Baker McKenzie.

TMT
Singapore

Client Alert

October 2019

For more information, please contact:

Ken Chia
+65 6434 2558
ken.chia@bakermckenzie.com

Anne Petterd
+65 6434 2573
anne.petterd@bakermckenzie.com

Alex Toh
+65 6434 2783
alex.toh@bakermckenzie.com

Daryl Seetoh
+65 6434 2257
daryl.seetoh@bakermckenzie.com

Binh Vong
+65 6434 2538
binh.vong@bakermckenzie.com

New PDPC guidelines on cloud services and data access requests

On 9 October 2019, the Personal Data Protection Commission ("**PDPC**") revised Chapter 6 (Organisations) and Chapter 15 (Access and Correction Obligations) and introduced a new Chapter 8 on cloud services in the Advisory Guidelines on the PDPA for Selected Topics ("**Guidelines**"). The Guidelines, while not legally binding, reflects the PDPC's approach in interpreting the Personal Data Protection Act ("**PDPA**").

In response to the increasing use of cloud services by organisations, the new Chapter 8 offers more clarity on the responsibilities of cloud service providers ("**CSP**") and organisations using cloud services to process personal data. Updates to Chapter 6 provide more clarity on the roles of an organisation and its data intermediary with regards to safeguarding personal data while updates to Chapter 15 focus on access requests by data subjects.

A summary of the PDPC's updates to the Guidelines are provided below.

Data intermediaries and cloud services

The updates address the PDPA Transfer Limitation Obligation which will apply when a CSP, while processing personal data on behalf of an organisation, transfers the personal data outside of Singapore. The new Chapter 8 clarifies that the CSP would be considered a data intermediary and that the organisation engaging the CSP to process personal data on the organisation's behalf and for its purpose remains responsible for complying with the Transfer Limitation Obligation.

Processing personal data. Chapter 8 explains that a CSP who is processing personal data for another organisation is considered a data intermediary and would be subject to PDPA obligations applied to data intermediaries, namely, the Protection and Retention Limitation Obligation. The Protection Obligation requires the CSP to have reasonable security arrangements to safeguard the personal data being processed by it. The Retention Limitation Obligation requires the CSP to cease to retain documents that contain personal data or to anonymise such personal data as soon as it is reasonable to assume that the personal data is no longer needed for the purpose for which it was collected.

Overseas transfer of personal data. Chapter 8 also makes clear that an organisation engaging a CSP as a data intermediary is still responsible for complying with the PDPA's Transfer Limitation Obligation, regardless of where the CSP is located. This means that an organisation must ensure that personal data transferred overseas by a CSP is done in accordance to PDPA requirements. Examples provided in Chapter 8 on how an organisation may meet PDPA requirements include:

- Taking appropriate measures to ensure that personal data transferred by the CSP is only to overseas destinations with comparable data protection laws, or that the recipient in those destinations are legally bound by similar contractual standards.

- If the contract between an organisation and the CSP does not specify the destinations where personal data will be transferred, the organisation should ensure that the CSP, if based in Singapore, is certified or accredited as meeting relevant industry standards and that the CSP provides assurances that overseas data centers comply with these industry standards.

Organisations engaging CSPs and the CSPs themselves should ensure that they are each familiar with the requirements in the Guidelines so they know where each other are coming from when discussing agreement provisions on data protection. In particular, organisations and CSPs should ensure that they understand what is required to meet the Transfer Limitation Obligation.

Responding to access requests by data subjects

The previous version of the Guidelines stated that the PDPA "does not require" that an access request be accompanied by a reason for making such request; the updated Chapter 15 changes "does not require" to "does not expressly state." This suggests that the PDPC may be shifting to being more in favor of including the reason for making an access request.

Other additions to Chapter 15 reiterate the PDPA and the Personal Data Protection Regulations' requirements on when:

- An organisation does not need to accede to an access request (i.e. in cases of exemptions data collected for investigations) or if the applicant does not agree to pay an estimated fee provided by the organisation for responding to the request).

- An organisation does not need to inform any individual or organisation that it has disclosed personal data to a law enforcement agency.

- If an organisation cannot find the requested data within 30 days, it must inform the applicant within that time frame when the organisation will be able to respond to the access request. After that, the organisation must still respond as soon as it is reasonably possible.

The update on access requests is a timely reminder for organisations to ensure that they have PDPA compliant access request processes in place and that relevant personnel are familiar with applying these processes.

For more details on the new updates, please refer to the Guidelines here. Please let us know if you have any queries regarding the information provided in the Guidelines or any other related matters.