CLIFFORD
CHANCE

Briefing note June 2012

Singapore's new personal data protection legislation and how it compares to data protection legislation in other jurisdictions

Introduction

The Singapore Ministry of Information, Communications and the Arts ("**MICA**") has released the much-anticipated draft Personal Data Protection Bill ("**Draft Bill**"). Parliament is expected to pass the Draft Bill in the third quarter of 2012.

The introduction of personal data protection legislation in Singapore is considered by many to be a timely move in light of the high-profile thefts of customer personal data from companies such as Sony Corporation and UK-based Codemasters. Prior to this, Singapore did not have any over-arching legislation to protect personal data.

The Draft Bill when passed will be known as the Personal Data Protection Act ("**PDPA**"). While the PDPA is intended to be a baseline law which will operate along with the existing sector specific laws, the PDPA is fairly ambitious in proposing to extend its provisions to organisations which may not be physically located in Singapore but are engaged in data collection, processing or disclosure of such data within Singapore.

The main features of the PDPA (as set out in the Draft Bill) are:-

(a) the establishment of a Data Protection Commission ("**DPC**") to administer and enforce the PDPA;

(b) the application of the PDPA to all private sector organisations in Singapore as well as all organisations located outside of Singapore that are engaged in data collection, processing or disclosure of such data within Singapore;

(c) the requirement of at least one designated individual within each organisation to be responsible for compliance with the PDPA ("**Personal Data Officer**");

(d) the requirement for organisations to implement policies and practices to comply with the PDPA;

(e) introduction of general rules and exclusions relating to the collection, use and/or disclosure of personal data;

(f) to allow individuals to request access to their personal data held by an organisation in order to find out how organisations have used or are using the personal data collected, to correct any inaccurate information collected and to seek redress for suspected breaches of the PDPA;

(g) introduction of a penalty and enforcement regime for breaches of the PDPA; and

(h) introduction of the Do Not Call Registry ("**DNC Registry**").

Establishment of the DPC

The PDPA establishes the DPC for amongst other purposes, to administer and enforce the PDPA. Members of the DPC are appointed by the Minister of Information, Communication and the Arts. The powers of the DPC include the power to enter into any co-operation agreement with a regulatory authority. Such a co-operation agreement may include provisions to enable each regulatory authority to furnish to the other regulatory authority information in its possession if the information is required by that other authority for the performance of any of its functions.

Application of the PDPA

The PDPA is intended to apply to all private-sector organisations in Singapore as well as all organisations located outside of Singapore that are engaged in data collection, processing or disclosure of such data within Singapore. While MICA acknowledged there may be difficulty in enforcement against organisations with no physical presence in Singapore, it was thought that extending coverage to overseas organisations would act as necessary deterrence.

Designation of Personal Data Officers within organisations

A key feature of the PDPA is the requirement for organisations to appoint at least one Personal Data Officer to be responsible for ensuring compliance with the PDPA. The business contact information of the designated Personal Data Officer(s) must be made available to the public. Notwithstanding the designation of Personal Data Officer(s), the organisation ultimately remains responsible for complying with its obligations under the PDPA.

Implementation of policies and practices to ensure compliance with the PDPA

Under the PDPA, organisations are required to develop and implement policies and practices that are necessary to comply with their obligations under the PDPA. In addition, organisations shall develop a complaint process to receive and respond to complaints that may arise. Such policies and practices must be communicated to the staff in the organisation and this may be done by way of the appropriate mention in the relevant employee manuals or by posting on the staff portal or intranet as the case may be.

Rules and exclusions relating to the collection, use and/or disclosure of personal data

Requirement of consent

The PDPA imposes a general requirement to obtain consent for the collection, use and/or disclosure of personal data. Data which had been previously collected is exempt from this requirement. However, fresh consent is required for such data if there has been a change in the original purpose for which the data was collected.

The PDPA prohibits organisations from requiring an individual to consent to the collection, use and/or disclosure of personal data as a condition of supplying the product or service to the individual beyond what is reasonable to provide the product or service in question.

According to MICA, organisations are expected to clearly state the purpose(s) for which they propose to collect, use and/or disclose the personal data. The stated purpose(s) must be reasonable in scope and must not be overly broad. Consent may be deemed to have been given if the personal data was voluntarily provided and it is reasonable that the individual would have voluntarily provided the data. Critically, the failure by an individual to object to the collection, use and/or disclosure of personal data within a reasonable timeframe is not considered to be deemed consent.

Withdrawal of consent

The PDPA provides that an individual may withdraw consent to the use and/or disclosure of personal data at any time. However, such withdrawal will only apply to the prospective use and/or disclosure of the data collected.

