Bloomberg BNA

Privacy and Security Law Report®

Privacy Laws in Asia

By Cynthia Rich

Introduction/Region at-a-Glance

Privacy legislation in Asia has been extremely active in the past few years, and the level of activity and enforcement does not show any signs of slowing down. Eleven jurisdictions in Asia now have comprehensive privacy laws: Australia, Hong Kong, India, Japan, Macao, Malaysia, New Zealand, the Philippines, Singapore, South Korea and Taiwan. New Zealand is the only jurisdiction in the region that has been recognized by the European Commission as providing adequate protection.

Notably absent from this list are countries such as China, Thailand, Vietnam and Indonesia. China is slowly moving toward a privacy regime, taking a piecemeal, sectoral approach.[1] Thailand, according to recent reports, may be on the verge of enacting privacy legislation. Vietnam appears to be moving slowly in that direction, but Indonesia does not appear to be close to adopting privacy legislation any time soon.

This article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments.

[1] For a detailed discussion of recent privacy law and network security developments in China, see Paul D. McKenzie & Jing Bu, *China Update: Privacy Law and Network Security Developments*, 14 Bloomberg BNA Privacy & Sec. L. Rep. 677 (Apr. 20, 2015), *available at* http://www.mofo.com/~/media/Files/Articles/2015/04/150420BloombergBNAPrivacySecurityLawReport.pdf (14 PVLR 677, 4/20/15).

Cynthia Rich is a senior advisor at 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.

Common Elements Found in Asian Laws

Notice: All of the laws in Asia include some type of notice obligation. That is, every law requires that individuals be told what personal information is collected, why it is collected and with whom it is shared.

Choice: Every privacy law also includes some kind of choice element. The level or type of consent varies significantly from country to country. For example, South Korea has a much stronger emphasis on affirmative opt-in consent than does New Zealand, but all of the laws include choice as a crucial element in the law.

Security: Furthermore, all of the laws require organizations that collect, use and disclose personal information to take reasonable precautions to protect that information from loss, misuse, unauthorized access, disclosure, alteration and destruction. Some of the countries, such as South Korea and Japan, have specified in greater detail how these obligations are to be met.

Access & Correction: One of the core elements of every privacy law is the right of all individuals to access the information that organizations have collected about them and where possible and appropriate, correct, update or suppress that information. Unlike their Latin American counterparts, which require organizations to respond to access and correction requests in very short periods of time, most countries in Asia provide organizations with a more reasonable time frames, similar to those found in European countries.

Data Integrity: Organizations that collect personal information must also ensure that their records are accurate, complete and kept up-to-date for the purposes for which the information will be used.

Data Retention: Generally these laws require organizations to retain the personal information only for the period of time required to achieve the purpose of the processing. Some laws may mandate specific retention periods of time, while others set limits on how long data may be retained by an organization once the purpose of use has been achieved.

 ISSN 1538-3423

Differences in Approaches

While the core data protection principles and requirements are embodied in all of these laws, specific requirements, particularly with respect to cross-border transfers, registration, data security, data breach notification and the appointment of a data protection officer (DPO), vary widely from each other and from laws in other regions of the world.

For example, two-thirds of the countries in this region restrict cross-border transfers of personal information to countries that do not provide adequate protection. Generally a contract, consent or a contract and consent are required to transfer outside the country. In almost all cases, the data protection authorities (DPAs) have not specified what must be contained in these contracts or rules. Most of the DPAs in the region also have not issued lists of countries that they believe provide adequate protection, and thus companies are left to assume that all countries are deemed to be inadequate and must put in place mechanisms (such as consent or contracts) to satisfy the rules. In addition, unlike their European counterparts, registration is not required in all but two of the jurisdictions in the region.

The differences widen when comparing their respective rules on data breach notification, security and DPO obligations: Slightly more than one-third require notification in the event of a data breach, and less than half require the appointment of a DPO.

