TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS & DATA PROTECTION

Public Consultation Papers Issued for Upcoming Guidelines on Data Protection Impact Assessment, Data Protection by Design, and Automated Decision Making and Profiling under the Personal Data Protection Act 2010

Introduction

With the introduction of the Personal Data Protection (Amendment) Act 2024 ("**Amendment Act**"), which has begun coming into force in stages from 1 January 2025 and will be fully implemented by 1 June 2025, the Personal Data Protection Commissioner ("**Commissioner**") also announced the development of a suite of subsidiary guidelines to supplement the changes introduced by the Amendment Act.

Since then, the Commissioner has issued several public consultation papers for these upcoming guidelines. In February 2025, two of these guidelines, namely "The Appointment of Data Protection Officer Guideline" and "The Data Breach Notification Guideline", were issued.

For more details on the requirements and guidance outlined in these two guidelines, please refer to our February 2025 Legal Update titled "Launch of Personal Data Protection Guidelines for Data Protection Officer Appointment and Mandatory Data Breach Notification".

The Commissioner has now issued three new public consultation papers to seek feedback on the following upcoming guidelines:

1. Data Protection Impact Assessment Guideline;
2. Data Protection by Design Guideline; and
3. Automated Decision Making and Profiling Guideline.

This Update provides a brief overview of the key information and matters addressed in the public consultation papers, which offer valuable insights into what can be expected in the forthcoming

guidelines once finalised as well as their implications on organisations' data protection compliance frameworks in the future. The public consultation period for these guidelines is open until **19 May 2025**, and the online feedback form is accessible here.

Overview of the Status of the Guidelines

As our country's data protection regulatory landscape continues to evolve rapidly, we recognise that staying updated on all changes can be challenging. To help our readers navigate these developments, the table below provides an overview of the status of each guideline that has been or is currently being developed by the Commissioner.

No.	Guideline	Status
1.	The Appointment of Data Protection Officer Guideline	**Issued on 25 February 2025, taking effect on 1 June 2025.** To be read together with Circular of Personal Data Protection Commissioner No. 01/2025: Appointment of Data Protection Officer
2.	The Data Breach Notification Guideline	**Issued on 25 February 2025, taking effect on 1 June 2025.** To be read together with Circular of Personal Data Protection Commissioner No. 02/2025: Data Breach Notification
3.	The Right to Data Portability Guideline	**Public consultation closed on 18 October 2024.** Pending issuance of Guideline.
4.	Cross-Border Data Transfers Guideline	**Public consultation closed on 18 October 2024.** Pending issuance of Guideline.
5.	Revised Personal Data Protection Standard 2015 ("**PDP Standard**") ** This is not a guideline but a mandatory and enforceable Standard pursuant to the Personal Data Protection Act 2010 ("**PDPA**").*	**Public consultation closed on 18 October 2024.** Pending issuance of PDP Standard.
6.	Data Protection Impact Assessment Guideline	**At public consultation stage.** Public consultation paper issued; the consultation period is currently open until **19 May 2025**.
7.	Data Protection by Design Guideline	**At public consultation stage.**

No.	Guideline	Status
		Public consultation paper issued; the consultation period is currently open until **19 May 2025**.
8.	Automated Decision Making and Profiling Guideline	**At public consultation stage.** Public consultation paper issued; the consultation period is currently open until **19 May 2025**.

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

Public Consultation Paper No. 01/2025: Data Protection Impact Assessment Guideline ("DPIA Guideline")

Under the Appointment of Data Protection Officer Guideline ("**DPO Guideline**"), data protection officers ("**DPOs**") are required to support and advise on the implementation of data protection impact assessments ("**DPIAs**"). Accordingly, the Commissioner aims to provide guidance to DPOs on how to conduct DPIAs through the upcoming DPIA Guideline.

In line with the approach taken in other jurisdictions, including the United Kingdon (UK), the Commissioner defines a DPIA as a process to assess how planned/intended data processing operations or activities may affect personal data protection. This includes identifying, evaluating, and managing potential data protection risks based on the organisation's needs and operations.

