Wong & Partners.
Member Firm of
Baker & McKenzie International

Client Alert

9 May 2025

Malaysia: Cross Border Personal Data Transfer Guideline

In brief

Following the public consultation in 2024, the Personal Data Protection Commissioner has now issued the Personal Data Protection Guideline on Cross Border Personal Data Transfer ("**Guideline**").

The Guideline provides guidance on the operationalisation of section 129 of the Personal Data Protection Act 2010 ("**PDPA**") and sets out specific responsibilities of data controllers[1] when transferring personal data to any place outside Malaysia ("**Transfer**").

This client alert seeks to summarise the key takeaways from the Guideline.

Contents

In More Detail

Section 129 of the PDPA provides the different legal bases (or known as conditions in the Guideline) for a Transfer. A data controller must meet **at least one** (rather than all) of these legal bases in order to undertake a Transfer.

The Guideline helps organisations determine the most appropriate legal mechanism for facilitating a Transfer, by providing guidance on how the requirements under section 129 of the PDPA can be operationalised.

Similar Law or Adequate Protection

To recap, effective 1 April 2025, two additional legal bases under section 129(2) of the PDPA were introduced i.e., a data controller can undertake a Transfer (i.e., to a place outside Malaysia), if the said place ("**Location**"):

(a) has law in force that is substantially similar to the PDPA ("**Similar Law**"); or

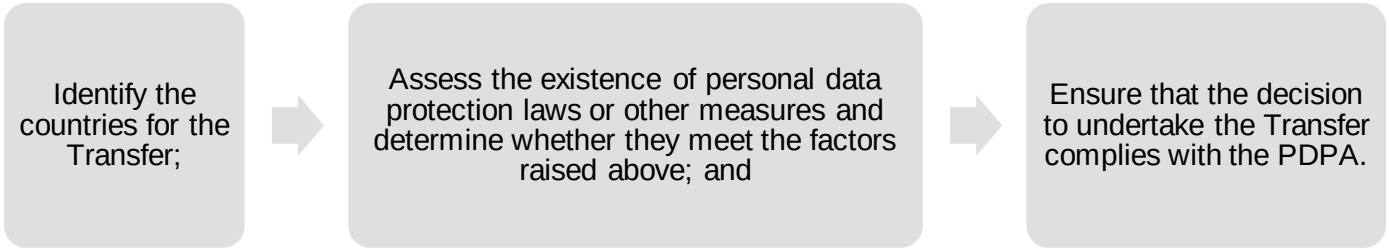
(b) ensures an adequate level of protection regarding personal data processing, which is at least equivalent to the level of protection afforded by the PDPA ("**Adequate Protection**").

[1] Put it simply, a **data controller** collects, stores or otherwise processes personal data (or has control over or authorises such processing). This excludes and is in contrast with a **data processor**, who essentially processes personal data not for its own purposes but solely on behalf of the data controller.

The Guideline requires the data controller to **make a finding** that the Location has Similar Law or Adequate Protection, by at least considering the following **prescribed factors** such as:

- *Similar Law* – The law has similar data subject rights, personal data protection principles, data protection officer requirement, data breach notification requirement, data processor obligation and regulatory authority to enforce such law.
- *Adequate Protection* – The receiver of personal data in the Location ("**Receiver**") has security measures and policies, the Receiver has in place security related certifications which have assessed that the systems in place are deemed secure, there are legally enforceable obligations (via contract or by law) imposed, the Receiver's history of compliance and existence of equivalent regulatory authority.

To this end, the data controller may conduct a Transfer Impact Assessment ("**TIA**") to ascertain if either of the Similar Law or Adequate Protection concepts are met. In carrying out a TIA, the data controller will need to:

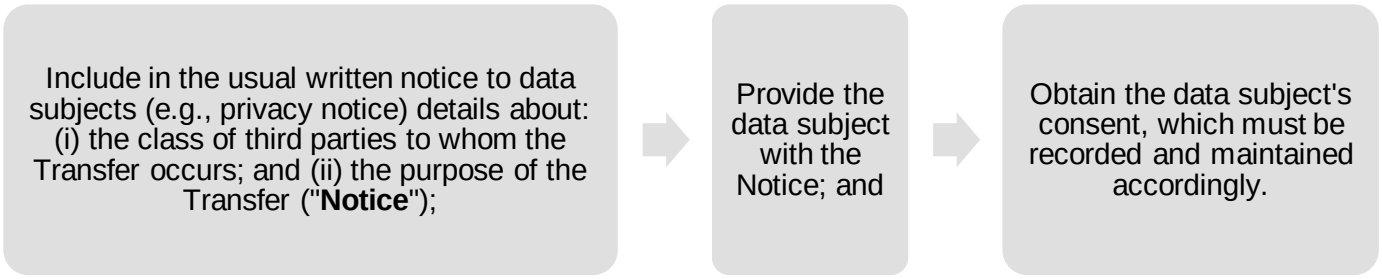


The TIA findings are valid for up to 3 years only; a follow-up TIA needs to be conducted thereafter. A review is also needed, if there are changes to the laws or measures, to determine whether the Location still satisfies the Similar Law or Adequate Protection concepts.

Consent

By virtue of section 129(3)(a) of the PDPA, **consent** of the data subject[2] is an existing legal basis which a data controller may rely on for a Transfer.