Lastly, two of the countries, South Korea and Singapore, rely more heavily on consent to legitimize collection, use and disclosure of personal information.

A careful read of these laws is imperative, therefore. These differences pose challenges to organizations, with respect to the adjustments that may be required to global and/or local privacy compliance practices, as well as privacy staffing requirements. Compliance programs that comply with only European Union and Latin American obligations will run afoul of many of the Asian country obligations.

A country-by-country summary of the obligations in these key areas is provided below. Other noteworthy characteristics are also highlighted and, where applicable, the responsible enforcement authority is identified. In addition, a chart is provided at the end to show at a glance the countries with mandatory cross-border, DPO, data security breach notification and registration obligations.

Trends

Enforcement

Violations of these laws can result in significant criminal and civil and/or administrative penalties being imposed; however, the enforcement approaches vary widely from one jurisdiction to another. Japan, New Zealand, Australia and Hong Kong encourage businesses and individuals to resolve disputes voluntarily without resorting to the imposition of fines, except in large data breach cases. In contrast, authorities in South Korea are quick to investigate and impose fines for violations. In Taiwan, the enforcement approach is more varied because enforcement is largely carried out by the competent industry-specific regulators, so the level of enforcement, as well as the interpretations of the compliance obligations under the law, often vary from one regulator to another. In jurisdictions such as Singapore and Malaysia, the regulators are still working with industry to encourage compliance with these new laws.

That said, the growing number of data breaches in the region is clearly forcing regulators to step up their enforcement efforts, particularly against organizations that suffer repeated or massive breaches. For example, after Singtel Optus Pty Ltd., Australia's second-largest telecommunications company, suffered three significant data security breaches, the Australian DPA entered into its first enforceable undertaking that required the company to engage an independent auditor to comprehensively review its data protection practices, develop an implementation plan to rectify any deficiencies found in the audit and obtain the auditor's confirmation that it has implemented the recommended improvements (14 PVLR 621, 4/6/15). After a massive data breach involving three major Korean credit card companies in January 2014, South Korea's Financial Supervisory Service (FSS) issued a three-month business suspension order against the credit card companies, and several employees of the companies are under investigation by the FSS (13 PVLR 98, 1/13/14). The Financial Services Commission also ordered the companies to cover any financial losses suffered by their customers. As a result of the breaches, the Ministry of Government Administration and Home Affairs (MOGAHA), the authority responsible for enforcing the privacy law, announced plans to expand its on-site investigations to include both data handlers and their third-party service providers. It also announced its intention to amend applicable laws and regulations to impose stricter obligations and liabilities on the service providers.

Data breaches have also resulted in increased civil litigation, particularly in Japan and South Korea. For example, in January 2015, a large multi-plaintiff litigation (involving 1,789 plaintiffs) was filed in court in connection with a data breach that affected 48.6 million customers of Benesse Holdings Inc., a Tokyo-based company that operates Shinkenzemi correspondence education courses for schoolchildren (14 PVLR 208, 2/2/15). In addition, hundreds of civil actions are now pending for claims arising from the January 2014 credit card breach in South Korea.

Privacy Legislation Under Development

New privacy laws are being debated in Japan and Thailand. Discussions are currently underway in the Japanese Diet on the government's proposed new privacy framework, which was announced in June 2014. The proposed reforms, if enacted, would, among other things, expand the definition of ''personal data'' to include biometric information such as fingerprint data and face recognition data; establish separate protections for ''sensitive'' information; and establish an independent enforcement authority that would have stronger powers than each industry ministry currently has.

The Thai government is also working on new privacy legislation. In January 2015, the Cabinet announced that it had approved ''in principle'' a draft privacy bill that would impose basic data privacy obligations on organizations such as notice, consent, access, data retention and security (14 PVLR 123, 1/19/15). Transfers to countries that do not provide adequate protection would be restricted. The Minister of Digital Economy and Society is the designated agency responsible for enforcement of the law. At present, there are no obligations in the bill that would require registration, the appointment of a DPO or data breach notification.

