Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 14, NUMBER 5 >>> MAY 2014

Privacy Laws in Asia

By Cynthia Rich, of Morrison & Foerster LLP, Washington.

Editor's Note: In this first part of a three-part Special Report on the status of data privacy laws in Asia, Latin America, the Caribbean, Africa and the Middle East, the author explores developments in Asia, where several countries have either enacted new laws or amended existing laws in the past few years.

Privacy rules in Asia are changing at a rapid pace. In the past three years alone, five countries have enacted brand new laws, and three countries or jurisdictions have amended existing laws to address emerging issues such as data breaches and direct marketing. Prior to this, only six laws were adopted in a 13–year period. Eleven jurisdictions in Asia now have comprehensive data privacy laws: Australia (amended), Hong Kong (amended), India (new), Japan, Macau, Malaysia (new), New Zealand, the Philippines (new), Singapore (new), South Korea (new) and Taiwan (amended).

While all of these laws are based on core data protection principles, the specific rules are quite different from each other and from laws found in other parts of the world. For example, unlike their European, Latin American and African counterparts, countries in Asia have largely eschewed registration requirements. However, like their European, Latin American and African counterparts, they have embraced cross-border restrictions and breach notification obligations, contrary to the approaches found until now in the established Asian privacy regimes. Moreover, in the wake of growing data breaches, laws with detailed security obligations continue to grow.

Implications for Businesses

Given the variances among these new privacy laws, businesses with operations in the region will want to re-examine their privacy policies and practices to ensure they will comply with these new regimes. Programs that comply only with the more established Asian or European regimes will run afoul of many of these new country obligations.

The European approach to privacy—establishing a limited set of conditions or legal bases for processing and imposing cross-border restrictions—is clearly being embraced by more countries in Asia. However, these countries are developing their own unique interpretations, which can present compliance challenges for companies seeking to establish global privacy approaches.

For example, the Philippines requires European-like legal bases for processing but exempts important sectoral activities or processing and provides for more flexible cross-border rules. Singapore has established a consent-based privacy regime, but the law provides for a complex array of exceptions that should give busi-

nesses considerable flexibility. In contrast, the Malaysian approach, which is perhaps the most closely aligned with the European approach, may impose more stringent requirements (*e.g.,* there is no provision for processing personal information to pursue legitimate business interests). In addition, Malaysia is now the second jurisdiction in the region (Macau was the first) to require registration of data processing activities.

Organizations will also need to adjust existing practices in a few jurisdictions with mature privacy regimes, particularly with respect to direct marketing and the processing of sensitive data.

It is hard to know precisely how all of these jurisdictions will implement and enforce these rules. As businesses begin to review and modify their practices in these jurisdictions, they will want to pay close attention to actions by the regulatory authorities in the months ahead.

Overview

Before discussing in detail the three most recent laws enacted in the region (in Malaysia, the Philippines and Singapore), this Special Report provides an overview of the other eight Asian jurisdictions that have established privacy regimes (Australia, Hong Kong, India, Japan, Macau, New Zealand, South Korea and Taiwan).

Established Privacy Regimes

AUSTRALIA

In 2000, Australia amended its Privacy Act 1988 (Australia Law), regulating public sector processing of personal information of natural persons, to cover processing by the private sector.[1] Under the Australia Law, the private sector must collect and use personal information in accordance with the National Privacy Principles (NPPs); the public sector is subject to a different set of principles, known as the Information Privacy Principles. The NPPs impose the usual range of obligations such as notice, consent, collection and use limitations, access and correction rights, data security, data retention and data integrity; however, there are no registration obligations. The protections provided by the NPPs apply to all personal information of natural persons except "acts or practices in relation to employee records of an individual if the act or practice directly relates to a current or former employment relationship between the employer and the individual."

In 2012, the Australia Law was amended again to replace the current privacy principles for the public and private sectors with a single set of privacy principles, referred to as the Australian Privacy Principles (APPs) (*see analysis at WDPR, December 2012, page 4*).[2] The amendment also implemented a comprehensive credit reporting system that provides for codes of practice under the APPs and a credit reporting code, and gives the Information Commissioner authority to develop and register codes that are binding on specified agencies and organizations. The amendments clarify the functions and powers of the Information Commissioner and improve the Information Commissioner's ability to resolve complaints, recognize and encourage the use of external dispute resolution services, conduct investigations and promote compliance with privacy obligations. Two more rounds of amendments are expected; however, there is no timetable for their development and enactment. The existing exemption for employee records remains intact; the intention is to revisit this issue in subsequent rounds.