Exclusions on consent

The PDPA provides for certain exclusions to the requirement of consent. The key exclusions include:-

(a) the collection, use or disclosure of personal data for artistic or literary purposes;

(b) the collection, use or disclosure of personal data made available by a public agency but only where it is consistent with the original purpose for which such data was made available by the public agency;

(c) the collection, use or disclosure of personal data by news organisations in the course of a news activity;

(d) the collection, use or disclosure of personal data for the purpose of establishing an employment relationship; and

(e) the collection, use or disclosure of personal data for beneficiaries of insurance policies and trusts.

Access to and correction of personal data

The PDPA allows individuals the right to request access to their personal data held by organisations and to find out how the organisations have used or are using the personal data collected as well as to correct any inaccuracies in the data collected.

Where the personal data collected has been disclosed to a third party, the organisation shall provide the individual with the list of third parties which the personal data may have been disclosed to. With regard to any inaccuracy in the data collected, an organisation should take steps to correct such inaccuracy at the request of the individual concerned. The corrected data should then be sent to any other third party organisation which the previous data had been disclosed to.

Penalty and enforcement regime

The DPC has the power to review complaints made against organisations and to give the appropriate directions accordingly. The DPC has the power to direct a non-complying organisation to pay a financial penalty of up to S$1 million. For the purposes of enforcement of any direction made by the DPC, an application may be made by the DPC to the District Court to register such direction.

Any individual who suffers loss or damage directly as a result of an organisation contravening the provisions of the PDPA shall have a right to take civil action against the organisation but only after the DPC's decision on the said contravention has become final.

DNC Registry

The PDPA provides for the setting up of a DNC Registry – the first of its kind in Singapore. The DNC Registry will consist of one or more registers for individuals to register their Singapore telephone numbers in order to stop receiving marketing messages. These registers cover messages addressed to a Singapore telephone number and therefore would not include messages delivered by post.

The DNC Registry adopts an "opt-out" approach such that individuals who do not wish to receive marketing messages should register their Singapore telephone numbers with the DNC Registry and the onus lies on organisations to check with the DNC Registry before sending such messages. A message addressed to a Singapore telephone number shall not be sent unless confirmation had been applied for and received from the DPC 30 days before sending the message that the number concerned is not listed in the relevant register.

Sunrise period

There will be a sunrise period of at least 18 months after the PDPA is enacted to allow organisations to implement the necessary policies to comply with the PDPA. In addition, MICA is expected to issue guidelines to provide further clarification on the operation of the PDPA in due course.

Comparison between the PDPA and other data protection legislation

Jurisdiction	Existence of data protection legislation	Types of data covered	Entities covered	Penalties
Australia	The primary legislation is the Privacy Act 1988 (Cth) which is supported by the Privacy (Private Sector) Regulations 2001 and the Privacy Regulations 2006. The Privacy Act 1988 (Cth) does not regulate State or Territory agencies, except for the Australian Capital Territory. The States and Territories also have their own privacy laws and regulations. There are also a number of other laws that link the privacy laws to particular types of personal data and data collection, including the Telecommunications Act 1997 (Cth) and the Personal Property Securities Act 2009 (Cth).	Personal information: which is information that does or can identify a person such as name and address and other information which may be collected or held by government or by private enterprise including medical, tax and insurance records, bank account details, photos, and information about personal preferences, opinions or, where the person works.	Any individual, organisation or agency both public and private, that collects, holds, processes, manages or uses personal data is regulated in relation to those activities. The legislation gives individuals rights in relation to their personal information including access and ensuring use only for the purposes they have been told about.	Injunctions, damages, imprisonment or any order as the court may see fit. Case by case conciliation through the Office of the Australian Information Commission may also result in compensation to individuals and/or specific practices being imposed on data collectors and users against which a complaint has been made.
European Union	The European Union (EU) Data Protection Directive (EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) Implemented by local law in each country (Proposal to replace with EU Regulation from circa. 2015).	Information relating to 'an identifiable person'. This includes information about a natural person directly identified by an identification number or indirectly with one or more facts that relate to his 'physical, physiological, mental, economic, cultural, or social identity'.	Persons or entities which collect and process personal data. "Controllers", who determine the purposes and means of processing. Some countries also apply some rules to "processors", who process on behalf of controllers. Proposed Regulation would extend obligations of processors.	Criminal penalties, including imprisonment; fines; DPA enforcement orders; civil damages. Proposed Regulation would introduce substantial fines, linked to global turnover.
Hong Kong	The Personal Data (Privacy) Ordinance and the Code on Access to Information.	Any representation of information (including an expression of opinion) in any document relating to a living individual from which it is practicable for his/her identity to be ascertained.	Any person or organisation, both public and private, that collects, holds, processes or uses personal data The Code on Access to Information applies to government departments (excluding courts,	Fines and compensation. Offenders may also be sentenced to imprisonment.