   ISSN 1538-3423

Lastly, South Korean data privacy rules are undergoing important changes, largely in response to massive data security breaches that have occurred in the past year. In May 2014, the National Assembly amended its Internet service provider law to strengthen, among other changes, the data breach notification provisions. In July 2014, a pan-government task force announced a Comprehensive Solution Package to strengthen data privacy protection that will lead to a series of legislative changes to South Korea's umbrella privacy law and various sectoral laws that contain privacy provisions. In December 2014, the Ministry of Government Administration and Home Affairs amended its data security standards.

Country-by-Country Review of Differences

AUSTRALIA

Australia's Privacy Act 1988 (Cth) (''Australian Law'') has been amended twice since it was enacted, first in 2000 and most recently in 2012 (11 PVLR 1709, 12/3/12).[2] As part of the most recent changes to the law, a single set of privacy principles, referred to as the Australian Privacy Principles (APPs), covering both the public and private sectors was adopted. In addition, a comprehensive credit reporting system that provides for codes of practice under the APPs and a credit reporting code were implemented. The privacy commissioner was also given the authority to develop and register codes that are binding on specified agencies and organizations. The 2012 amendments also clarify the functions and powers of the commissioner and improve the 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 time table for their development and enactment.

In Brief. *Like most of the jurisdictions in the region, the Australian Law does not require the appointment of a DPO, registration and data security breach notification; however, the privacy commissioner recommends that organizations appoint a DPO and provide notice in the event of a data security breach. Under the amended law, there are more detailed rules on cross-border transfers, and the application of the law has been expanded to cover all organizations with ''Australian links.'' Lastly, the exemption for employee records remains intact.*

Special Characteristics

Data Protection Authority. The Australian Law is administered by the privacy commissioner in the Office of the Australian Information Commissioner (DPA).[3] The DPA has the power to conduct privacy compliance assessments of Australian government agencies and some private sector organizations, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of privacy. In May 2014, the Australian government announced plans to disband the Office of the Australian Information Commissioner (OAIC) for budgetary reasons by Jan. 1, 2015, but the position and responsibilities of the privacy commissioner would remain intact. However, the necessary legislation was not enacted by the end of 2014, so, for the moment, the OAIC remains operational.

Application of the Act. One of the significant changes to the Australian 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 not 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 DPA's guidelines,[4] 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.

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

Employee Records. The existing exemption for employee records covering ''acts or practices in relation to employee records of an individual if the act or practice directly relates to a current or former employment rela-

[2] The Privacy Act is available at http://www.comlaw.gov.au/Details/C2013C00482. The Privacy Amendment (Enhancing Privacy Protection) Act 2012 is available at http://www.comlaw.gov.au/Details/C2012A00197.

[3] The website address for the Australian DPA is http://www.privacy.gov.au.

[4] The APP guidelines are available at http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf.

tionship between the employer and the individual'' remains intact; the intention is to revisit this issue in subsequent rounds.

Cross-Border Transfers. Before disclosing personal information to a recipient overseas, organizations must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information received, except where one of the following situations applies:

- the recipient is subject to a law or binding scheme that protects the information in a substantially similar manner, and there are mechanisms available to the individual to enforce that protection;
- the individual is expressly informed that, if he or she consents to the disclosure of the information, the organization is relieved of its obligation to take the required reasonable steps above to ensure that the overseas recipient does not breach the APPs, and, after being so informed, the individual consents to the disclosure;
- the disclosure of the information is required or authorized by or under an Australian law or a court/tribunal order; or
- there is an exception under the law that covers the disclosure of the information by the organization.

The cross-border rules apply to transfers by the organization to its overseas affiliates but not an overseas office.