One of the significant changes to the Australia Law is the extension of the APPs to cover overseas handling of personal information by an organization if it has an "Australian link." An organization has an Australian link if the organization is:

- an Australian citizen;
- a person whose continued presence in Australia is not subject to a limitation as to time imposed by law;
- a partnership formed in Australia or an external territory;
- a body corporate incorporated in Australia or an external territory; or
- an unincorporated association that has its central management and control in Australia or an external territory.

An organization that does fall within one of the above categories will also have an Australian link where:

- the organization carries on business in Australia or an external territory; and
- the personal information was collected or held by the organization in Australia or an external territory, either before or at the time of the act or practice.

According to the Information Commissioner's recently released guidelines (*see analysis at WDPR, March 2014, page 7*), activities that may indicate that an entity with no physical presence in Australia carries on business in Australia include:

- the entity collects personal information from individuals who are physically in Australia;
- the entity has a website that offers goods or services to countries including Australia;
- Australia is one of the countries on the drop-down menu appearing on the entity's website; or
- the entity is the registered proprietor of trademarks in Australia.[3]

Where an entity merely has a website that can be accessed from Australia, this is generally not sufficient to establish that the website operator is "carrying on a business" in Australia.

[Editor's Note: The Australian government announced May 13, 2014, that it will abolish the Office of the Australian Information Commissioner, and that its privacy functions will be undertaken in the future by the Privacy Commissioner as an independent statutory position within the Australian Human Rights Commission (see report in this issue).]

   ISSN 1473-3579

HONG KONG

Hong Kong was the second jurisdiction in Asia to enact a comprehensive data protection law, in 1995. The Personal Data (Privacy) Ordinance (Hong Kong Law) protects all personal information of natural persons and applies to both the private and public sectors.[4] It imposes the usual range of obligations such as notice, consent, collection and use limitations, access and correction rights, data security, data retention and data integrity; however, there are no registration obligations. While the Hong Kong Law contains a provision that limits the transfer of personal information to places outside Hong Kong that do not provide data protection similar to that under Hong Kong law, it is not yet in force and there is no schedule as to when it will come into force. Consequently, transfers both within and outside Hong Kong are governed by general legal restrictions on data collection and data use.

The Hong Kong Law was amended in 2012 (*see analysis at WDPR, July 2012, page 4*). One of the most significant changes was to regulate more closely the use and provision of personal information in direct marketing activities. Under the new direct marketing rules, an organization can use or transfer personal information for direct marketing purposes only if that organization has provided the required information (notice) and consent mechanism to the individual concerned and obtained his or her consent. "Consent" in the direct marketing context includes an indication of no objection to the use (or provision); however, written consent is required prior to providing personal information to others for their direct marketing purposes. Failure to comply with these requirements is a criminal offense, punishable by fines of HK$500,000 (U.S.$64,483) and three years' imprisonment. In cases involving transfer of personal data for gain, a fine of HK$1 million (U.S.$128,966) and five years' imprisonment are possible.

INDIA

In 2011, India issued final regulations implementing parts of the Information Technology (Amendment) Act, 2008, dealing with the protection of personal information (*see analysis at WDPR, May 2011, page 11*). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India Privacy Rules) prescribe how personal information may be collected and used by virtually all organizations in India, including personal information collected from individuals located outside India.[5] The India Privacy Rules impose requirements with respect to notice, choice, data security, data retention, purpose limitation, access and correction rights and cross-border transfers. Database registration is required. While the consent rules apply only to sensitive information, sensitive information is very broadly defined and includes information that is not generally regarded as sensitive in other jurisdictions.[6]

The India Privacy Rules raised significant issues and caused concern among organizations that outsource business functions to Indian service providers. As drafted, the India Privacy Rules apply to all organizations that collect and use personal information of natural persons in India regardless of where the individuals reside or what role the company that is collecting the information plays in the process of handling the information. In particular, the provisions apply to a "body corporate," which is defined as "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities," as well as, in many instances, "any person on its behalf." As a result, industry both within and outside India expressed concern that the India Privacy Rules would decimate the outsourcing industry.

In response to these concerns, on Aug. 24, 2011, the Indian Ministry of Communications & Information Technology issued a clarification of the India Privacy Rules (Clarification), stating that the India Privacy Rules apply only to organizations in India (*see WDPR, September 2011, page 24*).[7] Therefore, if an organization in India receives information as a result of a direct contractual relationship with an individual, all of the obligations under the India Privacy Rules continue to apply. However, if an organization in India receives information as a result of a contractual obligation with a legal entity (either inside or outside India)—*e.g.,* is acting as a service provider—the substantive obligations of notice, choice, data retention, purpose limitation, access and correction do not apply, but the security obligations and the obligations relating to the transfer of information do apply.