Overview of the key requirements/guidance outlined by the public consultation paper for the DPIA Guideline are set out below:

Scope Areas	Proposed Requirements
Who needs to conduct DPIA?	Only data controllers will be subject to the DPIA requirement
When to conduct a DPIA?	A DPIA is required if the planned processing operation meets any of the prescribed "quantitative threshold" OR "qualitative factors": "Quantitative Threshold" A DPIA is required if: • The processing of sensitive personal data is expected to involve more than 10,000 data subjects; • The processing of personal data for automated decision-making purposes is expected to involve more than 10,000 data subjects; or • The processing of personal data is expected to involve more than 20,000 data subjects.

Scope Areas	Proposed Requirements
	"Qualitative Factors" A DPIA is required if: • There are potential legal or significant effects on data subjects (e.g. a noticeable impact on individuals' legal status/rights or their financial status); • There is systematic monitoring of publicly accessible area (e.g. closed-circuit television (CCTV) with profiling capability); • There is use of innovative technology (e.g. combining fingerprint and facial recognition for enhanced access control); • There is denial or restriction of data subjects' rights (e.g. using automated decision-making to approve and reject loan/insurance applications); • There is tracking of data subjects' location or behaviour (e.g. eye-tracking to generate data to provide more tailored direct marketing); or • There is targeting of children or other vulnerable individuals.
How to conduct DPIA?	A DPIA is to be conducted using a five-step approach, abbreviated as "**DEICA**": • **D**escribe the processing operations and their purposes; • **E**valuate the necessity and proportionality of the processing operation in relation to its purposes; • **I**dentify and analyse the specific risks to personal data protection for data subjects; • **C**onsider measures to mitigate the identified risks and safeguard personal data; and • **A**ssess the overall residual risk level (e.g. high, medium, low) of the processing operation.
Notification to the Commissioner	If the DPIA assesses the overall residual risk to be **high**, data controllers must report/notify the Commissioner about the DPIA's findings. However, there is no requirement to consult or obtain the Commissioner's approval before proceeding with the processing operation.
Post-DPIA Obligations	Upon completion of the DPIA, data controllers must: • implement measures proposed in the DPIA to mitigate identified risks; • continuously monitor from time-to-time developments which may impact the processing operations and the risks, and address them accordingly; and • maintain records of all DPIAs conducted, along with relevant documentation, for at least two years, and provide them upon request for inspection by the Commissioner.

Public Consultation Paper No. 02/2025: Data Protection by Design Guideline ("DPbD Guideline")

Although Data Protection by Design ("**DPbD**") is not expressly referenced in the PDPA, it has become an established concept in recent years and has since been recognised under the data protection laws of many other jurisdictions. To encourage data controllers to shift from a reactive to a proactive approach — one that integrates privacy considerations from the outset and by default — the proposed DPbD Guideline aims to provide a framework to help data controllers incorporate DPbD into their operations.

Scope Areas	Proposed Requirements
Seven foundational Principles for DPbD	The Commissioner outlines seven foundational principles as a guiding framework for the operationalisation of DPbD in practice. These principles are: • **DPbD Principle 1: Proactive not reactive; preventative not remedial** – anticipating and preventing privacy risks before they occur and actively building processes to prevent data breaches, instead of only reacting to them when they happen (e.g. undertake regular data protection assessment and audits) • **DPbD Principle 2: Privacy as the default setting** – ensuring personal data of individuals are automatically protected and no action is required on the part of the individual to protect his/her privacy (e.g. adoption of data minimisation approach) • **DPbD Principle 3: Privacy embedded into design** – integrating privacy into technologies, operations and information architectures into a holistic, integrative and creative way (e.g. employing multi-layered encryption protocols to protect personal data, and conducting DPIAs to identify any privacy risks) • **DPbD Principle 4: Full functionality –** accommodating all legitimate interests and objectives in a manner that benefits all stakeholders, without making unnecessary trade-offs against privacy (e.g. adopting nuanced/multi-layered approach to minimise the collection and processing of personal data) • **DPbD Principle 5: End-to-end security – full lifecycle protection**– ensuring data security throughout the entire lifecycle of the personal data involved (e.g. ensuring that appropriate security measures are in place to protect personal data through the personal data's lifecycle) • **DPbD Principle 6: Visibility and transparency – keep it open** – demonstrating accountability for personal data processing activities (e.g. ensuring that privacy notices issued are easily accessible and organised in a clear and layered manner)

