TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS & DATA PROTECTION

Public Consultation Papers Issued for Upcoming Guidelines under the Personal Data Protection Act 2010

Introduction

Earlier this year in January, Digital Minister Gobind Singh announced that the Personal Data Protection Department ("**JPDP**" or *Jabatan Perlindungan Data Peribadi*) will be developing a suite of supplementary guidelines to complement amendments that will be introduced to the Personal Data Protection Act 2010 ("**PDPA**").[1] These guidelines include the following:

(i) The Implementation of Data Breach Notification Guideline ("**DBN Guideline**");
(ii) The Appointment of Data Protection Officer Guideline ("**DPO Guideline**");
(iii) The Right to Data Portability Guideline ("**Data Portability Guideline**");
(iv) The Cross Border Data Transfer Guideline;
(v) The Privacy by Design Guideline; and
(vi) The Profiling and Automated Decision-Making Guideline.[2]

Following the Malaysian Parliament's passing of the Personal Data Protection (Amendment) Bill 2024 ("**Amendment Bill**") on 31 July 2024, the Personal Data Protection Commissioner ("**Commissioner**") has issued public consultation papers to seek feedback on the following initial set of guidelines:

(i) The DBN Guideline;
(ii) The DPO Guideline; and
(iii) The Data Portability Guideline.

The public consultation period is open until **6 September 2024**, and feedback can be submitted through the Google Forms provided here.

These public consultation papers offer valuable insights into what can be expected in the forthcoming guidelines and how they will shape the implementation of the new changes introduced by the Amendment Bill. For further information regarding the key changes introduced by the Amendment Bill, please refer to our previous Legal Update.

This Update aims to provide a brief overview of the key information and matters addressed in the public consultation papers.

[1] Gobind: Seven guidelines to be developed under Personal Data Protection Act 2010: https://www.malaymail.com/news/malaysia/2024/01/16/gobind-seven-guidelines-to-be-developed-under-personal-data-protection-act-2010/112720

[2] In addition, JPDP is also looking at introducing amendments to the Personal Data Protection Standard 2015 (PDP Standard) to enhance the Commissioner's requirements regarding minimum security, retention and data integrity standards that data controllers must maintain under the PDPA.

© CHRISTOPHER & LEE ONG

Overview of the Additional Guidance and Requirements Highlighted by the Public Consultation Papers

[I] Public Consultation Paper No. 1/2024: DBN Guideline

As a brief recap, the Amendment Bill introduces a new obligation on data controllers to notify both the Commissioner and affected data subjects of personal data breaches. Non-compliance with this notification requirement can result in fines of up to RM250,000 and/or imprisonment for up to two years, or both.

The public consultation paper for the DBN Guideline (accessible here) provides further details on the additional guidance and requirements proposed by the Commissioner for the implementation of the new mandatory data breach notification ("**DBN**") requirement under the Amendment Bill:

Scope Areas	Proposed Requirements for DBN to the Commissioner	Proposed Requirements for DBN to Affected Data Subjects
DBN Notification Thresholds	Limited to only instances where: (a) Personal data breach is likely to cause/ have caused *"significant harm"*[3]; **AND/OR** (b) Personal data breach is likely to be of a *"significant scale"* (i.e. 500 or more data subjects are affected).	Similar to the proposed notification thresholds for DBN to the Commissioner
Manner and Form of DBN	Notification to be made through a simplified version of JPDP's existing voluntary DBN reporting form.	Notification must be made directly to affected data subjects unless doing so would involve a disproportionate effort. A prescribed minimum list of information must be provided, including details of the breach and recommendations for steps that affected data subjects can take.
DBN Timeframe	72 hours after the data controller becomes aware of a personal data breach	At the same time as the DBN submitted to the Commissioner, or as soon as practicable thereafter.
Exemptions from/ Postponement of DBN	N/A	Exemption from/postponement of DBN allowed where: (a) Appropriate measures have been taken that renders it unlikely that the breach will

[3] A personal data breach will be considered to be of *"significant harm"* if: (a) the personal data breach results or is likely to result in bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the data subjects' credit record, or damage to or loss of property; (b) the personal data breach results or is likely to result in serious harm to affected data subjects to whom the information relates, or has been, is being or will likely be misused for illegal purposes; **or** the personal data compromised by the personal data breach includes sensitive personal data or any other information that may be used to enable identity fraud such as usernames, passwords or identification numbers.

		result in significant harm to affected data subjects; (b) Personal data compromised or affected by the breach is protected by one or more security measures that make the information unintelligible or meaningless to any individual who is not authorised to obtain the information; or (c) the Commissioner directs otherwise.
Data Processors' Obligation	Data controllers are required to contractually obligate their data processors to promptly notify them of any personal data breaches and to provide the necessary assistance to enable the data controller to meet its DBN obligations.	N/A
Record-Keeping Obligations	Data controllers will be required to develop and implement a data breach management plan to ensure that they are able to promptly respond to any personal data breaches.	