With respect to cross-border transfers, a company may transfer sensitive personal information or information to any other body corporate or a person in India or to another country that ensures the same level of data protection that is adhered to the body corporate as provided by these India Privacy Rules. The transfer may be allowed only if it is necessary for the performance of the contract between the body corporate or its agent and the provider of the information *or* where the person has consented to the transfer.

JAPAN

Japan's Protection of Personal Information Law (Japanese Law) took effect in April 2005 and regulates the handling of personal information of natural persons by private sector organizations that "use personal information databases in their business operations," and such databases contain information on 5,000 or more individuals on any day in the past six months.[8] Businesses must provide notice about the purposes for which they collect and use information, adopt security control measures, respond to access and correction requests from individuals and establish a complaint handling system. Unlike the EU Data Protection Directive (95/46/EC), the Japanese Law does not impose additional requirements on cross-border data transfers or require registration of databases.

There are some other noteworthy differences with respect to the provision of notice and consent. Unlike in other jurisdictions, notice may be provided directly to the individual or through a public announcement. Consent is not required, provided the purposes of use have been previously specified (such as in a notice or public

announcement). Opt-in consent is required for purposes of use beyond what can be reasonably imagined by the individual, or beyond the extent necessary to achieve the specified purpose of use. To share information with third parties, a business must obtain consent to share information with third parties (or provide the individual with the ability to opt out of such sharing if such sharing was included in a previous notice and made part of the stated purpose of use). In addition, the Japanese Law establishes a role for Approved Personal Information Protection Organizations (akin to dispute resolution bodies) that are required to respond promptly to individual complaints. Local public entities will mediate when complaints cannot be resolved by businesses and/or Approved Personal Information Protection Organizations.

Like other Japanese basic laws, the Japanese Law is framework legislation and delegates discretion to national administrative agencies and local governments to develop implementing regulations to accomplish the purposes of the law. At least 40 guidelines for 27 areas have been promulgated. Such guidelines include those issued by the Ministry of Economy, Trade and Industry; the Ministry of Internal Affairs and Communications (formerly the Ministry of Public Management, Home Affairs, Posts and Telecommunications); the Ministry of Finance; the Ministry of Health, Labor and Welfare; and the Ministry of Land, Infrastructure, Transport and Tourism. These guidelines detail specific obligations and recommendations. The guidelines contain both mandatory and voluntary provisions. As a result, businesses operating in Japan must carefully examine the guidelines issued by the competent ministries under whose jurisdiction they operate. A business may be subject to multiple guidelines depending on the scope of its business operations, and the provisions of such guidelines may not be the same; in fact, they may actually conflict.

MACAU

The Personal Data Protection Act (Macau Law), which took effect in 2006, made Macau the first jurisdiction in Asia to adopt an EU-style data protection law.[9] Virtually all of the provisions (notice, consent, collection and use, data security, data integrity, data retention, access and correction, cross-border limitations and registration) closely follow the requirements found in EU laws. The Macau Law applies to both public and private sector processing of the personal information of natural persons. Macau was the first jurisdiction in the region to require registration and impose EU-style cross-border restrictions.

NEW ZEALAND

New Zealand was the first country in the region to enact a data protection law applicable to the processing of personal information by the private sector. The Privacy Act 1993 (New Zealand Law), which regulates the processing of all personal information of natural persons by both the public and private sectors, is also the first and only law in Asia to be recognized by the EU as providing an adequate level of protection for personal data transferred from the EU/European Economic Area.[10] This adequacy determination was issued after New Zealand amended its law in 2010 to establish a mechanism for controlling the transfer of personal information outside New Zealand in cases where the information has been routed through New Zealand to circumvent the privacy laws of the country from where the information originated (*see WDPR, January 2013, page 25*).

The New Zealand Law requires that notice be provided, but does not require individuals to consent to their personal information being collected, transferred or used in a certain manner, provided the notice obligations are complied with. However, like the Hong Kong Law, if notice is not provided at the time the information is collected, and an exception does not apply, the individual's consent will be required for the use, processing, disclosure and transfer of the information. Also similar to the Hong Kong Law, sensitive personal information is not treated differently than other personal Information under the New Zealand Law.

The New Zealand Law also imposes basic requirements regarding collection and use, data security, data integrity, data retention and access and correction, but there are no registration and cross-border transfer requirements.

