GATEWAY LAW CORPORATION
Advocates and Solicitors | Notary Public | Commissioners for Oaths
Patent, Design and Trade Mark Agents

39 Robinson Road
#20 – 03
Singapore 068911
Telephone: (65) 62216360
Facsimile: (65) 62216375

Technology, Media and Telecommunications Practice Update

Singapore's Personal Data Protection Regime: In a Nutshell

Overview

A little over 3 years since the provisions of the Personal Data Protection Act 2012 (the "PDPA") fully came into force, we have seen close to 40 decisions[1] that have been issued by the Personal Data Protection Commission (the "PDPC"), and counting. This article aims to discuss some of the implications these decisions may have on Singapore's personal data protection regime. But first, here is a quick recap of the important concepts in the PDPA.

1. Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access.

2. The PDPA establishes a data protection law that is made up of rules governing the collection, use, disclosure and care of personal data. It allows for individuals to protect their personal data (including rights of access and correction) as well as recognises the needs of organisations to collect, use or disclose personal data for legitimate and *reasonable* purposes.

3. The PDPA provides for the establishment of a national Do Not Call (DNC) Registry. The DNC Registry enables individuals to opt out of receiving marketing phone calls, mobile text messages such as SMS or MMS, and faxes from organisations. All one has to do is register one's Singapore telephone number(s) with the DNC Registry.

4. Every organisation needs to appoint a Data Protection Officer (DPO). The business contact information of the DPO must be made public.

5. Every organisation must develop and implement policies and practices in order to fulfil the obligations under the PDPA. Organisations must also develop a process to receive and respond to complaints that may arise in relation to matters under the PDPA and communicate the same to all staff in the

[1] As at October 2017

39 Robinson Road
#20 – 03
Singapore 068911
Telephone: (65) 62216360
Facsimile: (65) 62216375

organisation. In addition, said policies and practices as well as complaint process must be made available to the public on request.

6. The PDPA is largely premised on the following 3 key principles: -

- **Consent** – Organisations may collect, use or disclose personal data only with the individual's knowledge and consent (with some exceptions);
- **Purpose** – Organisations may collect, use or disclose personal data in an appropriate manner for the circumstances, and only if they have informed the individual of purposes for the collection, use or disclosure; and
- **Reasonableness** – Organisations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.

Breaches and Penalties

The PDPC is empowered to give any organisation directions if it thinks fit in the circumstances to ensure compliance with the PDPA. Apart from issuing warnings from time to time, from the line of decisions, the PDPC have issued directions to:-

(a) comply with the direction of the PDPC (*Re Tiger Airways Singapore Pte Ltd; SATS Ltd; Asia-Pacific Star Private Limited* [2017] SGPDPC 6; *Re National University of Singapore* [2017] SGPDPC 5); and/or
(b) pay financial penalty (*Re Aviva Ltd; Toh-Shi Printing Singapore Pte Ltd* [2016] SGPDPC 15; *Re JP Pepperdine Group Pte Ltd* [2017] SGPDPC 2).

Under the PDPA, the PDPC may direct an organisation to pay a financial penalty of up to S$1,000,000.00 if it thinks fit. Thus far, the highest sum of penalty imposed that we have seen is $50,000.00 (*Re K Box Entertainment Group Pte. Ltd.; Finantech Holdings Pte. Ltd.* [2016] SGPDPC 1).

It is observed that a breach of protection obligation– which usually comes in the form of failing to make reasonable security arrangements– tends to be heavily penalised. However, in assessing the breach and determining the directions to be imposed on the organisation from case to case, the PDPC takes into account several factors. Albeit a non-exhaustive list, these factors typically include:-

(a) the number of individuals affected or could have been impacted by the breach;
(b) whether such breach would expose (more) individuals to further risks;
(c) whether the organisation in question had made reasonable efforts to put in place improved security measures;

39 Robinson Road
#20 – 03
Singapore 068911
Telephone: (65) 62216360
Facsimile: (65) 62216375

(d) whether the organisation was generally cooperative and forthcoming in providing timely responses to the PDPC during the investigation;
(e) whether the organisation took prompt remedial action after being alerted to the data breach incident (as well as other corrective measures);
(f) whether on the facts, there were any mitigating factors for that particular case; and
(g) whether the personal data in question is considered to be sensitive in nature (although there is no statutory definition of "sensitive personal data").

Continued Developments

In developing the PDPA, references were made to the data protection regimes of key jurisdictions that have established comprehensive data protection laws, including the EU, UK, Canada, Hong Kong, Australia and New Zealand, as well as the OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, and the APEC Privacy Framework.

Today, we see that the PDPA is slowly developing into its own individual self, partly assisted by the growing body of "Advisory Guidelines" that the PDPC issues, in a bid to inject further clarity on various relevant topics in relation to this subject matter. Some of these Advisory Guidelines are doing more than just providing the baseline standard of protection for personal data that the PDPA aims to achieve. For instance, we now have other guides such as "Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data" as well as "Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data". Soon enough and once we can deal with the banal issues, we might just have a *Guide on Data Protection when Using a Drone* amongst other guides to address higher-level and complex issues.

Should you have any queries as to how this update may affect you or your organisation or require further information, please do not hesitate to email us.

Max Ng
Managing Director
Gateway Law Corporation

Email: max.ng@gateway-law.com

Amira Nabila Budiyano
Senior Associate
Gateway Law Corporation

Email: amira.budiyano@gateway-law.com