Baker McKenzie Wong & Leow.

Information Technology & Communications
Singapore

Client Alert

February 2017

Updates to the Personal Data Protection Regime in Singapore

For more information, please contact:

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

Seng Yi Lin
+65 6434 2713
YiLin.Seng@bakermckenzie.com

Lisa Cameron
+65 6434 2635
Lisa.Cameron@bakermckenzie.com

Executive Summary

The Personal Data Protection Commission ("PDPC") has recently introduced and updated its advisory guidelines to help companies better protect personal data in compliance with the Personal Data Protection Act ("PDPA"). The new Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data as well as updates to the (a) Guide to Securing Personal Data in Electronic Medium; (b) Guide to Disposal of Personal Data on Physical Medium; and (c) Guide on Building Websites for SMEs, were released on 20 January 2017.

The PDPC also released two enforcement decisions on 25 January 2017, relating to the breach of personal data protection obligations under the PDPA. Financial penalties were imposed on the organisations in breach for the failure to prevent unauthorised access of individuals' personal data stored online. In one of the decisions, the PDPC also directed the organisation to cease storage of documents containing personal data via its internal system until appropriate remedial actions have been completed. To learn more about the PDPC enforcement decisions, please click here.

Organisations concerned about compliance with the PDPA should take note of the PDPC's serious view of any non-compliance and the approach that the PDPC will take to enforce the PDPA.

Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data

This guide aims to equip organisations with the knowledge for preventing accidental disclosure when processing and sending out personal data.

The guide recommends good practices that organisations should adopt, including:

i. ensuring destination information is correct, which can be implemented through measures such as the use of automated processing of documents or communications containing personal data, and the adoption of checking mechanisms to ensure the accuracy and reliability of automated processing;

ii. ensuring personal data to be sent is correct, which can be implemented through measures such as the performance of additional checks to ensure the right document or the right personal data is sent;

iii. ensuring only the relevant personal data is disclosed to the recipients, which can be implemented through measures such as establishing a policy for sending compiled sets of personal data of different individuals, ensuring that individuals have consented to the sending of their personal data to recipients other than themselves, and ensuring that emails sent externally to a group have the recipients' email addresses placed in the 'bcc' fields;

iv. ensuring correct usage of software, which can be implemented through measures such as ensuring staff are trained and familiar with the software used to process and send out documents with personal data, and establishing clear procedures for using software to send out emails; and

v. minimising impact of accidental disclosure, which can be implemented through measures such as an e-mail policy for documents containing personal data to be secured with passwords when sending to both internal and external recipients, including a notice in all communications to warn recipients against unauthorised use, retention or disclosure of personal data, and to inform recipients to delete and notify the organisation immediately of any personal data sent to them in error.

In addition to recommending good practices for preventing accidental disclosure of personal data, the guide also includes learning points from case studies and highlights the relevant PDPA obligations that organisations should be aware of. In particular, the guide reminds organisations that a data intermediary will still be required to comply with the protection (Section 24) and retention limitation (Section 25) obligations under the PDPA.

The guide also highlights that organisations may be held liable for the actions or omissions of its data intermediary that amounts to a breach of the PDPA, and reminds organisations to ensure that its contract with its data intermediary imposes sufficient obligations on the data intermediary to ensure the organisation's own compliance with the PDPA.

Updates to Existing Guides

The PDPC also revised the Guide to Securing Personal Data in Electronic Medium and Guide to Disposal of Personal Data on Physical Medium to provide new examples that further illustrate good practices in the handling of personal data for organisations. The Guide to Disposal of Personal Data on Physical Medium introduced new examples and has been updated in respect of disposal chain control, while the Guide to Securing Personal Data in Electronic Medium has been expanded to provide more guidance regarding the use of ready-made software.

Further, the Guide on Building Websites for SMEs has been updated and now includes a section on the use of ready-made software that advises organisations

to understand the features of the software and how it should be configured to handle personal data.

Recent Enforcement Actions

The PDPC recently imposed a financial penalty of S$10,000 each on JP Pepperdine Group and Propnex Realty separately for breach of the protection obligation under the PDPA, in their respective cases.

In the Propnex decision, it was highlighted that Propnex's internal Do Not Call list was accessible to the public on the internet due to weaknesses with Propnex's internal virtual office system and the lack of appropriate security arrangements despite such weaknesses being known to Propnex. Accordingly, the PDPC found Propnex to be in breach of the protection obligation. In determining the penalty to be imposed, the PDPC took into account factors such as the number of individuals involved in the data breach, how cooperative the organisation had been during investigations as well as activities undertaken by the organisation's in-house compliance team in respect of assessing system access and data integrity risks. Apart from the financial penalty imposed, the PDPC also directed Propnex to: (i) cease the storage and/or sharing of documents containing personal data using its internal system until the system's flaw had been fixed; and (ii) conduct a security scan of its internal system before such system was made accessible online.

In the JP Pepperdine decision, it was highlighted that personal data of members of JP Pepperdine's membership programme was available online by entering a randomly simulated membership number on a webpage listed on its membership brochure, or by performing a search using the search functions available on its webpage. The PDPC found that the website had been designed without any security measures and that relevant security arrangements had not been put in place to protect personal data. Some of the factors taken into account by the PDPC in determining the relevant penalty to impose include the substantial amount of personal data involved (approximately 30,000 members), that sensitive personal data such as NRIC and passport numbers of individual were involved, and prompt action taken to remedy the breach upon being notified by the PDPC.

How This May Affect You

This decision is a timely reminder that the PDPC takes a very serious view of any non-compliance under the PDPA. The decisions also illustrate that the PDPC may issue directions to an offending organisation in respect of the use of its internal systems until appropriate remedial actions have been completed.

The PDPC's willingness to enforce the PDPA sends a clear message to organisations in control of personal data, as well as data intermediaries, that the PDPC will take any breach of the data protection obligations seriously. The PDPC highlighted in its decision that it will not hesitate to take appropriate enforcement action against organisations. Accordingly, organisations concerned

about compliance with the PDPA should take action immediately to ensure compliance with their obligations under the PDPA.

In the event of a data breach, we recommend that organisations ensure that they undertake breach mitigation measures, which may include promptly informing the Commission and the relevant individuals of the relevant data breach. Organisations should also co-operate with the PDPC in any proceeding investigations.

Please contact us if you would like further information or to discuss your organisation's compliance with the PDPA.

Baker McKenzie Wong & Leow lawyers earn Certified Information Privacy Professional / Asia (CIPP/A) Certification

As part of our team's commitment to remain at the forefront of data protection developments, four lawyers from the Firm recently earned the Certified Information Privacy Professional / Asia (CIPP/A) certification launched in early 2017. The lawyers certified are Principal, Ken Chia, Local Principal, Seng Yi Lin, and Associates, Lisa Cameron and Daryl Seetoh. Additionally, Ken Chia was also appointed as a Fellow of Information Privacy (FIP).

Both the CIPP/A certification and the FIP designation are awarded by the International Association of Privacy Professionals. Achieving a CIPP/A credential demonstrates understanding of a principles-based framework and knowledge base in information privacy within the Asian context, including laws and practices specific to the regions of Singapore, Hong Kong and India. Going one step further, the FIP designation signifies not only comprehensive knowledge of privacy laws, privacy program management and essential data protection practices but also a practitioner's significant experience in navigating the dynamic data protection industry.

www.bakermckenzie.com

Baker McKenzie Wong & Leow
8 Marina Boulevard
#05-01 Marina Bay Financial Centre
Tower 1
Singapore 018981

Tel: +65 6338 1888
Fax: +65 6337 5100