SOUTH KOREA

The Data Protection Act (Korean Law), which took effect in September 2011 (*see analysis at WDPR, September 2011, page 6*), regulates public and private sector processing of the personal information of natural persons.[11] The Korean Law does not require database registration, but does impose extensive obligations in a number of areas such as notice, consent and data security. In particular, prior notice and express consent are required to collect, use and transfer personal information. The notice must separately detail the collection and use of personal information, third-party disclosures (including any cross-border disclosures), processing for promotional or marketing purposes, processing of sensitive information or particular identification data (such as resident registration number and passport number), disclosures to third-party outsourcing service providers and transfers in connection with a merger or acquisition. The individual must consent separately to each item. The uses that do not require consent must be distinguished from those that do require consent.

The Korean Law and subsequent guidance issued by the regulatory authorities also impose significant data security obligations. For example, organizations are required to encrypt particular identification data, passwords and biometric data when such data are in transit or at rest. If personal information is no longer necessary after the retention period has expired or when the purposes of the processing have been accomplished, the organization must, without delay, destroy the personal information unless any other law or regulation requires otherwise. In addition, when becoming aware of a data security breach, the organization must, without delay, notify the relevant individuals, prepare measures to minimize possible damages and, when the volume of affected data

   ISSN 1473-3579

meets or exceeds a threshold set by executive order (*i.e.,* in the case of a leak involving 10,000 or more individuals), notify the regulatory authorities.

There are a few different agencies actively involved in overseeing compliance with the law: the Ministry of Security and Public Administration (MOSPA), the Data Protection Commission, the National Information Society Association and the Korea Internet & Security Agency. A government-wide joint task force team consisting of officials specialized in data protection matters from the MOSPA, the Korea Communications Commission, the Financial Services Commission and the police has also been established to investigate illegal leaks, sales or purchases of personal information.

TAIWAN

Taiwan's Personal Data Protection Act (Taiwanese Law) entered into effect in October 2012 (*see analysis at WDPR, December 2012, page 9*).[12] The Taiwanese Law replaced the 1995 Computer Processed Personal Data Protection Act that regulated computerized personal information in specific sectors such as the financial, telecommunications and insurance sectors. The Taiwanese Law now provides protection to the personal information of natural persons across all public and private entities and across all sectors. Because of public concerns about the rules pertaining to the use of sensitive personal information and personal information collected prior to the enactment of the new law, the government has delayed implementation of these provisions.

The Taiwanese Law imposes the usual range of obligations such as notice, consent, collection and use limitations, access and correction rights, data security, data retention and data integrity; however, there are no registration obligations or cross-border restrictions. In addition, there is a breach notification requirement. Individuals must be notified when their personal information has been stolen, divulged or altered without authorization, or infringed upon in any way.

New Privacy Regimes

MALAYSIA

Overview

The Personal Data Protection Act (Malaysian Law) was enacted in 2010 but did not come into effect until November 2013 (*see analysis at WDPR, December 2013, page 9*); organizations were given three months (until Feb. 15, 2014) to comply.[13] The Malaysian Law protects all personal information of natural persons processed in respect to commercial transactions that are 1) processed in Malaysia and 2) processed outside Malaysia where the data are intended to be further processed in Malaysia.

A "commercial transaction" is defined as:

> any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a Credit Reporting Business carried out by a Credit Reporting Agency under the Credit Reporting Agencies Act 2009.

Given this definition, there has been much speculation about whether this law would apply to the processing of human resources data. While no official guidance has been issued, all indications are that the Malaysian Law does apply to human resources data.

The Malaysian Law is quite similar to the reach of most European laws except that it does not apply to personal information processed by federal and state governments.

Notice and Consent

Organizations acting as data controllers (referred to as Data Users) must provide notice to individuals whose personal information is collected and processed as soon as practicable, but specifically prior to or at the time the organization uses the information for a purpose other than that for which it was originally collected or discloses the information to a third party.

Consent is required to process personal information unless an exception applies. Explicit consent is required to process sensitive personal information. The individual has the right, at any time, to revoke his or her consent or require the organization to cease or not begin processing his or her personal information for direct marketing purposes. Consent is not defined in the Malaysian Law. The legal bases listed in the Malaysian Law correspond with many of those found in European data protection laws. For example, organizations may process personal information without consent when the processing is necessary to fulfill a contract to which the individual is a party or to take steps at the request of the individual prior to entering into a contract. However, unlike a number of European laws, there is no provision in the Malaysian Law for processing personal information without consent when it is necessary to pursue the organization's (or a third party's) legitimate business interests.