Scope Areas	Proposed Requirements
	• **DPbD Principle 7: Respect for user privacy – keep it user-centric** – keeping the interests of the individual by offering measures such as strong privacy defaults, appropriate notice and empowering user-friendly options
Additional Considerations for the Protection of Children's Privacy	The Commissioner proposed to outline additional specific guidance for products and services that are directed at/intended for access by children. This includes imposing the following obligations on data controllers: • **Best interests of child**: Obligation to take into account the best interests of children in the processing of children's personal data (e.g. protecting and supporting children's own views and identity) • **Age verification**: Obligation to make reasonable efforts to verify the age of their users and that they have received consent of the children's parent/guardian to process the children's personal data (e.g. implementing appropriate age verification mechanisms to verify the age of its users) • **Strictest privacy settings for children**: Obligation to ensure that the strictest privacy settings apply to services directed at/intended for access by children (e.g. information provided to children regarding the collection and processing of their personal data should be available in an obvious, easy to find place) • **Profiling/automated decision making**: Prohibition on profiling children, engaging in automated decision-making concerning children, otherwise use their personal data for advertising/marketing purposes

In addition to the seven foundational DPbD principles, the public consultation paper also outlines recommended measures and considerations for data controllers when implementing DPbD in alignment with each of the seven Personal Data Protection Principles under the PDPA.

Public Consultation Paper No. 03/2025: Automated Decision Making and Profiling Guideline ("ADMP Guideline")

Similarly, while automated decision-making and profiling are not expressly recognised as concepts under the PDPA, the increasing use of emerging technologies such as artificial intelligence ("**AI**") to process data and make decisions automatically has prompted the Commissioner to issue the ADMP Guideline. This guideline aims to provide guidance on the introduction and implementation requirements for automated decision-making and profiling.

Scope Areas	Proposed Requirements
Scope of ADMP Guideline	• "Automated decision making" means the "process of making decisions by automated means without any human involvement". • "Profiling" means "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects

Scope Areas	Proposed Requirements
	concerning that data subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".
Trigger	• Automated decision making and profiling operations/activities that may legally or significantly affect an individual
Regulation of Automated Decision Making and Profiling	The ADMP Guideline aims to regulate automated decision making and profiling by providing data subjects with the following: • **Right to refuse**: The right to refuse to be subjected to decision based solely on automated decision making and profiling which produces legal effects or significantly affects an individual • **Right to information**: The right to information on the automated decision making and profiling being undertaken • **Right to human review**: The right to request a human review of the automated decision making and profiling undertaken (collectively, "**ADM Restrictions**")
Exceptions to ADM Restrictions	The ADM Guideline sets out exceptional circumstances where some or all of the ADM Restrictions can be dispensed with/waived. For instance, the ADM Guideline proposes to dispense with/waive the right to refuse and the right to human review in the following exceptional circumstances (the right to information remains applicable): • where the processing is necessary for entering into, or performance of, a contract between an individual and the data controller; • where the processing is necessary for compliance with laws; or • where the data subject has given their prior explicit consent.
Use of Personal Data for AI Training and Output	It is proposed that the ADMP Guideline recognises the use of AI and Generative AI (whether to train large language models or as part of obtaining an output from such models) as a form of "automated decision making".
Additional Restrictions for use of Biometric Data	Given the recognition of biometric data as a new type of sensitive personal data by the Amendment Act, the ADMP Guideline proposes to introduce additional measures for the processing of biometric data in general (e.g. transparency requirements and security requirements for biometric data)

Comment

The public consultation papers provide valuable insights into the upcoming guidelines on DPIA, DPbD, and automated decision-making and profiling.

It is worth noting that, unlike the other guidelines being developed by the Commissioner, the concepts and requirements introduced in this tranche of guidelines are not currently expressly recognised or referenced under the amended PDPA (pursuant to the Amendment Act). It remains to be seen how the Commissioner will address the legal status of these upcoming guidelines.

We encourage businesses and organisations to review the public consultation papers and provide feedback, particularly regarding any concerns about the practicality or potential challenges in implementing the proposed requirements. Additionally, if further clarification is needed on specific aspects addressed in the public consultation papers, businesses and organisations should highlight these points in their feedback.

In any event, the requirements introduced by these public consultation papers will undoubtedly impact the personal data protection compliance framework of organisations once they are finalised and issued. Therefore, organisations and businesses should remain mindful of these developments and prepare accordingly.

