Malaysia: Public consultations on cross-border transfer and personal data protection standards

04 Oct 2024 • 7 minute read

Privacy | PII | Cybersecurity | Data | Governance | ESG | DT Featured Content

In brief

The Personal Data Protection Department (PDPD) has issued two public consultation papers on:

- Introducing specific rules and guidance on **cross-border transfer** of personal data.
- Revamping the personal data protection standards (i.e., minimum compliance requirements) covering **security**, **retention** and **data integrity**.

The deadline to provide feedback is Friday, 18 October 2024.

In more detail

We have previously highlighted in our client alerts:

- Key changes brought by the Personal Data Protection (Amendment) Bill 2024 to the Personal Data Protection Act 2010 (PDPA).
- First batch of public consultations on data breach notification, data protection officer and data portability which involve fresh legal obligations.

In this second batch of public consultations, the PDPD is focusing on aligning existing concepts with international standards and practices in the:

- Public Consultation Paper No. 04/2024: Personal Data Protection Standards (PDPS PCP).
- Public Consultation Paper No. 05/2024: Cross-Border Personal Data Transfer Guidelines (CBT PCP).

Cross-border transfer

Section 129 of the PDPA provides different legal bases for transferring personal data out of Malaysia. The CBT PCP seeks to provide clarity on how some of the legal bases can be satisfied.

Section 129(2)

The CBT PCP proposes to mandate the adoption by data controllers of a **Transfer Impact Assessment** (TIA) in order to rely on any of the following two legal bases to transfer personal data to a place outside Malaysia:

	Legal basis	
	Section 129(2)(a)	Section 129(2)(b)
	There is in that place in force any law which is **substantially similar** to the PDPA	That place ensures at least **equivalent level of protection** afforded by the PDPA
Proposed steps for TIA	1. Identifying all countries that the personal data is to be transferred to. 2. Assessing the mechanisms to safeguard personal data that are in place in each of the receiving countries based on the factors listed below. 3. Conducting periodic TIAs to ensure that the level of protection is still similar.	
Proposed factors to consider in TIA	• Whether there are similar personal data protection principles in place, and similar requirements and protections regarding the processing, transfer, retention, disclosure and cross-border data transfer of personal data. • Whether the law provides similar data subject rights (e.g., right to access and correct) and there are similar requirements regarding data protection officers and data breach notification. • Whether the law has in place similar penalties and enforcement mechanisms to deal with breaches of the local data protection law and data breaches.	• Whether the transferee has security measures and policies that are in line with the security principle and the minimum security standards prescribed under the PDPA. • Whether the transferee has in place any security-related certifications which have assessed the systems it has in place and deemed its systems to be secure. • Whether the transferee is bound by legally enforceable obligations (e.g., via contract or by law) and whether such obligations can be enforced by the data controller or data subjects whose personal data is to be transferred to.

Section 129(3)(f)

Particularly, Section 129(3)(f) allows data controllers to transfer personal data out of Malaysia, if they have taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not, at the hands of the transferees, be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA. To rely on this legal basis, the CBT PCP proposes three options as proof that data controllers have "taken all reasonable precautions" and satisfy Section 129(3)(f):

- **Binding Corporate Rules** (BCRs): A set of data protection rules or policies that apply to intra-group cross-border data transfers, which **must** contain certain prescribed information e.g., the requirement for transferees to ensure a standard

of protection equivalent to that under the PDPA, procedures for handling data subject requests/ complaints, security measures that must be implemented etc.

- **Standard Contractual Clauses** (SCCs): Contracts relied on by parties to conduct cross-border transfers, which **must** contain one of the following:
    - Minimum clauses set out by the Commissioner, which may include a statement that all processing to comply with the PDPA and the minimum security measures that must be implemented to protect personal data.
    - Regional/ international model contractual clauses recognized by the Commissioner e.g., the EU SCCs and the ASEAN Model Contractual Clauses for Cross-Border Data Flows, adapted to address matters prescribed under the PDPA.
- **Certification**: Transferees issued with a valid certificate that is recognized by the Commissioner e.g., the Asia Pacific Economic Cooperation Cross Border Privacy Rules System (APEC CBPR), **provided that** there is also a contract guaranteeing that the transferees apply appropriate safeguards to protect the data transferred to them.

Section 129(3)(a), (b), (c) and (g)

The CBT PCP also seeks to clarify how some other legal bases under Section 129(3) of the PDPA can be satisfied if relied upon:

- To rely on **consent** for cross-border transfers of personal data, data controllers must inform the data subjects via the written notice (e.g., privacy policy) on the class of third parties who may have access and the purpose of such transfers. Consent obtained must also be capable of being recorded and maintained.
- For legal bases premised on **necessity** (e.g., necessary for the performance of contract with the data subjects), the transfers should be for specific reasons and made to achieve a specific purpose which cannot reasonably be achieved through alternative means.

Last but not least, the PDPD proposes that data controllers must also keep and maintain certain prescribed information and such other records that may sufficiently prove that each cross-border transfer of personal data complies with Section 129 of the PDPA.

Feedback to the CBT PCP may be provided via this link.

Security, retention and data integrity

For context, the existing Personal Data Protection Standards 2015 (PDPS) sets out the security standard, the retention standard and the data integrity standard, outlining the minimum compliance requirements for the corresponding personal data protection principles under the PDPA.

The PDPS PCP proposes to replace the more "black and white" rules under the existing PDPS with requirements based on a more **outcome-based approach**. The intent is for the amended PDPS to:

- Define the Commissioner's expectations and the outcomes organizations should aim to achieve.
- Set out that organizations, in applying the standards, should take a risk-based approach such that the measures implemented to meet the outcomes must be proportionate to the level of risk faced by them (e.g., nature, scope and volume of personal data processing activities, and potential harm and impact in the event of security breach).

The following key elements for each of the specific standards, are being proposed for incorporation in the amended PDPS:

- **Security standard**: In the context of security controls (applicable to both data controllers and data processors), the amended PDPS will seek to address what the expectations are in relation to governance structure, access control, asset and data inventory management, digital threats, network security and software updates, third-party risk management, and training/ awareness. The current differentiation on how to comply with the security principle as between personal data processed electronically and non-electronically is also intended to be removed.

- **Retention standard**: In this context (applicable to data controllers only), the amended PDPS will seek to address what the expectations are in relation to the duration of retention period, documentation and records for retention and disposal of personal data, methods of destruction or deletion of personal data, and third-party retention of personal data.
- **Data integrity standard**: In this context (applicable to data controllers only), the amended PDPS will seek to address what the expectations are in relation to data validation and verification, data quality monitoring, data consistency, and data lifecycle management.

Last but not least, and in line with practices of some other jurisdictions, the PDPD proposes that the adoption by data controllers of industry certifications (e.g., ISO 27001, ISO 27017, ISO 27701), can also be an avenue to demonstrate compliance with the PDPS (although it does not automatically imply blanket compliance or immunity for data controllers).

Feedback to the PDPS PCP may be provided via this link.

* * * * *

Chun Hau Ng, Associate, has co-authored this legal update.

Wong & Partners.
Member Firm of
Baker & McKenzie International

© 2024 Wong & Partners. All rights reserved. Wong & Partners, member of Baker & McKenzie International. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome

Contact Information

Kherk Ying Chew
Partner
Kuala Lumpur
Read my Bio
kherkying.chew@wongpartners.com

Serene Kan
Partner
Kuala Lumpur
Read my Bio
serene.kan@wongpartners.com

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the

extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME.

Reproduction: Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.