Data Security and Data Retention

The organization must take all reasonable steps to protect personal information it processes from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. When organizations hire service providers to process personal information on their behalf, they must ensure that the service providers provide sufficient guarantees regarding the technical and organizational security measures governing the processing and take reasonable steps to ensure compliance with such measures.

Personal information may not be kept longer than necessary to fulfill the purposes for which it was collected. Further, the organization must take all reasonable steps to ensure that all personal information is destroyed or permanently deleted if it is no longer required for the purposes for which it was collected.

Access and Correction Rights

Individuals have the right to access and correct their personal information where the personal information held is inaccurate, incomplete, misleading or not up-to-date. The organization must comply with the request where it is satisfied that the personal information is inaccurate, incomplete, misleading or not up-to-date. Interestingly, where the personal information has been disclosed to a third party (and the third party is believed to be using it for purposes (or directly related purposes) for which it was disclosed) within 12 months of when the correction is made, the organization must supply the third party with a copy of the personal information as corrected, accompanied by a written notice stating the reasons for the correction. This obligation to notify third parties goes well beyond the obligations in most older data protection laws.

Cross-Border Data Transfers

Organizations may transfer personal information only to countries outside Malaysia that have been approved by the Minister of Communications and Multimedia (Minister) unless an exception applies. The exceptions largely mirror those found in many European laws such as:

- the individual has consented to the transfer;
- the transfer is necessary to perform a contract with or at the request of an individual;
- the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
- the transfer is necessary in order to protect the vital interests of the individual; or
- the organization has taken all reasonable precautions and exercised all due diligence to ensure that the personal information will not be processed in any manner which, if the data were processed in Malaysia, would be a contravention of the Malaysian Law.

Approved countries will be published by the Minister in the official Gazette.

Establishment of Data Protection Authority

The Malaysian Law provides for the establishment of a Personal Data Protection Commissioner (Malaysian Commissioner) responsible for regulating and overseeing compliance with the law, and a Personal Data Protection Advisory Committee charged with advising the Malaysian Commissioner on all matters relating to data protection and administration and enforcement of the law.

Database Registration

Data Users (mainly licensed organizations) from the following sectors are required to register: communications; banking and financial institutions; insurance; health; tourism and hospitalities; transportation; education; direct selling; services (such as legal, audit, accountancy, engineering or architecture, retail or wholesale dealing as defined under the Control Supplies Act 1961); private employment agencies; real estate; and utilities.

Penalties

Failure to comply with the requirements of the Malaysian Law can result in criminal and administrative penalties. Criminal sanctions include fines of up to 500,000 Malaysian ringgits (approximately U.S.$164,000) and/or two years of imprisonment. Organizations are liable for offenses under the law; directors, chief executive officers, chief operating officers, managers, secretaries or other similar officers of the organization may be charged severally or jointly in the same proceedings, and, where the organization is found guilty of the offense, individuals will also be deemed to have committed the offense unless they can prove otherwise. In addition, the Malaysian Commissioner may serve an enforcement notice directing the organization to take steps to remedy any contraventions of the Malaysian Law within a specified time period, and may order processing of personal information to cease pending such a remedy.

There is no right to private action under the law.

THE PHILIPPINES

Overview

Philippine President Benigno Aquino signed the Data Privacy Act of 2012 (Philippine Law) into law Aug. 15, 2012 (*see analysis at WDPR, September 2012, page 4*).[14] The law entered into force Sept. 8, 2012. Organizations have one year from when the implementing rules and regulations become effective (or another period determined by the data protection authority to come into compliance with the law. As of April 2014, implementing regulations had not yet been issued, and the data protection authority had not yet been established.

The Philippine Law applies to the processing of all personal information by individuals and public and private sector organizations, with some important exceptions. The following personal information is exempted from the requirements of the Philippine Law:

- personal information that is collected from residents of foreign jurisdictions in accordance with the laws (*e.g.,* data privacy laws) of those jurisdictions and that is being processed in the Philippines;
- information necessary for banks and other financial institutions under the jurisdiction of the central monetary authority to comply with the anti-money laundering laws and other laws;
- information necessary to carry out functions of public authority;
- information about government contractors that relates to the services performed, including the terms of the contract and the name of the individual; and
- information about any government official that relates to the position or functions of the individual, in-

   ISSN 1473-3579

cluding business contact information, job classification, responsibilities and salary range.

The exemption addressing personal information collected from residents of foreign jurisdictions is unusual but particularly relevant for companies that outsource their processing activities to the Philippines. As a result, outsourcing providers in the Philippines will not need to comply with the Philippine Act's requirements for information collected as part of their outsourcing operations relating to personal information received from outside the Philippines.