Data Protection Officer. There is no obligation to appoint a DPO; however, there is a general obligation to implement appropriate practices, procedures and systems to comply with the APPs. The APP guidelines cite the example of designated privacy officers as a possible governance mechanism to ensure compliance with the APPs.

Data Security Breach Notification. There is no obligation under the Australian Law and the APPs to provide notice in the event of a data security breach; however, the DPA has issued voluntary breach notification guidance which recommends that notice be provided to the DPA and affected individuals where the breach creates a real risk of serious harm to individuals.[5] Mandatory breach notification rules for the telecommunications companies and Internet service providers are currently under consideration by the legislature.

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.[6] The Hong Kong Law was amended in 2012, and one of the most significant changes was to more closely regulate the use and provision of personal information in direct marketing activities (11 PVLR 1117, 7/9/12). In addition, certain changes to the data protection principles were made, new offenses and penalties were introduced, the authority of the Office of the Privacy Commissioner for Personal Data (DPA) was enhanced and a new scheme whereby the DPA may provide legal assistance to individuals was introduced. The majority of the changes went into effect Oct. 1, 2012; the new direct marketing and the legal assistance provisions took effect April 1, 2013.

In Brief. *The Hong Kong Law does not require the appointment of a DPO, data security breach notification or registration; however, the DPA does recommend that organizations appoint a DPO and provide notice in the event of a data security breach. The Hong Kong Law contains a provision that restricts cross-border transfers to countries that do not provide adequate protection; however, the provision is not in force.*

Special Characteristics

Data Protection Authority. The Office of the Privacy Commissioner for Personal Data is responsible for enforcement.[7]

Cross-Border Transfers. While the Hong Kong Law contains a provision (Section 33) that limits the transfer of personal information to a place outside Hong Kong that does 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.

In December 2014, the DPA issued voluntary guidance to help organizations understand their compliance obligations under Section 33.[8] The guidance contains a set of recommended model data transfer clauses for such transfers. The DPA has called upon the government to implement Section 33 and has also developed and submitted to the administration a white list of 50 jurisdictions that, in his view, provide similar protection. If and when Section 33 is implemented, the transfers to jurisdictions on the white list would be exempted from the requirements under Section 33.

Data Protection Officer. There is no statutory requirement to appoint a DPO. However, the DPA recommends it. Appointment of a DPO is a common business practice in Hong Kong.

Data Security Breach Notification. There is no legal obligation on any entities to give notice in the event of a data security breach under the Hong Kong Law; however, the DPA issued voluntary guidance which recommends that organizations ''seriously consider'' notifying individuals affected by a breach where there is a real risk of harm.[9] Organizations may also choose to notify the privacy commissioner.

---

[5] The voluntary breach guidelines are available at http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/data-breach-notification-guide-august-2014.pdf.

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

[7] The website of the Hong Kong DPA is http://www.pcpd.org.hk.

[8] The Section 33 guidance is available at http://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf.

[9] The data breach guidance is available at http://www.pcpd.org.hk/english/publications/files/DataBreachHandling_e.pdf.

  PVLR ISSN 1538-3423

Marketing. One of the most significant changes was to more closely regulate the use and provision of personal information in direct marketing activities. Under the new direct marketing rules, an organization can only use or transfer personal information for direct marketing purposes if that organization has provided the required information (notice) and consent mechanism to the individual concerned and has obtained his or her consent.[10] ''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 ($64,503) and three years' imprisonment. In cases involving transfer of personal data for gain, a fine of HK$1 million ($129,006) and five years' imprisonment are possible.

