BAKER & MCKENZIE.WONG & LEOW

# Client Alert

May 2016

For further 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

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

**www.bakermckenzie.com**

## Guidelines on the Enforcement of the Data Protection Provisions

On 21 April 2016, the Personal Data Protection Commission ("**Commission"**) issued Advisory Guidelines on the Enforcement of the Data Protection Provisions ("**Guidelines**"), which outline the Commission's objectives and approach to enforcing the data protection provisions of the Personal Data Protection Act (the "**Act**").

The Commission also released its nine enforcement decisions on 21 April 2016, relating to the breach of the personal data protection obligations under the Act. The penalties imposed ranged from warnings for failure to obtain consent or put in place reasonable security measures to prevent the disclosure of personal data, to the imposition of financial penalties against organisations. The highest financial penalty to date imposed is against K Box Entertainment Group Pte. Ltd. ("**K Box**"), a Singapore karaoke chain that suffered a data breach of approximately 317,000 members' sensitive personal data in 2014. K Box was fined S$50,000 for breaching the protection and openness data protection obligations. The Commission also enforced the Act against K Box's data intermediary for breaching the protection obligation, namely, the failure to put in place reasonable security measures to provide adequate protection. The data intermediary was also fined S$10,000.

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

### Guidelines

The Guidelines clarify the objectives and approach the Commission will take when enforcing the Act. The Commission's objectives are to facilitate the resolution of an individual's complaint relating to an organisation's contravention of the Act and to ensure that organisations comply with the obligations imposed by the Act.

In the event of a complaint by an individual for contravention of the data protection provisions, the Guidelines provide that the Commission will attempt to facilitate a resolution between the individual(s) and the organisation prior to the Commission exercising its right of investigation under the Act. Such an approach may include referring the parties to mediation or directing parties to attempt to resolve the complaint. In the event that a complaint is resolved, the Commission will generally not proceed with an investigation unless, in the Commission's view, it is warranted.

When deciding whether to conduct an investigation, the Commission has indicated that it will take into account certain factors, including:

- Whether the organisation may have failed to comply, whether intentionally, negligently, or for any other reason, with all or a significant part of its obligations under the Act;

- Whether the organisation's conduct indicates a systematic failure to establish and maintain the necessary policies and procedures required under the Act;

- The number of individuals affected by the organisation's conduct and whether the affected individual may have suffered loss, injury or other damage;

- Previous contraventions of the Act; and

- Public interest.

In terms of investigation powers, the Commission is empowered to enter premises without a warrant in connection with an investigation. Notice to the relevant organisation is not required.

Following an investigation, the Commissioner has the discretion to issue directions to secure compliance with the Act, which includes the power to issue a financial penalty to the organisation. When exercising the discretion to direct an organisation to pay a financial penalty, the Commission will take into account the seriousness and impact of the organisation's breach, and the steps that the organisation has taken to address the breach (i.e. "aggravating" and "mitigating" factors). To assess the seriousness of the breach, the Commission will take an "objective approach" by considering how a reasonable organisation ought to have behaved in a particular situation.

The Guidelines also set out, amongst others, procedures relating to the reconsideration of a decision or direction of a decision issued by the Commission as well as in respect of appeals and the rights of private action by an aggrieved individual or organisation.

## Case Study – K Box

In the K Box decision, K Box was found to be in breach of the protection and openness data protection provisions. The Commission applied the Guidelines to consider whether a financial penalty was appropriate and considered the aggravating and mitigating factors of K Box's conduct. Aggravating factors in favour of a financial penalty included that the breach involved a large amount of sensitive personal data, and that K Box was not forthcoming in providing information during the investigation. Conversely, mitigating factors against imposing a financial penalty included that the remedial actions post data breach by K Box were fair and prompt.

Further, in the case of K Box's vendor processor (i.e. data intermediary), the Commission found the vendor to also be in breach of the protection obligation. The Commission reviewed the role and functions of the vendor, and considered that the vendor was expected to uphold a certain professional standard in relation to the protection of the K Box members' personal data. Failures on behalf of the data intermediary put K Box members' personal data at risk. The Commission viewed this breach as serious enough to justify a financial penalty of S$10,000 against the data intermediary.

## How This May Affect You

The Commission's willingness to enforce the Act sends a clear message to organisations in control of personal data, as well as data intermediaries, that the Commission will take any breach of the data protection obligations seriously. Organisations concerned about compliance with the Act should take action immediately to ensure compliance with the Act.

Although the Commission has awarded a number of financial penalties against organisations in breach of the Act, the Guidelines reinforce that the overall objective of the Act is to facilitate the resolution of complaints by individuals and to ensure an organisation's compliance with the Act, rather than to serve as a purely punitive instrument.

The Guidelines aim to educate organisations about the circumstances in which the Commission will view a complaint as serious enough to warrant an investigation, and the aggregating factors that must be present to warrant a financial penalty against an organisation.

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 Commission in any proceeding investigations. Based on the Guidelines, these steps may mitigate the financial penalty that may be awarded against an organisation which infringes the data protection obligations under the Act by the Commission.

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