The Philippine Law applies to organizations and service providers that are not established in the Philippines but that use equipment located in the Philippines, or those that maintain an office, branch or agency in the Philippines. The Philippine Law also applies to processing outside the Philippines if the processing relates to personal information about a Philippine citizen or resident and the entity has links to the Philippines. This last provision seeking to extend the obligations of the law based on the citizenship of the individuals is very unusual in data protection laws.

Establishment of Data Protection Authority

The Philippine Law establishes the National Privacy Commission (Philippine Commission) as a data protection authority located within the Department of Information and Communications Technology. The Philippine Commission will be responsible for administering, implementing and monitoring compliance with the Philippine Law, as well as investigating and settling complaints. However, unlike many other data protection authorities, it will not have the power to directly impose penalties; it can only recommend prosecution and penalties to the Department of Justice. The Philippine Commission was charged with drafting and issuing the rules and regulations within 90 days of the Philippine Law's effective date.

Appointment of a Data Protection Officer

While database registration is not required for private sector organizations, organizations must designate one or more individuals to be accountable for the organization's compliance with the Philippine Law.

Notice and Consent

Organizations must provide individuals with information about their processing activities, including a description of the personal information collected, the processing purposes, the recipients or categories of recipients with whom the information may be shared, access rights and contact information for the organization. Notice is not required, however, when the collection and processing of personal information are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, or when the information is being collected and processed as a result of a legal obligation.

Consent is required to process personal information or disclose personal information to third parties for all purposes, including marketing, unless another justification or an exception applies. The justifications or "legal bases" listed in the Philippine Law correspond with many of those found in European data protection laws. For example, organizations may process personal information without consent when the processing is necessary to comply with a legal obligation, to pursue the organization's (or a third party's) legitimate interests or to protect vitally important interests of the individual, including life and health. Consent must be freely given, specific and informed. It also must be evidenced in writing, electronic form, or by recorded means.

With respect to sensitive personal information and privileged information, processing is prohibited unless the individual has consented or one of the more narrow exceptions applies (*e.g.*, permitted by law, necessary to protect vital interests, provide medical treatment or protect or defend one's legal rights). Consent to process sensitive personal information must be specific to the purpose and obtained prior to processing.

Data Security and Data Retention

The organization must implement reasonable and appropriate organizational, physical and technical measures to protect personal information. Security measures must include: 1) safeguards to protect computer systems; 2) a written security policy; 3) a risk assessment and mitigation process; 4) regular monitoring for security breaches and a security incident response process; 5) ensuring that service providers implement required security measures; and 6) requiring that employees, agents and representatives maintain the confidentiality of personal information, including after termination. Additional guidelines may also be established by the Philippine Commission.

Organizations must further ensure that third parties processing personal information on their behalf implement the security measures required by the Philippine Law. In particular, the organization is responsible for implementing the Philippine Law's information processing principles and ensuring that proper safeguards are in place in the context of any subcontracting of processing.

Personal information should be retained only for the time necessary for: 1) the purposes for which it was obtained; 2) establishment, exercise or defense of legal claims; 3) legitimate business purposes; or 4) as otherwise provided by law.

Access and Correction Rights

Individuals must be provided with reasonable access to personal information held about them, and have the right to correct or change information. Further, if correction is reasonably requested by the individual, the organization is responsible for correcting information held by third parties to whom the information was previously disclosed.

Data Transfers to Third Parties/Cross-Border Data Transfers

The organization is responsible for personal information under its control or custody, including information that has been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. The organization is accountable for complying with the requirements of the Philippine Law and must use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party. This approach to domestic and international transfers is similar to the approaches found in Canadian and Japanese laws that are based on the concept of accountability.

Breach Notification

Organizations must promptly notify the Philippine Commission and affected individuals when sensitive personal information or other information that might lead to identity fraud has been, or is reasonably believed to have been, acquired by an unauthorized person and the Philippine Commission or the organization believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected individual. Notification must describe the nature of the breach, the sensitive personal information believed to be involved and measures taken to address the breach. The Philippine Commission may exempt an organization from the requirement to provide notice to individuals if it decides that notification is not in the interest of the public or the affected individual.

Penalties

Failure to comply with the requirements of the Philippine Law can result in significant criminal and administrative penalties. Violations could result in imprisonment for six months to six years and fines of between 500,000 Philippine pesos (approximately U.S.$12,000) and 5 million Philippine pesos (approximately U.S.$120,000). Maximum penalties will be imposed for large-scale violations, which are defined as those impacting 100 or more individuals.