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

Contacts

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS & DATA PROTECTION

Deepak Pillai

HEAD

D +60 3 2275 2675
F +60 3 2273 8310
deepak.pillai@christopherleeong.com

Intan Haryati Binti Mohd Zulkifli

PARTNER

D +60 3 2675 2674
F +60 3 2273 8310
intan.haryati@christopherleeong.com

Anissa Maria Anis

PARTNER

D +60 3 2267 2750
F +60 3 2273 8310
anissa.anis@christopherleeong.com

Yong Shih Han

PARTNER

D +60 3 2273 1919
F +60 3 2273 8310
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 | +855 23 963 113
kh.rajahtannasia.com

China

Rajah & Tann Singapore LLP Representative Offices

Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820

Shenzhen Representative Office
T +86 755 8898 0230
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 +603 2273 1919
F +603 2273 8310
www.christopherleeong.com

Myanmar

Rajah & Tann Myanmar Company Limited

T +951 9253750
mm.rajahtannasia.com

Philippines

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

T +632 8248 5250
www.cagatlaw.com

Singapore

Rajah & Tann Singapore LLP

T +65 6535 3600
sg.rajahtannasia.com

Thailand

Rajah & Tann (Thailand) Limited

T +66 2656 1991
F +66 2656 0833
th.rajahtannasia.com

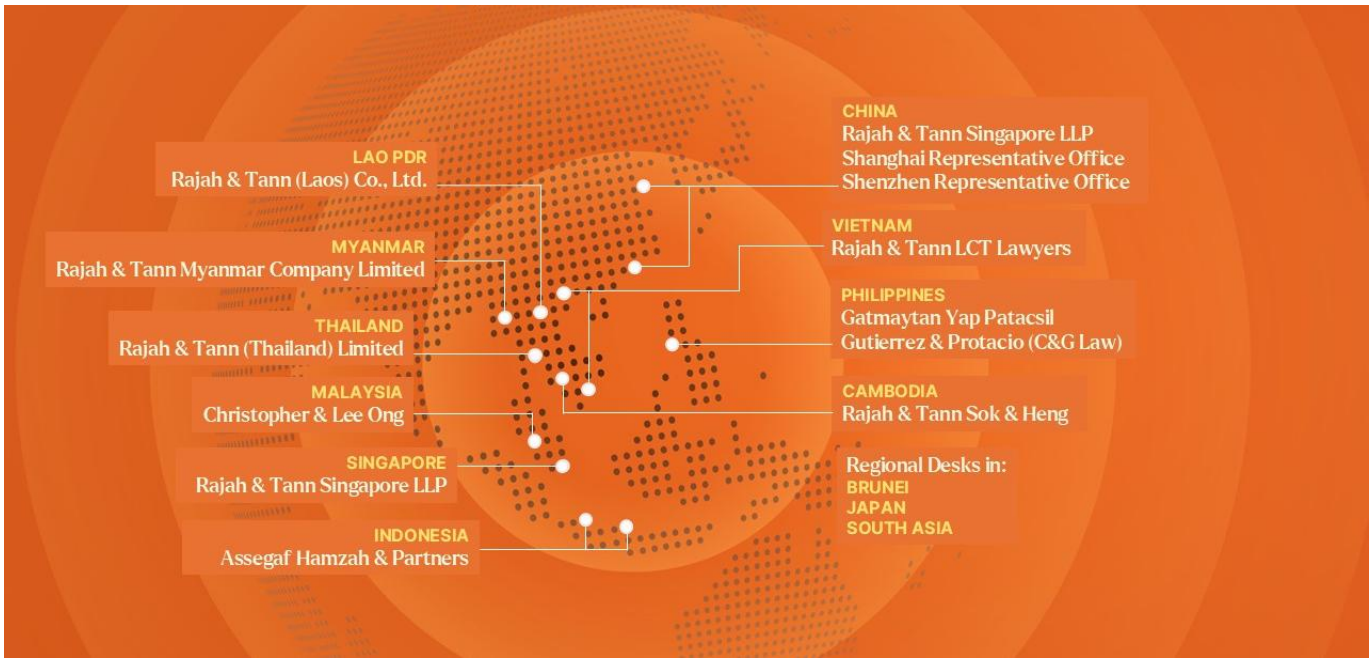
Vietnam

Rajah & Tann LCT Lawyers

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

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

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.