Jurisdiction	Existence of data protection legislation	Types of data covered	Entities covered	Penalties
			tribunals and inquiries).	
Japan	The Act on the Protection of Personal Information 2003.	Personal information that constitutes a database; i.e. information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information.	Persons/entities that use a personal information database, which contains information on more than 5,000 individuals, for business at any time within the past 6 months.	Monetary fines or any order issued by the competent minister and/or regulatory measures. Offenders may also be sentenced to imprisonment.
People's Republic of China ("PRC")	No over-arching data protection legislation. However, limited data protection provisions may be found in the PRC Constitution and the judicial interpretation by the Supreme People's Court ("SPC").[1]	The Constitution provides for freedom and privacy of telecommunication and correspondence (subject to national security and criminal offences). The SPC Opinions have held that a party will be liable for publicising another individual's matters of "privacy", if doing so causes damage to the latter's reputation and honour.		
	In addition, the *Amendment (VII) to the Criminal Law of the PRC* promulgated in 2009 makes it a criminal offence to sell or illegally obtain personal information and to illegally obtain personal information by using one's position in any state organ or financial, telecommunication, medical, educational or transportation institutions.	Personal information.	Staff member of a state organ or an entity in such a field as finance, telecommunications, transportation, education or medical treatment.	Fixed-term imprisonment (up to 3 years) or criminal detention, and/or financial penalty.
	Order No. 20, *'Several Provisions Regulating the Market Order of Internet*	'Users' personal data' includes data capable of identifying the user	Internet information service providers.	Financial penalty of up to RMB 30,000 (approx. €3, 598).

[1] A draft law is being deliberated at the National's People's Congress but there is no indication when the law will be passed.

Jurisdiction	Existence of data protection legislation	Types of data covered	Entities covered	Penalties
	Information Services' - issued by the Ministry of Industry and Information Technology (which took effect on 15 March 2012) also prohibits internet service providers from collecting processing, storing and disclosing users' personal data to third parties without the user's permission.	either by itself or combined with other information.		
Singapore	The proposed PDPA as well as various other sector specific laws.	The PDPA covers all forms of personal data including both electronic and non-electronic forms.	All private sector persons, companies and organisations in Singapore as well as organisations located outside Singapore and engaged in personal data collection and processing in Singapore.	Financial penalty of up to S$1 million in addition to any other orders made by the DPC.
Thailand	No over-arching data protection legislation. However, some data protection provisions may be found in – (i) The Constitution of Thailand; (ii) The Credit Bureau Act; (iii) The Official Information Act; (iv) The Criminal Code; (v) The Civil and Commercial Code (tort law); (vi) The Citizen Registration Act; and (vii) various other sector-specific laws and regulations.[2]	(i) Personal data kept with the Credit Bureau or provided to and used by financial institutions/ securities companies/ insurance companies; (ii) personal data (physiological information, education, health record, criminal record, information that can identify a person) disclosed by government entities; and (iii) information collected for the purpose of telecommunication law.	Any individual, entities or state agency that collects, holds, access, processes, manages or uses personal data.	Financial penalties, compensation or imprisonment.

Conclusion

The PDPA is an important piece of legislation that all organisations should review and be familiar with due to the likely impact of the PDPA on their operations. Please contact us for a discussion if you would like more information about the PDPA or if you would like to discuss the possible implications that the PDPA may have on you or your business.

[2] A draft Protection of Personal Data Act has been in the drafting process for the last 10 years.

Contacts

Martin Rogers
T: +852 2826 2437
E: martin.rogers@cliffordchance.com

Cameron Hassall
T: +852 2826 2459
E: cameron.hassall@cliffordchance.com

Patrick Zheng
T: +86 10 6535 4998
E: patrick.zheng@cliffordchance.com

Nish Shetty
T: +65 6410 2285
E: nish.shetty@cliffordchance.com

Diana Chang
T: +61 2 8922 8003
E: diana.chang@cliffordchance.com

Tim Grave
T: +61 8922 8028
E: tim.grave@cliffordchance.com

Ben Luscombe
T: +61 9262 5511
E: ben.luscombe@cliffordchance.com

Simon Greenberg
T: +33 1 4405 5114
E: simon.greenberg@cliffordchance.com

Lena Ng
T: +65 6410 2215
E: lena.ng@cliffordchance.com

Kathryn Sanger
T: +852 2826 3404
E: kathryn.singer@cliffordchance.com

William Langran
T: +852 2825 8804
E: william.langran@cliffordchance.com

Mingfen Tan
T: +65 6410 2298
E: mingfen.tan@cliffordchance.com