[II] Public Consultation Paper No. 2/2024: DPO Guideline

The Amendment Bill introduces a new obligation for *both* data controllers and data processors to appoint at least one DPO for their organisation, who needs to be registered with the Commissioner. No specific penalty is prescribed under the Amendment Bill for non-compliance with the DPO appointment requirement.

The Commissioner has also since clarifed that the DPO appointment will not be a blanket requirement, and it will only apply to data controllers and data processors that meet certain prescribed criteria.[4]

The public consultation paper for the DPO Guideline (accessible here) offers further insights on the proposed implementation requirements for the new DPO appointment requirement under the Amendment Bill:

Scope Areas	Proposed Requirements
Threshold Requirement for Mandatory Appointment of DPO	Mandatory DPO appointment requirement to only apply to data controllers and data processors that carry out data processing activities of a "large scale". To determine whether data processing activities qualify as "large scale," a list of factors is provided, such as the volume of data subjects involved, and the nature and volume of data processed. Notwithstanding the above, the Commissioner has the discretion to mandate certain classes or specific data controllers data processors to comply with the DPO appointment requirement (e.g. where the data controller/data processor has a history of non-compliance with the PDPA).
Matters Relating to the Appointment of DPO	(a) An appointed DPO may carry out additional job functions aside from their data-specific roles as a DPO. (b) A single DPO may be appointed to serve multiple entities within the same group of companies.

[4] Data Protection Officer for some companies soon: https://www.nst.com.my/news/nation/2024/08/1086316/data-protection-officer-some-companies-soon

	(c) A DPO may be appointed internally, or externally outsourced to third parties. (d) The appointed DPO will be required to be ordinarily resident in Malaysia for the purposes of accessibility and responsiveness to the Commissioner.
Minimum Responsibilities of DPOs	A prescribed list of minimum responsibilities for DPOs is established to promote consistency and accountability in their role of overseeing and monitoring a data controller's or data processor's data protection practices. These responsibilities include, among others, supporting and monitoring compliance with personal data protection laws and acting as the main contact point for data subjects and the Commissioner.
Reporting Line for DPOs	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.
Minimum Expertise and Qualifications for DPOs	DPOs are required to meet a minimum set of prescribed expertise and qualifications (e.g. good knowledge about the requirements of the PDPA). Additionally, the Commissioner may develop/prescribe training or certification programs for DPOs.

[I] Public Consultation Paper No. 3/2024: Data Portability Guideline

The Amendment Bill introduces a new right of data portability which allows data subjects to request that their personal data be directly transmitted from one data controller to another. No specific penalty is prescribed under the Amendment Bill for non-compliance with the data portability requirement.

The public consultation paper for the Data Portability Guideline (accessible here) provides further information regarding the scope and application of this right:

Scope Areas	Proposed Requirements
Types of Personal Data Subject to the Right of Data Portability	It is proposed that the right be limited to only personal data that meets the following requirements: (a) personal data that is directly provided by the data subject; (b) personal data processed based on consent, or based on a consent or based on a contract to which the data subject is a party to; (c) personal data processed electronically/by automated means; and (d) personal data that is not inferred data or derived data. Additionally, the Commissioner is also considering employing a whitelisting approach where data controllers will only be required to transmit data belonging to the categories listed in the whitelist. However, where a data subject requests for data that does not belong to any category listed in the whitelist, data controllers may voluntarily transmit such data.
Timeline for Responding to Data Portability Requests	21 days, with additional 14-days of extension available.

