Hogan Lovells

New PDPC guidelines on cloud services, data intermediaries, and access requests

28 November 2019

As the issues surrounding data protection become increasingly complex, in recent years the advisory guidelines (Guidelines) issued by the Personal Data Protection Commission of Singapore (PDPC) have been invaluable in guiding corporations on the scope and implementation of the Personal Data Protection Act 2012 (PDPA). Whilst the Guidelines are not legally binding, they are issued pursuant to section 49(1) of the PDPA, which requires them to be indicative of the manner in which the PDPC will interpret the PDPA – as such, they reflect the PDPC's approach and attitude to the PDPA.

On 9 October 2019 the PDPC introduced a new Chapter eight (*Cloud Services)* to the Guidelines and made revisions to Chapters six (*Organisations)* and 15 (*Access and Correction Obligations)* – the key elements of these changes are noted below.

Cloud service providers – who is responsible?

A central purpose of the revised Guidelines is to ensure that data transferred across boundaries in a cloud environment will be protected. The Guidelines now make clear that a cloud service provider (CSP) engaged by an organization pursuant to a written contract will be considered a "data intermediary." This means that the CSP will be subject to the same duties and responsibilities that apply to data intermediaries, the key responsibilities being the protection and retention limitation obligations under the PDPA, and the rules surrounding overseas transfer of personal data.

Why is this important? Because the organization that engages the CSP is ultimately responsible for ensuring that the CSP complies with the PDPA, insofar as it relates to the processing of personal data on its behalf, and for its purposes. This applies whether the CSP is located in Singapore or overseas.

Key takeaways when engaging with a CSP

Given this, an organization engaging a CSP will want to ensure that their contract with the CSP complies with the PDPA and adequately protects the organization. A few key takeaways:

- Protection and retention limitation obligations: The organization should ensure that the CSP complies with the protection and retention limitation obligations which, briefly, require the

CSP to: (a) have reasonable security arrangements in place to safeguard personal data; and (b) cease retaining documents that contain personal data or anonymize personal data as soon as it could be reasonably assumed that the data is no longer needed. These requirements should be covered in the written contract between the organization and the CSP.

- Overseas transfer of personal data (I): The organization should ensure that the CSP only transfers data to locations with a comparable data protection regime to Singapore, or where recipients are legally bound by similar contractual standards. This undertaking should ideally be given in the written contract between the organization and the CSP.

- Overseas transfer of personal data (II): Where the contract between an organization and its CSP is silent on the locations to which a CSP may transfer personal data, the organization should ensure that: (a) the CSP based in Singapore is certified or accredited as meeting the relevant industry standards; and (b) the CSP provides assurances that all overseas data centers or subprocessors comply with the relevant industry standards.

Refusing Access Requests

Chapter 15 of the Guidelines has also been revised to provide clarity on situations where organizations do not need to comply with an access request (being a request from an individual to access their personal data to see how it is maintained and/or used). Generally, organizations must respond to access requests unless there are valid reasons for rejecting the request. The grounds for rejection are stated in the Guidelines as follows:

- Exceptions apply: If any of the grounds set out in the fifth schedule of the PDPA apply, such as the personal information relating to an examination, being kept for evaluative purposes or relating to legal privilege.

- Access fees: If the individual has failed to pay the reasonable fees specified by the organization to respond to the request.

- Presents a threat to others: If access to the personal data could: (a) reasonably threaten the safety, physical, or mental health of a third party; or (b) cause immediate or grave harm to such an individual.

- Legal proceedings: Where the personal data has been collected for the purposes of legal proceedings, even if the personal data has been collected prior to legal proceedings commencing, the Guidelines state that the proper process is to obtain access through criminal and civil discovery procedures.

Whilst the above hasn't changed, the revised Guidelines make it clear that organizations can now consider the "purpose of the request" in assessing whether to provide the data requested, as well as the form in which the data should be provided.

Organizations and overseas transfers

In keeping with the new chapter on *Cloud Services*, Chapter six of the Guidelines has been revised to provide further clarity around the transfer of personal data overseas where organizations are concerned. Under the revised Chapter six, when an organization employs a data intermediary to process personal data on its behalf, that organization remains responsible for ensuring the prescribed requirements limiting the overseas transfer of personal data under the PDPA (the transfer limitation obligation) are still met. This remains the case whether the organization itself is transferring the personal data to an overseas intermediary or whether a Singapore-based intermediary is making the transfer for them.

In either case, the employing organization is obliged to carry out the requisite due diligence and ensure the intermediary in question is capable of complying with the transfer limitation obligation.

Conclusion

Since the adoption of the PDPA in 2012, the PDPC has continuously revised and improved the Guidelines to provide greater clarity on the implementation and interpretation of the PDPA. The introduction of the new Chapter eight, *Cloud Services*, in the Guidelines is yet another example of the benefits of the PDPC's continuing evolvement in, and engagement with, the business community in Singapore.

Contacts

Stephanie Keen
Office managing partner, Singapore
T +65 6302 2553
stephanie.keen@hoganlovells.com

Matthew Bousfield
Counsel, Singapore
T +65 6302 2565
matthew.bousfield@hoganlovells.com

Rachel Wong
Associate, Singapore
T +65 6302 7152
rachel.wong@hoganlovells.com