INDIA

In 2011, India issued final regulations implementing parts of the Information Technology (Amendment) Act, 2008 dealing with protection of personal information (10 PVLR 687, 5/9/11). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (''Indian 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 of India.[11]

In Brief. *The Indian Privacy Rules do not require the appointment of a DPO, data security breach notification or registration. There are limitations on cross-border transfers, but they apply only to sensitive personal information. Furthermore, as explained below, outsourcing providers are subject to a narrower set of obligations, the consent obligations only apply to sensitive information and sensitive information is very broadly defined.*

Special Characteristics

Data Protection Authority. The Ministry of Communications & Information Technology is responsible for enforcement of the Indian Privacy Rules.[12]

Application of the Rules. The Indian Privacy Rules raised significant issues and caused concern among organizations that outsource business functions to Indian service providers. As drafted, the Indian 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 Indian Privacy Rules would decimate the outsourcing industry.

In response to these concerns, on Aug. 24, 2011, the Indian Ministry of Communication & Technology issued a clarification of the Indian Privacy Rules (''Clarification''), stating that the Indian Privacy Rules apply only to organizations in India (10 PVLR 1240, 9/5/11).[13] 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 Indian 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.

Consent. The consent rules apply only to sensitive information.

Sensitive Information. Sensitive information is very broadly defined and includes information that is not generally regarded as sensitive in other jurisdictions. In particular, it 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.

Cross-Border Transfers. An organization may transfer sensitive personal information to any organization or person in India or to another country that ensures the same level of data protection; however, the government has not issued a list of countries that, in its view, provide such protection. The transfer may only be allowed if it is necessary for the performance of the contract between the organization (or its agent) and the individual or where the individual has consented to the transfer.

JAPAN

Japan's Protection of Personal Information Law (PPIL or ''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 the information on 5,000 or more individuals on any day in the past six

[10] The rules are contained in the amended act. A guidance note on the direct marketing rules is available at http://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf.

[11] The Indian Privacy Rules are available, in English, at http://bit.ly/RmRV8T.

[12] The website of the Indian Ministry is http://www.mit.gov.in.

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

months (4 PVLR 456, 4/11/05).[14] Like other Japanese basic laws, the PPIL is framework legislation that delegates discretion to national administrative agencies and local governments to develop and implement regulations to accomplish the purposes of the law. To date, 39 guidelines on the protection of personal information have been issued for 27 areas by 12 governmental agencies.

In Brief. *The Japanese Law does not impose restrictions on cross-border transfers or require registration. There are requirements to appoint a DPO and provide notice in the event of a data security breach under some of the ministry guidelines. There are special notice rules for sharing with third parties.*

Special Characteristics

Data Protection Authority. The ministries responsible for enforcement in their individual sectors include: the Ministry of Economy, Trade and Industry (METI); the Ministry of Internal Affairs and Communications (MIC) (formerly the Ministry of Public Management, Home Affairs, Posts and Telecommunication); the Ministry of Finance (FSA); the Ministry of Health, Labour and Welfare (MHLW); and the Ministry of Land, Infrastructure, Transport and Tourism (MLIT).[15] Their 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.

Cross-Border Transfers. There are no limitations on cross-border transfers. The rules for disclosures to third parties would apply, however. In particular, personal information must not be provided to third parties without prior consent of the individual unless an opt-out notice of third-party sharing has been provided prior to the personal information being collected.

Data Protection Officer. There is no requirement for a DPO under the Japanese Law; however, under some of the ministry guidelines, a DPO is required or recommended. In particular, a DPO is required in the financial and credit sectors and recommended in other sectors.

Data Security. Under the Japanese Law, there is a general requirement for organizations to adopt measures necessary and appropriate for preventing the divulgence, loss or damage of personal information and otherwise control the security of that information. In addition, some of the guidelines impose more extensive security requirements, including encryption and service provider supervision.

Data Security Breach Notification. Data security breach notification is not explicitly addressed in the Japanese Law but is addressed in the ministry guidelines. Citing the Japanese Law's security control measures as the basis for their notification obligations, some of the ministry guidelines require or expect notification whenever there is a loss of personal information.

