Shearn Delamore &co.

Launch of Guidelines on Cross Border Personal Data Transfer

On 29 April 2025, we attended the launch ceremony of the *Guidelines on Cross Border Personal Data Transfer* ("CBPDT Guidelines"), officiated by the Personal Data Protection Commissioner, YBrs. Prof. Dr. Mohd Nazri bin Kama.

The *CBPDT Guidelines* were introduced following recent amendments to section 129 of the **Personal Data Protection Act 2010** ("PDPA"), which governs the transfer of personal data to places outside Malaysia.

Under the amended section 129(2), a data controller may now transfer personal data of a data subject to any place outside Malaysia if:

- the receiving jurisdiction has a law which is substantially similar to the PDPA; or
- the receiving jurisdiction ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA.

A foreign law is deemed "*substantially similar*" if it includes protection mechanisms, rights, and data processing requirements (e.g. on collection, disclosure, retention and cross border transfer) comparable to the PDPA.

Data controllers may conduct a Transfer Impact Assessment ("TIA") to assess this by considering factors such as:

- the presence of data subject rights;
- the presence of data protection principles (e.g. Security Principle);
- processing requirements;
- the existence of a comparable regulatory authority; and
- similar data breach notification requirements.

Personal Data Protection & Privacy Laws Update

MAY 2025

Shearn Delamore & Co
7th Floor
Wisma Hamzah Kwong-Hing,
No 1, Leboh Ampang
50100, Kuala Lumpur, Malaysia
T: 603 2027 2727
F: 603 2078 5625
info@shearndelamore.com
www.shearndelamore.com
www.linkedin.com/company/shearn-delamore-&-co

An "*adequate level of protection*" means that the receiving country must be able to ensure that transferred personal data will be protected to a level at least equivalent to that under the PDPA. This may also be demonstrated through a TIA, by evaluating:

- security measures and security related certifications of the receiver;
- legally enforceable obligations of the receiver;
- enforceability of laws;
- receiver's past history of compliance; and
- the existence of a comparable regulatory authority.

TIAs are valid for a maximum of three years, after which a follow-up TIA must be undertaken. In cases of significant changes or amendments to systems or policies relating to the security and protection of personal data during the validity period, a review of the TIA is required.

Exceptions under section 129(3)

Section 129(3) allows for cross-border transfers even in the absence of substantially similar laws or adequate protection, if certain exceptions apply. These include:

- where the transfer is necessary for the performance of a contract between the data subject and the data controller;
- where the data controller has taken all reasonable precautions and exercised due diligence to ensure that the personal data will not be processed in a manner which, if that place were Malaysia, would be a contravention of the PDPA.

Cross-border transfer is permitted where such transfer is necessary for the performance of a contract between the data controller and the data subject, provided that the obligations are for the core purpose of the contract.

There must be a direct and objective link between the performance of the contract and the transfer. The transfer must be for a specific purpose — not as part of a general practice — and the data controller must not be able to reasonably achieve that purpose through alternative means.

As regards to the requirement to demonstrate that the data controller has taken all reasonable precautions and exercised all due diligence to ensure the personal data will not be processed in a manner that would contravene the PDPA if the processing occurred in Malaysia, it was suggested that mechanisms such as Binding Corporate Rules ("BCRs"), Contractual Clauses ("CCs"), and certifications under an approved certification scheme may serve as evidence of such precautions and diligence.

BCRs are internal data protection policies implemented by multinational corporate group, groups of undertakings or a group of enterprise engaged in joint economic

activity such as franchise, joint venture or professional partnership. CCs are a set of clauses incorporated into contracts which would legally bind both the data controller and the receiver to ensure adequate level of protection in relation to the processing of personal data.

Concluding Remarks

The CBPDT Guidelines provide clarity on the requirements for transferring personal data outside Malaysia. Organisations and businesses are recommended to review and, where necessary, revise their data protection operations, policies, procedures, playbooks, as well as contracts.

For further enquiries, please contact:

Janet Toh Yoong San
Head, Personal Data Protection & Privacy
Co-Head, Technology, Media & Telco
E: janet.toh@shearndelamore.com
T: +603 2027 2978

Boo Cheng Xuan
Associate, Personal Data Protection & Privacy
Associate, Technology, Media & Telco
E: boo.chengxuan@shearndelamore.com
T: +603 2027 2662

Yee Yong Xuan
Associate, Personal Data Protection & Privacy
Associate, Technology, Media & Telco
E: yongxuan.yee@shearndelamore.com
T: +603 2027 2615