Historical Data	No time limits or limitation periods to be imposed on data portability requests in respect of personal data previously collected and retained by data controllers.
Fees	Data controllers will be allowed to charge a fee for responding to data portability requests, but a fee cap may be imposed by the Commissioner.
Method of Transmission of Personal Data	It is proposed that data controllers have the flexibility to determine the most appropriate method for transmitting data in response to data portability requests, as long as specific requirements are met regarding the format of the transmitted data and the security measures in place to protect the personal data during transmission.

Conclusion

The public consultation papers provide data controllers and data processors with crucial insights into the anticipated guidelines and their impact on implementing the changes introduced by the Amendment Bill, particularly concerning the new DBN obligation, the DPO appointment obligation, and the recognition of right to data portability for data subjects. The information highlighted by the public consultation papers will be useful guidance for businesses when reviewing and updating your personal data protection practices to comply with the new requirements introduced by the Amendment Bill.

We encourage businesses to review the public consultation papers and submit any feedback or concerns by **6 September 2024** using the links provided above. Engaging in this process allows businesses to voice their perspectives on the proposed implementation requirements and contribute to shaping the final guidelines.

We trust the above provides a helpful overview of the guidance/requirements proposed by the public consultation papers. Should you require any further assistance or clarification regarding the above or any other matter pertaining to personal data protection, please feel free to get in touch with us at your convenience.

Contacts

Deepak Pillai

PARTNER

D +603 2267 2675
M +6012 213 4674
deepak.pillai@christopherleeong.com

Intan Haryati

PARTNER

D +603 2267 2674
F +603 2273 8310
intan.haryati@christopherleeong.com

Anissa Maria Anis

PARTNER

D +603 2267 2750
M +6012 371 9129
anissa.anis@christopherleeong.com

Yong Shih Han

PARTNER

D +603 2267 2715
M +6012 480 8863
shih.han.yong@christopherleeong.com

Contribution Note

This Legal Update is contributed by the Contact Partners listed above, with the assistance of **Yeap Yee Lin** (Associate, Christopher & Lee Ong).

Please feel free to also contact Knowledge Management at RTApublications@rajahtann.com.

Regional Contacts

Cambodia
Rajah & Tann Sok & Heng Law Office

T +855 23 963 112 / 113
kh.rajahtannasia.com

China
Rajah & Tann Singapore LLP
Shanghai & Shenzhen Representative Offices

T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

Indonesia
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

Lao PDR
Rajah & Tann (Laos) Co., Ltd.

T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

Malaysia
Christopher & Lee Ong

T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

Myanmar
Rajah & Tann Myanmar Company Limited

T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

Philippines
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)

T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

Singapore
Rajah & Tann Singapore LLP

T +65 6535 3600
sg.rajahtannasia.com

Thailand
Rajah & Tann (Thailand) Limited

T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

Vietnam
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
vn.rajahtannasia.com

Rajah & Tann Asia is a network of legal practices based in Asia.

Member firms are independently constituted and regulated in accordance with relevant local legal requirements. Services provided by a member firm are governed by the terms of engagement between the member firm and the client.

This update is solely intended to provide general information and does not provide any advice or create any relationship, whether legally binding or otherwise. Rajah & Tann Asia and its member firms do not accept, and fully disclaim, responsibility for any loss or damage which may result from accessing or relying on this update.

Our Regional Presence

Christopher & Lee Ong is a full service Malaysian law firm with offices in Kuala Lumpur. It is strategically positioned to service clients in a range of contentious and non-contentious practice areas. The partners of Christopher & Lee Ong, who are Malaysian-qualified, have accumulated considerable experience over the years in the Malaysian market. They have a profound understanding of the local business culture and the legal system and are able to provide clients with an insightful and dynamic brand of legal advice.

Christopher & Lee Ong is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.

The contents of this Update are owned by Christopher & Lee Ong and subject to copyright protection under the laws of Malaysia and, through international treaties, other countries. No part of this Update may be reproduced, licensed, sold, published, transmitted, modified, adapted, publicly displayed, broadcast (including storage in any medium by electronic means whether or not transiently for any purpose save as permitted herein) without the prior written permission of Christopher & Lee Ong.

Please note also that whilst the information in this Update is correct to the best of our knowledge and belief at the time of writing, it is only intended to provide a general guide to the subject matter and should not be treated as a substitute for specific professional advice for any particular course of action as such information may not suit your specific business or operational requirements. It is to your advantage to seek legal advice for your specific situation. In this regard, you may call the lawyer you normally deal with in Christopher & Lee Ong.