Joint Use Notice. If an organization intends to jointly use personal information with third parties (including corporate affiliates), it must provide information on the scope of joint users, items of personal information to be jointly used, purpose of joint use and the name of the individual or entity primarily responsible for the management of the data. The information must be provided through a notice to the individual or by placing the individual in circumstances whereby he or she can easily find out. Any change in purposes of joint use and/or the name of the individual or entity primarily responsible for the management of the data must also be notified to the individuals or publicly announced.

MACAO

The Personal Data Protection Act (''Macao Law''), which took effect in 2006, was the first jurisdiction in Asia to adopt an EU-style data protection law.[16] 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 member state laws. The Macao Law applies to both the public and private sector processing of personal information of natural persons. Macao was the first jurisdiction in the region to require registration and impose EU-style cross-border restrictions.

In Brief. *The Macao Law imposes restrictions on cross-border transfers that mirror EU member state cross-border border restrictions and requires registration of databases. It does not require the appointment of a DPO or data security breach notification.*

Special Characteristics

Data Protection Authority. The Office for Personal Data Protection (DPA) is responsible for enforcement.[17]

Registration. Registration is required unless an exemption applies.

MALAYSIA

The Personal Data Protection Act (''Malaysian Law'') was enacted in 2010 but did not come into effect until November 2013 (12 PVLR 2002, 11/25/13); organizations were given three months (until Feb. 15, 2014) to

[14] The PPIL is available, in English, at http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

[15] A complete list of the guidelines and responsible ministries is available at http://www.caa.go.jp/planning/kojin/gaidorainkentou.html.

[16] The Macao Law is available, in Chinese and Portuguese, at http://images.io.gov.mo/bo/i/2005/34/lei-8-2005.pdf.

[17] The website of the Macao DPA is at http://www.gpdp.gov.mo.

  PVLR ISSN 1538-3423

comply.[18] The Malaysian Law protects all personal information of natural persons processed in respect to ''commercial transactions'' (explained below) that are (i) processed in Malaysia and (ii) processed outside Malaysia where the data are intended to be further processed in Malaysia. The Malaysian Law does not apply, however, to personal information processed by federal and state governments.

In Brief. *The Malaysian Law restricts cross-border transfers and requires registration. It does not require the appointment of a DPO or data security breach notification.*

Special Characteristics

Data Protection Authority. The Department of Personal Data Protection (DPA), located within the Ministry of Communication and Multimedia, is responsible for regulating and overseeing compliance with the Malaysian Law.[19]

Application of the Law. 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.

Cross-Border Transfers. Organizations may only transfer personal information to countries outside Malaysia that have been approved by the minister of communication and multimedia 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 act.

As of May 2015, no countries have been approved. Approved countries will be published by the minister in the official Gazette.

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 and retail or wholesale dealing as defined under the Control Supplies Act 1961), private employment agencies, real estate and utilities.

NEW ZEALAND

New Zealand was the first country in the region to enact a data protection law. 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 (11 PVLR 1855, 12/24/12).[20] 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 of 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 (9 PVLR 1287, 9/13/10).

In Brief. *The New Zealand Law requires the appointment of a DPO but does not restrict cross-border transfers or require registration. There are no mandatory requirements to provide notice in the event of a data security breach; however, such notice is recommended by the DPA.*

Special Characteristics

Data Protection Authority. The Office of the Privacy Commissioner (DPA) regulates and administers the New Zealand Law.[21]

Data Protection Officer. A DPO must be appointed regardless of the size of the agency. One DPO per agency is required.

Data Security Breach Notification. There are no mandatory notification obligations; however, the DPA has issued voluntary guidelines that recommend notice be provided to individuals and/or the DPA in the event of a security breach that presents a risk of harm to the individuals whose personal information is involved in the breach. Necessity to provide notice should be assessed on a case-by-case basis.

THE PHILIPPINES

Philippine President Benigno Aquino III signed the Data Privacy Act of 2012 (''Philippine Law'') into law Aug. 15, 2012 (11 PVLR 1357, 9/3/12).[22] The law entered

[18] The Malaysian Law is available, in Malay, at http://www.pdp.gov.my/images/AKTA_PERLINDUNGAN_DATA_PERIBADI.pdf.

