Bloomberg BNA

Privacy and Security Law Report®

The Changing Privacy Landscape in Asia



BY CYNTHIA J. RICH, MARIAN A. WALDMANN AGARWAL AND MATTHEW R. GALEOTTI

In the past several months, the privacy landscape in Asia has dramatically altered. Two countries, the Philippines and Singapore, enacted comprehensive data privacy laws for the first time; Malaysia is on the verge of finally implementing its first comprehensive data privacy law more than two years after its adoption; and Australia, Hong Kong and Taiwan have amended their existing privacy laws. These developments will profoundly affect organizations that do business in Asia, have employees in Asia, or who outsource services to Asia.

The following provides an overview of the changes that have or will be occurring in these jurisdictions and assesses the implications for businesses operating in Asia.

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. Marian Waldmann Agarwal and Matthew Galeotti are associates in Morrison & Foerster's New York office, and members of the firm's Global Privacy and Data Security Group. The Global Employee Privacy and Data Security Law, Second Edition, written by Morrison & Foerster, edited by partners Miriam H. Wugmeister and Christine E. Lyon and published by BNA, is now available for download on the iPhone, iPad, and iPod touch.

NEW COMPREHENSIVE PRIVACY LAWS

MALAYSIA

Overview

More than two years after Malaysia's Parliament approved a comprehensive data privacy law, the Personal Data Protection Act,[1] the law is moving toward its entry into force. First introduced by the government in 2009, the act was approved by the Parliament in May 2010 and then received Royal Assent and was published in the Official Gazette in June 2010. However, the act did not become effective immediately. The government was authorized to decide the date for its implementation. On Dec. 12, 2012, the Deputy Information, Communications and Culture Minister publicly announced that the act will come into force on Jan. 1, 2013. Once the act comes into force, organizations will have three months to comply.

The act protects all personal information of natural persons processed in the context of ''commercial transactions'' that are (i) processed in Malaysia, and (ii) processed outside Malaysia where the information is 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

[1] The Personal Data Protection Act is available, in English, at http://www.kpkk.gov.my/akta_kpkk/Personal%20Data%20Protection.pdf.

 ISSN 1538-3423

about whether this law would apply to the processing of human resources data; however, there are indications that the new law will be interpreted by the new data protection authority as applying to human resources data.

The act applies to any person who is either established in Malaysia or uses equipment in Malaysia for processing purposes, and who processes, has control over, or authorizes the processing of personal information in the context of commercial transactions. This is quite similar to the reach of most European laws. The act 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, at the time of, or before 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 act. The legal bases listed in the act 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 act 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 such a 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 Transfer

Organizations may only transfer personal information to countries outside Malaysia that have been approved by the Minister of Information, Communication and Culture 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.

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

Establishment of Data Protection Authority

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

Database Registration

The Minister has the authority to specify a category of organizations that will be required to register with the commissioner. Such organizations will be required to register all processing of personal information with the commissioner and obtain a certificate of registration for such processing. The commissioner will maintain a register of certified designated Data Users.

The Personal Data Protection Department recently conducted a public consultation on database registration under the act. The consultation focused on the categories of organizations that will be required to register with the commissioner in accordance with the act. In the context of the consultation, the Personal Data Protection Department proposed the following categories of organizations (by sector): communications; banking and financial institutions; insurance; health, tourism and hospitality; transportation; education; direct sales and direct marketing; services; property; utility; and sports and recreation. Stakeholders were asked for

  PVLR ISSN 1538-3423

comments on these categories and about the registration process under the act.

Penalties

Failure to comply with the requirements of the act can result in criminal and administrative penalties. Criminal sanctions include fines up to 500,000 MYR (approx. $164,000) and/or two years imprisonment. Organizations are liable for offenses under the act; 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 commissioner may serve an enforcement notice directing the organization to take steps to remedy any contraventions of the act within a specified time period and may order processing of personal information to cease pending such remedy. There is no right to private action under the act.

THE PHILIPPINES

Overview

Philippine President Aquino signed the Data Privacy Act of 2012 (the ''Philippine Act'') into law Aug. 15, 2012.[2] The law entered into force Sept. 8, 2012, and rules and regulations are expected to be published within 90 days of that date. Organizations will then 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 act.

The Philippine Act 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 Act:

- 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, including 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, outsource 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 Act applies to organizations and service providers that are not established in the Philippines but that use equipment located in the Philippines, or those who maintain an office, branch, or agency in the Philippines. The Philippine Act 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.

Establishment of Data Protection Authority

The Philippine Act establishes the National Privacy Commission (the ''commission'') as a data protection authority (DPA) located within the Department of Information and Communications Technology (''DICT''). The commission 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. The commission is charged with drafting and issuing the rules and regulations within 90 days of the Philippine Act'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 Act.

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 Act 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,

[2] The Data Privacy Act of 2012 is available, in English, at http://www.gov.ph/2012/08/15/republic-act-no-10173.

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 commissioner.

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

Personal information only should be retained 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 Transfer

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 Act 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 which are based on the concept of accountability.

Breach Notification

Organizations must promptly notify the commissioner 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 commissioner 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 commissioner 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.