If the offender is a corporation, partnership or any legal person, the penalty will be imposed upon the responsible officers who participated in or, by their gross negligence, allowed the commission of the crime. If the offender is a legal person, the court may suspend or revoke any of its rights under the Philippine Law. If the offender is an alien, he or she will, in addition to the penalties prescribed, be deported without further proceedings after serving the penalties prescribed.

SINGAPORE

Overview

Two months after the Philippines enacted its privacy law, Singapore's legislature approved the Personal Data Protection Act 2012 (Singapore Law) Oct. 15, 2012 (*see analysis at WDPR, October 2012, page 4*).[15] The Singapore Law, which came into force in January 2013, governs the collection, use and disclosure of personal information by private sector organizations, and establishes a Personal Data Protection Commission (Singapore Commission) and a Do Not Call Registry.[16] The Singapore Law is being implemented in phases, with the Do Not Call Registry provisions coming into force Jan. 2, 2014, and the data protection rules coming into force July 2, 2014.

The Singapore Law marks Singapore's transition from reliance on a voluntary Model Data Protection Code and limited sectoral laws to an omnibus data protection regime. The transition was largely motivated by Singapore's desire to become a global data hub for data management industries, such as cloud computing and business analytics.

The Singapore Law applies to all private sector organizations incorporated or having a physical presence in Singapore; however, service providers that process on behalf of other organizations are exempted from all but the security and data retention provisions. All personal information of natural persons is protected, with some important exceptions. For example, business contact information—defined as an individual's name, position name or title, business telephone number, address, e-mail or fax number and other similar information—is exempted from the provisions pertaining to the collection, use and disclosure of personal information.

The following summarizes only the data protection provisions of the Singapore Law. It does not address its Do Not Call Registry provisions.

Appointment of a Data Protection Officer

Organizations must designate one or more data protection officer(s) responsible for ensuring the organization's compliance with the Singapore Law.

Notice and Consent

At or before the time of collection, organizations must provide individuals with notice regarding the purposes of collection, use or disclosure of their personal information. In addition, when one organization collects personal information about an individual from another organization without the individual's consent, the collecting organization must provide the disclosing organization notice containing sufficient information regarding the purposes of the collection to allow the disclosing organization to determine whether the disclosure is permissible under the law. This provision is unusual.

The general rule is that consent is necessary to collect, use and disclose personal information unless an exception applies. An individual cannot give valid consent unless he or she has been provided with the requisite notice and consents to the purposes identified in the notice. Moreover, an organization may not impose conditions for consent beyond what is reasonably required to provide a product or service to the individual and must not obtain consent by deceptive or misleading practices. Where the individual voluntarily provides or it is reasonable that the individual would voluntarily provide his or her personal information to an organization

   ISSN 1473-3579

for such purposes, consent is deemed to have been given. No specific form of consent (*e.g.,* verbal, handwritten or electronic) is required. Individuals may withdraw consent at any time with reasonable notice.

Exceptions from the Consent Requirement

An organization may process—collect, use and/or disclose—personal information about an individual without consent in a host of circumstances. For example, consent is not required where:

- personal information is provided to an organization by an individual to enable the organization to provide a service to the individual;
- personal information is included in a document produced in the course of the individual's employment, business or profession and is collected for purposes consistent with the purposes for which the document was produced;
- personal information is collected by the individual's employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the organization and the individual;
- the collection, use or disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual; or
- the collection, use or disclosure is necessary for any purpose that is clearly in the interest of the individual and the individual's consent cannot be obtained in a timely way.

Data Security and Data Retention

There is a general obligation on organizations to be responsible for personal information in their possession or under their control, including making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks. In addition, service providers must comply with the security provision of the Singapore Law.

An organization must cease retaining documents containing personal information or anonymize the information once the purposes for which the information was collected have been achieved and retention is no longer necessary for legal or business purposes.

Access and Correction Rights

Upon request, an organization must, as soon as reasonably possible, provide an individual with his or her personal information that the organization possesses or controls. An individual may request that an organization correct an error or omission in his or her personal information, and the organization is required to do so as soon as practicable unless it is satisfied on reasonable grounds that a correction should not be made. The correcting organization must also send the updated personal information to all other organizations to which it disclosed the inaccurate personal information within a year before the date the correction was made, unless the recipient organization does not need the corrected personal information for any legal or business purpose. This obligation to provide notice to organizations with which the information has been shared is not found in older data protection laws, but is similar to the obligation under the new Malaysian Law.