[19] The website of the Malaysian DPA is at http://www.pdp.gov.my/index.php/en.

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

[21] The website of the New Zealand DPA is at http://www.privacy.org.nz.

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

into force Sept. 8, 2012. Organizations have one year from when the implementing rules and regulations become effective (or another period determined by the DPA) to come into compliance with the law. As of May 2015, implementing regulations had not been issued, and the DPA had not been established.

In Brief. *The Philippine Law imposes the same rules for both domestic and international (cross-border) transfers and requires the appointment of a DPO and data security breach notification. It does not require registration. In addition, the Philippine Law contains an exemption for outsourcing providers.*

Special Characteristics

Data Protection Authority. The Philippine Law establishes the National Privacy Commission (the ''Commission'') as a DPA located within the Department of Information and Communications Technology (DICT). The Commission, which had not been established as of May 2015, will be responsible for administering, implementing and monitoring compliance with the Philippine Act, 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.

Application of the Law. The Philippine Law applies to the processing of all personal information of individuals by public and private sector organizations with some important exceptions. For example, 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 is excluded. This exception is 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 Law's requirements for information collected as part of their outsourcing operations relating to personal information received from outside the Philippines.

In addition, the Philippine Law also applies to organizations and service providers that are not established in the Philippines but that use equipment located in the Philippines or maintain an office, branch or agency in the Philippines. It also applies to processing outside the Philippines if the processing relates to personal information about a Philippine citizen or a 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.

Cross-Border Transfers/Transfers to Third Parties. Organizations are responsible for personal information under their 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. Organizations are 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.

Data Protection Officer. While 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.

Data Security Breach Notification. Organizations must promptly notify the 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 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 Commission may exempt an organization from the requirement to provide notice to individuals if he or she decides that notification is not in the interest of the public or the affected individual.

SINGAPORE

Singapore's Personal Data Protection Act 2012 (''Singapore Law'') came into force in January 2013 (11 PVLR 1562, 10/22/12).[23] The Singapore Law governs the collection, use and disclosure of personal information by private sector organizations. It also prohibits the sending of certain marketing messages to Singapore telephone numbers, including mobile, fixed-line, residential and business numbers registered with the Do Not Call (DNC) Registry. The Singapore Law was implemented in phases, with the DNC Registry provisions coming into force in January 2014 and the data protection rules coming into force in July 2014 (13 PVLR 980, 6/2/14).

The following summarizes the special characteristics of data protection provisions only. It does not address the DNC Registry provisions contained in the Singapore Law.

In Brief. *The Singapore Law restricts cross-border transfers and requires the appointment of a DPO. Data security breach notification and registration are not required. The Singapore Law provides special exemptions for outsourcing providers and the collection, use and disclosure of business contact information.*

Special Characteristics

Data Protection Authority. The Personal Data Protection Commission is responsible for enforcement of the Singapore Law.[24]

Application of the Law. 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

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

[24] The website address of the Singapore DPA is http://www.pdpc.gov.sg.

  PVLR ISSN 1538-3423

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.

Cross-Border Transfers. Transferring organizations are required to take appropriate steps to determine whether, and ensure that, the recipient outside Singapore is bound by legally enforceable obligations to provide the transferred information with a comparable standard of protection. To satisfy these requirements, consent, a transfer contract, binding corporate rules or another exception under the Singapore Law must apply.