Penalties

Failure to comply with the requirements of the Philippine Act can result in significant criminal and administrative penalties. Violations could result in imprisonment for six months to six years and fines of between PHP 500,000 (approx. $12,000) and PHP 5 million (approx. $120,000). Maximum penalties will be imposed for large scale violations, which are defined as those impacting one hundred (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 Act. 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 (''act'' or ''PDPA'') on Oct. 15, 2012.[3] The act, which is expected to come into force sometime in January 2013, governs the collection, use, and disclosure of personal information by private sector organizations, establishes a Personal Data Protection Commission (''Commission'' or ''DPA''), and a Do Not Call Registry.[4] The act will be implemented in phases, with the Do Not Call registry provisions coming into force after a transition period of 12 months, and the data protection rules coming into force after 18 months.

The act 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 act 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 secu-

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

[4] The PDPA is split into two parts, covering 1) data protection; and 2) the Do Not Call Registry. This client alert focuses on the data protection regime.

  PVLR ISSN 1538-3423

rity and data retention provisions. All personal information of natural persons are protected with some important exceptions. For example, business contact information – defined as an individual's name, position name or title, business telephone number, address, email 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 the data protection provisions only. It does not address the Do Not Call provisions contained in the act.

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 act.

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 act. 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 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 act.

An organization must cease to retain 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 whom 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 Transfer

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

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

Enforcement/Penalties

The act designates a new regulatory body, the Personal Data Protection Commission, with the responsibility for administering and enforcing compliance with the act. The 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 act. Criminal sanctions include fines up to Singapore $10,000 (ap-

prox. $8,000) and/or up to 3 years imprisonment. The Commission has the power to assess financial penalties up to Singapore $1 million (approx. $800,000). In addition, the act creates a private right of action for any person who suffers loss or damage as result of an organization's contravention of the act. In that case, the district court is entitled to grant an injunction, damages, or any other relief it deems fit.

AMENDMENTS TO EXISTING LAWS

Australia

The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (the ''Privacy Bill'')[5] passed the Parliament Nov. 29, 2012 and is awaiting Royal Assent. The Privacy Bill amends the Privacy Act 1988 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). It also implements a comprehensive credit reporting system which provides for codes of practice under the APPs and a credit reporting code and gives the commissioner authority to develop and register codes that are binding on specified agencies and organizations. The Privacy Bill clarifies the functions and powers of the commissioner and improves 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.

Several last minute changes were made to the Privacy Bill, including an extension of the Privacy Bill's transition period to 15 months after it receives Royal Assent. In addition, financial institutions had raised concerns about a proposed ''Australian link'' requirement that could have prevented any offshore disclosure of credit-related material. The Privacy Bill as passed modifies this requirement. The supplementary explanatory memorandum states that it is not the government's policy to prevent cross-border disclosures of credit eligibility information that are currently permitted by the Privacy Act. However, Australian credit providers will now have ongoing responsibility for the acts and practices of any overseas entity to whom they disclose credit eligibility information.

Hong Kong

The Personal Data (Privacy) (Amendment) Ordinance 2012 (''Amendment Ordinance'') was formally adopted in July 2012.[6] One of the most significant changes the Amendment Ordinance makes to the existing Personal Data (Privacy) Ordinance (''PDPO'') is to regulate more closely the use and provision of personal information in direct marketing activities. The Amendment Ordinance also made certain amendments to the data protection principles, introduced new offenses and penalties, enhanced the authority of the Privacy Commissioner for Personal Data (''commissioner''), and introduced a new scheme whereby the commissioner may provide legal assistance to data subjects. The majority of the Amendment Ordinance came into effect Oct. 1, 2012. However, the new direct marketing and the legal assistance provisions are not yet in force, and are expected to come into effect in the first half of 2013.

Taiwan

Taiwan's Personal Data Protection Act (''PDPA'') and Enforcement Rules entered into effect Oct. 1, 2012.[7] The PDPA replaces the 1995 Computer Processed Personal Data Protection Act (the ''CPPDPA'') that regulated computerized personal information in specific sectors such as financial, telecommunication, and insurance. The PDPA now provides protection to personal information 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 (Articles 6 and 54). Article 6 governs the collection, processing, and use of sensitive personal information such as medical history, genetic records, sex life, health check results, and criminal records; Article 54 requires data collectors to notify individuals within one year of the effective date of the Personal Data Protection Act if the personal information the collectors would like to use was not obtained directly from the individual before the effective date.

IMPLICATIONS FOR BUSINESS

With the adoption and/or implementation of three new privacy laws in Asia and amendments to three existing laws, businesses with operations in the 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, requiring the registration of data processing activities, and/or 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 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). Further, while the European countries and other countries' more recent laws

[5] The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 is available at http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4813.

[6] The Personal Data (Privacy) (Amendment) Ordinance 2012 is available, in English, at http://op.bna.com/pl.nsf/r?Open=byul-92x236.

[7] The Personal Data Protection Act (''PDPA'') is available, in English, at http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021.

  PVLR ISSN 1538-3423

have moved away from a registration requirement, several of the Asian countries will now require registration.

In the jurisdictions that have amended their well-established privacy regimes, the rules of the game will change as well, particularly with respect to direct marketing rules in Hong Kong and possibly the processing of sensitive data in Taiwan. How all of these countries 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. As always, the devil will be in the details.