Cross-Border Data Transfers

An organization can transfer personal data outside Singapore only if it acts in accordance with the requirements under the Singapore Law to ensure that the receiving organization provides protection for the transferred data that is comparable to the protection under the Singapore Law.

However, until implementing regulations are issued, it is unclear exactly what organizations will be required to do to satisfy these requirements. The Singapore Commission's authorization is not required for cross-border transfers; however, in response to a written request, the Singapore Commission may exempt the organization from any prohibitions pertaining to cross-border transfers.

Enforcement/Penalties

The Singapore Law designates a new regulatory body, the Personal Data Protection Commission, with the responsibility for administering and enforcing compliance with the Act. The Singapore Commission has the power to review complaints made against organizations, launch investigations on its own initiative and levy fines on organizations for their failure to comply with the Singapore Law. Criminal sanctions include fines of up to S$10,000 (approximately U.S.$8,000) and/or up to three years of imprisonment. The Singapore Commission has the power to assess financial penalties of up to S$1 million (approximately U.S.$800,000).

In addition, the Singapore Law creates a private right of action for any person who suffers loss or damage as a result of an organization's contravention of the law. In that case, the district court is entitled to grant an injunction, damages or any other relief it deems fit.

Conclusion

With the adoption and/or implementation of three new privacy laws (in Malaysia, the Philippines and Singapore) and amendments to three existing laws (in Australia, Hong Kong and Taiwan), businesses with operations in the Asia region will want to re-examine their privacy policies and practices to ensure they comply with this new environment.

The European approach to privacy—establishing a limited set of conditions or legal bases for processing and imposing cross-border restrictions—is clearly being embraced by more countries in Asia.

However, these countries are developing their own unique interpretations, which can present compliance challenges for companies seeking to establish global privacy approaches. For example, the Philippines requires European-like legal bases for processing but exempts im-

portant sectoral activities from processing and provides for more flexible cross-border rules. Singapore has established a consent-based privacy regime, but the law provides for a complex array of exceptions, which should give businesses considerable flexibility. In contrast, the Malaysian approach, which is perhaps the most closely aligned with the European approach, may impose more stringent requirements (*e.g.,* there is no provision for processing personal information to pursue legitimate business interests). In addition, Malaysia is now the second jurisdiction in the region (Macau was the first) to require registration of data processing activities.

Moreover, the rules of the game in the jurisdictions that have amended their existing privacy regimes are also new, particularly with respect to direct marketing rules in Hong Kong and possibly the processing of sensitive data in Taiwan.

How all of these jurisdictions will implement and enforce these rules remains to be known. As businesses begin to review and modify their practices in these jurisdictions, they will want to pay close attention to actions by the regulatory authorities in the months ahead.

NOTES

[1] The Australia Law is available at http://www.comlaw.gov.au/Details/C2013C00482.

[2] The Privacy Amendment (Enhancing Privacy Protection) Act 2012 is available at http://www.comlaw.gov.au/Details/C2012A00197.

[3] The Information Commissioner's guidelines are available at http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP_guidelines_complete_version_1_March_2014.pdf.

[4] The Hong Kong Law is available at http://bit.ly/1dgcETj.

[5] The India Privacy Rules are available at http://bit.ly/RmRV8T.

[6] Sensitive personal data or information is defined as "information relating to: (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise; provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules."

[7] The Clarification is available at http://deity.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf.

[8] The Japanese Law is available at http://www.caa.go.jp/seikatsu/kojin/foreign/act.pdf.

[9] The Macau Law is available at http://www.gpdp.gov.mo/uploadfile/2013/1217/20131217120421182.pdf.

[10] The New Zealand Law is available at http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

[11] The Korean Law is available at http://bit.ly/1nep6bw.

[12] The Taiwanese Law is available at http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021.

[13] The Malaysian Law is available at http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf.

[14] The Philippine Law is available at http://www.gov.ph/2012/08/15/republic-act-no-10173.

[15] The Singapore Law is available at http://www.parliament.gov.sg/sites/default/files/Personal%20Data%20Protection%20Bill%2024-2012.pdf.

[16] The Singapore Law is split into two parts, covering 1) data protection and 2) the Do Not Call Registry. This Special Report discusses only its data protection regime.

Cynthia Rich is a Senior International Policy Analyst in the Washington office of Morrison & Foerster LLP. As a member of the firm's International Privacy and Data Security Practice since 2001, Rich works with clients on legal issues relating to privacy around the world. She may be contacted at crich@mofo.com.

   ISSN 1473-3579