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

SOUTH KOREA

The Data Protection Act (PIPA or ''Korean Law''), which took effect in September 2011 (10 PVLR 522, 4/4/11), regulates public and private sector processing of personal information of natural persons.[25] PIPA serves as the umbrella privacy law in South Korea; however, there are various sector-specific laws, such as the Act on the Promotion of IT Network Use and Information Protection (''the Network Act''), the Use and Protection of Credit Information Act, the Electronic Financial Transactions Act and the Use and Protection of Location Information Act, that also regulate privacy and cybersecurity. The Network Act, enacted before PIPA, regulates the processing of personal information in the context of services provided by telecommunications service providers and commercial website operators.[26] While the privacy-related provisions are similar to PIPA, the Network Act regulates issues not covered by PIPA, such as spam.

In Brief. *The Korean Law restricts cross-border transfers and requires the appointment of a DPO and data security breach notification. It also imposes extensive obligations in such areas as notice, consent and data security. Registration is not required, however.*

Special Characteristics

Data Protection Authority. The Ministry of Government Administration and Home Affairs (MOGAHA) is the authority responsible for enforcing the Korean Law.[27]

Notice and Consent. 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.

Cross-Border Transfers. If an organization intends to provide personal information to a third party across the national border, it must give notice and obtain specific consent to authorize the cross-border transfer.

Data Protection Officer. Organizations must appoint a DPO with specified responsibilities.

Data Security. The Korean Law and subsequent guidance[28] issued by the regulatory authorities also impose significant data security obligations. These data security requirements are some of the most detailed in the world. 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.

Data Security Breach Notification. When becoming aware of a leak of personal information, organizations must, without delay, notify the relevant individuals, prepare measures to minimize possible damages and, when the volume of affected data 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 concerned or certain designated specialist institutions.

TAIWAN

Taiwan's Personal Data Protection Act (''Taiwanese Law'') entered into effect in October 2012 (11 PVLR 1322, 9/3/12).[29] The Taiwanese Law replaces 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 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.

[25] The Korean Act is available, in Korean, at http://bit.ly/1nep6bw.

[26] The Network Act is available, in Korean, at http://bit.ly/1JMZY3I.

[27] The website for MOGAHA is at http://www.mogaha.go.kr.

[28] The guidance is available, in Korean, at http://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000009963.

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

In Brief. *The Taiwanese Law requires data security breach notification but does not restrict cross-border transfers or require the appointment of a DPO or registration of databases.*

Special Characteristics

Data Protection Authority. The Ministry of Justice has overall responsibility for the Taiwanese Law; however, the individual government agencies that regulate specific industry sectors are authorized to regulate compliance by organizations under their regulatory jurisdiction.[30]

[30] The website for the Ministry of Justice is at http://www.moj.gov.tw.

Cross-Border Transfers. There are no restrictions imposed on cross-border transfers; however, the central competent authority for a specific industry may restrict cross-border transfers in certain circumstances, such as if the recipient country does not yet have proper laws and regulations to protect personal information so that the rights and interests of the individual may be damaged or personal information is indirectly transferred to a third country to evade the Taiwanese Law.

Data Security Breach Notification. Individuals must be notified when their personal information has been stolen, divulged or altered without authorization or infringed upon in any way.

COUNTRIES WITH PRIVACY LAWS	REGISTRATION REQUIREMENT	DPO REQUIRED[1]	CROSS-BORDER LIMITATIONS	DATA BREACH NOTIFICATION REQUIREMENT[2]
ASIA-PACIFIC (11)	**2**	**5**	**7**	**4**
Australia	No	No	**Yes**	No
Hong Kong	No	No	No	No
India	No	No	**Yes**	No
Japan	No	**Yes**	No	**Yes**
Macao	**Yes**	No	**Yes**	No
Malaysia	**Yes**	No	**Yes**	No
New Zealand	No	**Yes**	No	No
Philippines	No	**Yes**	No	**Yes**
Singapore	No	**Yes**	**Yes**	No
South Korea	No	**Yes**	**Yes**	**Yes**
Taiwan	No	No	**Yes**	**Yes**

[1] In some jurisdictions, the appointment of a DPO may exempt the organization from its registration obligations.

[2] This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.

  PVLR ISSN 1538-3423