Client Alert

July 2016

For further information please contact:

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

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

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

www.bakermckenzie.com

New Advisory Guidelines to Help Companies Better Protect Personal Data

On 20 July 2016, the Personal Data Protection Commission ("**PDPC**") introduced a new range of useful advisory guidelines to help companies better protect personal data in compliance with the *Personal Data Protection Act* 2012 ("**PDPA**").

The PDPC has issued three new guides, which are available on its website. These guides are about:

(a) disposing personal data on a physical medium;

(b) sample data protection clauses for data processing agreements; and

(c) building secure PDPA-compliant websites for small and medium enterprises ("SMEs")

Guide To Disposal of Personal Data On Physical Medium

This guide aims to educate companies that disposal refers to the overall process of transforming or destroying information in a way that renders it unreadable (for paper records) or irretrievable (for electronic records) and should not be taken lightly. For example, it does not mean simply discarding such records, whether physical or electronic, in the trash bin. This is because personal data can still be recovered through "dumpster diving" and/or an improperly cleared electronic trash bin. The guide also reminds companies not to overlook the protection of personal data contained on physical mediums (e.g. CD copies and paper printouts).

The guide recommends good practices that companies should adopt, such as:

i. checking recycled documents for any personal data that may allow the identification of an individual (even if such data may be inaccurate, outdated or incomplete);

ii. ensuring documents pending destruction are not left in an unsecured location or any location where a mix-up with recycled documents and/or unauthorised access may occur;

iii. supervising and documenting the collection of documents by a PDPA-compliant third party document disposal service provider (if such disposal is outsourced);

iv. using cross-cutting shredding machines to complicate attempts to reconstruct a shredded document containing personal data; and

v. utilising shredding, pulping and/or incineration disposal methods.

Guide On Data Protection Clauses For Agreements Relating To The Processing Of Personal Data

This guide provides sample data protection clauses that companies may consider adopting in their service agreements with the contractors engaged to provide data processing services on the companies' behalf. This is to ensure that the service agreements impose adequate obligations on these data processor contractors to ensure the companies can comply with their own PDPA obligations.

Guide On Building Websites For SMEs

This guide aims to assist SMEs building a website to ensure that websites which collect, use, disclose and store personal data are compliant with the PDPA. Where IT vendors are engaged to build such websites, the guide can be used by business owners to guide their discussion with their IT vendors. The guide reminds SMEs that website security and data protection are key design considerations at each stage of a website's life cycle.

Key considerations for SMEs to take note of include:

i. ensuring the confidentiality of the personal data handled by the website through confidentiality agreements and encryption;

ii. appropriate and regular security configuration of the website software and hardware components to prevent unauthorised access;

iii. regular penetration testing of website vulnerabilities and the prompt fixing of any vulnerabilities; and

iv. the implementation of access control schemes, server and network security measures, audit logs (for the detection of unauthorised activity) and incident response plans (in the event that website security and data protection are compromised).

Updated Guide on Securing Personal Data in Electronic Medium

In line with the three new guidelines, the "Guide To Securing Personal Data In Electronic Medium" has also been updated with a new list of good and enhanced practices that companies should adopt, such as:

i. the regular testing and application of updates and security patches to minimise security vulnerabilities;

ii. in respect of outsourcing, ensuring that (x) any "off-the-shelf" solutions and services selected offer appropriate protection to personal data; and/or (y) that vendors are made aware of the companies' security requirements through contractual clauses;

iii. ensuring that the security measures implemented by any cloud service providers provide reasonable security for the personal data;

iv. requiring cookie data and URL validation and prohibiting "backdoors" in websites and web applications that would allow access to personal data without proper user authentication;

v. periodically reviewing the encryption used for databases and email to ensure it remains relevant and secure; and

vi. implementing additional controls for shared computers to restrict access to personal data.

Although the use of the above resources does not mean that companies will automatically comply with the PDPA, companies will benefit from the added clarity and useful practical data protection guidelines in respect of meeting their PDPA obligations. In particular, companies should ensure that the sample data protection clauses for data processing agreements and good/enhanced practices implemented should be properly adapted to suit their companies' particular circumstances and needs.