In this regard, the Guideline makes clears that a data controller in obtaining consent for a Transfer will need to:



If the data subject **has not but would have given consent** to a Transfer, a data controller may rely on section 129(3)(e) of the PDPA, provided that the Transfer is for the avoidance or mitigation of adverse action against the data subject. The Guideline clarifies that this legal basis only applies if it is not possible for the data subject to give consent e.g., the data subject is unconscious or uncontactable (despite efforts having been made to do so).

[2] A data subject is basically an individual whose personal data is being processed. Note that the definition of "data subject" under the PDPA now excludes a deceased individual.

Necessary for Contract or Vital Interests

There are also three legal bases under section 129(3)(b), (c) and (g) of the PDPA which are premised on the Transfer being **necessary**:

- for the performance of contract with the data subject ("**Data Subject Contract**");
- for the conclusion or performance of contract with a third party which is entered into at the data subject's request or is in the data subject's interest ("**Third Party Contract**"); or
- to protect the data subject's vital interests (i.e., matters relating to life, death or security of a data subject).

The Guideline clarifies that the word "necessary" does not mean the Transfer has to be absolutely essential, but the following factors must be considered and satisfied before a Transfer is regarded as being necessary:

Reason for the Transfer	Purpose for the Transfer	Whether there are any feasible alternative available
Not just because the Transfer is a practice or is carried out on a regular basis;	Made to achieve a specific purpose only and not for general purpose; and	Cannot reasonably achieve the specified purpose through any alternative means that can be feasibly carried out.

For the Data Subject Contract concept, the Guideline further clarifies that the contractual obligations necessitating the Transfer, must be for the **core purpose of the contract**, such that the Transfer must be directly related to and for the purposes of performing the data controller's obligations as specified under the contract.

For the Third Party Contract concept, the Guideline also clarifies the two conditions as follows with respect to the contract:

- *At the data subject's request* – The request must be in written form or otherwise maintained as proof.
- *In the data subject's interests* – The primary aim of the contract shall provide direct benefits to the data subject, which can be clearly identified as a direct result of the contract.

Legal Purposes

A data controller can also rely on section 129(3)(d) of the PDPA to undertake a Transfer for purposes of legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights.

The Guideline clarifies that legal proceedings include claims at court and at tribunals as well as administrative and regulatory processes and out of court procedures (e.g., mediation, arbitration). This legal basis is also **available** if the data controller is engaged in pre-action correspondence, or has received a request for information from an overseas regulatory body with a view to it potentially taking formal action. However, this legal basis is **not available** if there is only a possibility that legal or other formal proceedings may be brought in the future.

Reasonable Precautions and Due Diligence

A data controller may also carry out a Transfer by relying on section 129(3)(f) of the PDPA, i.e., they have taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not (in that Location) be processed in any manner which would constitute a contravention of the PDPA (if that Location is Malaysia).

The Guideline clarifies that this legal basis may be satisfied, if the data controller can show that **any one of the following** mechanisms are adopted:

Binding Corporate Rules ("BCR")	Contractual Clauses	Certification
The Receiver is subject to **personal data protection policies** that are legally binding on entities within a multinational corporate group (and the like) to facilitate intra-group Transfers. The Guideline prescribes **minimum details** to be incorporated into such policies, which need to also be **legally enforceable** and be **periodically reviewed** for update, in order to qualify as a BCR.	The Receiver is bound by minimum contractual clauses which will **legally ensure adequate level of protection** regarding personal data processing. The contractual clauses shall at least cover: (i) the **security measures** to be implemented by the Receiver; and (ii) a **guarantee** that the Receiver's processing of personal data shall be **compliant** with the PDPA. At this stage, the ASEAN Model Contractual Clauses for Cross Border Data Flows and the EU GDPR Standard Contractual Clauses for the Transfers of Personal Data to Third Countries, have been cited as model clauses which can be adopted for evidencing compliance with this mechanism.	The Receiver is in possession of **recognised certifications**, which **verify its compliance** with data protection standards or laws. Some certifications cited for purposes of this mechanism are the Europrivacy certification scheme and the APEC CBPR and APEC PRP Certification.

Universal Responsibilities

Regardless of the legal basis relied upon by data controllers, the Guideline also introduces responsibilities that apply universally to the Transfer, which include:

- informing data subjects in writing about the Transfer;
- ensuring the method for the Transfer is secure and in line with the relevant requirements;
- ensuring any contract with any third party or data processor contains clauses governing the processing of personal data; and
- maintaining record of the Receiver containing the prescribed minimum details and proving that each Transfer complies with section 129 of the PDPA.

Concluding Remarks

The Guideline not only provides better colour on how the two new legal bases introduced under section 129 of the PDPA should be operationalised; it also provides insights into the Personal Data Protection Department's expectations with respect to the utilisation of existing legal bases for undertaking cross border personal data transfers.

In light of the Guideline, organisations should take the opportunity to review and reassess their personal data transfer mechanisms to ensure compliance with section 129 of the PDPA.

Keywords: Privacy; PII; Cybersecurity; Data; Governance; ESG; Transfers; Cross Border

* * * * *

Contact Us

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

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

Chun Hau Ng
Associate
Kuala Lumpur
chunhau.ng@wongpartners.com