SINGAPORE'S PERSONAL DATA PROTECTION ACT: TIME TO TAKE IT SERIOUSLY

Date: 7 July 2016

Privacy, Data Protection and Information Management Alert

By: Christopher Tan, Andre Jumabhoy

This publication is issued by K&L Gates Straits Law LLC, a Singapore law firm with full Singapore law and representation capacity, and to whom any Singapore law queries should be addressed. K&L Gates Straits Law is the Singapore office of K&L Gates, a fully integrated global law firm with lawyers located on five continents.

1. Singapore's Personal Data Protection Act ("**PDPA**") established a general data protection law that governs the collection, use and disclosure of individuals' personal data by organisations. Under the PDPA, organisations are obliged to inform individuals of the collection of their personal data and the use that will be made of such information. Individuals must consent to the use of their personal data,[1] and an organisation may not refuse to provide its services or products on the basis that the individual refuses to do so, unless the provision of the information was "reasonable" to the provision of the product or the service in question.[2] Interestingly, an individual may withdraw his consent to the use of his personal data,[3] and has the right to require the organisation to disclose what personal information they possess and the use that has been made of that information.[4]

2. Under the PDPA, the organisation is under a duty to protect the personal data of an individual in its possession by making "reasonable security arrangements" to prevent unauthorised access,[5] and where it fails to do so, the Personal Data Protection Commission ("**PDPC**") is empowered under section 29(1) of the PDPA to make a number of directions, including:

> Prohibiting the organisation from collecting and disclosing personal data;
>
> Destroying personal data collected in contravention of the PDPA;
>
> Complying with any direction the PDPC may make to ensure compliance of the PDPA;[6] and
>
> Ordering the payment of a financial penalty of such amount not exceeding $1 million as the PDPC thinks fit.

3. The PDPA was passed in 2012 and came into force on 2 July 2014. So far, the PDPC has adopted a relatively "light-touch" approach to enforcement of the PDPA, up until recently.

4. On 21 April 2016, the PDPC published details of a spate of data enforcement actions taken against eleven organisations, including details of a financial penalty of $50,000 imposed on K Box Entertainment Group Pte. Ltd. ("**K Box**"), an operator of karaoke premises, for breaches of its protection obligation under the PDPA. K Box had collected large amounts of personal data from its customers including their full names, residential addresses and date of birth. They had engaged another company, Finantech Holdings Pte. Ltd. ("**Finantech**"), to collect and store the information on their behalf. However, when K Box required the information from Finantech for marketing or promotional information, Finantech would export the information from their server into an excel document and email that document, unencrypted, to K Box. This vulnerable means of data transmission led to the unauthorised disclosure of some 317,000 customer details.

5. On the same day that details of the enforcement actions were published, the PDPC also issued the Advisory Guidelines on Enforcement of the Data Protection Provisions ("the **Guidelines**"). Organisations would do well to have regard to the Guidelines, which are intended to provide guidance on the manner in which the PDPC will interpret the PDPA's provisions relating to the enforcement of the "**Data Protection Provisions**" (namely the provisions in the PDPA setting out the obligations of organisations in relation to data protection as set out in Parts III to VI of the PDPA).

6. The Guidelines make clear that when deciding whether to exercise its powers to enforce the Data Protection Provisions, the PDPC takes into account two main objectives: (1) the resolution of an individual's complaint; and (2) ensuring that organisations comply with the Data Protection Provisions. The factors that would prompt the PDPC to conduct an investigation into an organisation's failure to comply with its data protection obligations include, amongst others, the following:[7]

> whether the organisation's conduct indicates a systemic failure to comply with the PDPA or establish and maintain the necessary policies and procedures to ensure compliance;
>
> the number of individuals who are, or may be, affected by the organisation's conduct;
>
> the impact of the organisation's conduct on the individual who may be affected, for example, whether the individual may have suffered loss, injury or other damage as a result of the organisation's contravention of the PDPA or whether they have been exposed to a significant risk of the same;
>
> whether the organisation has been approached by the individual to seek a resolution; and
>
> the public interest in the PDPC conducting an investigation.

7. What is clear from the Guidelines and the recent spate of enforcement actions is that organisations need to take seriously the need to protect an individual's personal data and, where there have been lapses, take immediate and corrective steps to remedy the breach, which will include cooperating with any

investigation.

8. As the Guidelines make clear, the decision whether to impose a financial penalty on a defaulting organisation will depend on a number of factors, in particular "the seriousness and impact of the organisation's breach and the immediacy and effectiveness of corrective actions" to address the breach.[8]

9. It is important that organisations constantly review their data protection measures to ensure compliance as the PDPC will have regard to whether the organisation "had known or ought to have known of the risk of a serious contravention and failed to take reasonable steps to prevent it".

NOTES:

[1] Section 20 of the PDPA

[2] Section 14(2) of the PDPA. Note that there are various exceptions to the requirement that the individual consent to the collection and use of his personal data: see section 17 and the second, third and fourth schedule of the PDPA.

[3] Section 16 of the PDPA

[4] Section 21 of the PDPA

[5] Section 24 of the PDPA

[6] Section 29 of the PDPA

[7] Section 15.3 of the Guidelines

[8] Section 24.1 of the Guidelines

KEY CONTACTS

CHRISTOPHER TAN
PARTNER
K&L GATES STRAITS LAW LLC
SINGAPORE
+65.6507.8110
CHRISTOPHER.TAN@KLGATES.COM

