pose a higher risk to data privacy and security, thereby necessitating the appointment of a DPO to ensure robust data protection practice by data controllers / data processors operating in those industries or sectors.

Question 7

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

Bearing in mind the existing threshold and factors for "large scale" above, do you think there are any specific high-risk processing activities or emerging risks and concerns that the Commissioner should bear in mind when exercising its discretion to require a data controller / data processor to comply with the DPO appointment obligation under the PDPA?