Bloomberg Law

Privacy and Security Law Report®

Data Protection

A Look at New Trends: Privacy Laws in East, Central, and South Asia and the Pacific

Data Protection

In this second article of a four-part series on the status of international data protection laws, the author explores developments in East, Central, and South Asia, and the Pacific, where 14 jurisdictions now have comprehensive data protection laws.

By Cynthia Rich

Introduction/Region at-a-Glance

Privacy legislation in East, Central, and South Asia and the Pacific (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. Fourteen jurisdictions in Asia now have comprehensive privacy laws: Australia, Hong Kong, India, Japan, Kazakhstan, Kyrgyzstan, Macao, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Taiwan, and Turkmenistan. New Zealand is the only jurisdiction in the region that has been recognized by the European Commission as providing adequate protection.

Cynthia Rich is a senior adviser 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.

Notably absent from this list are countries such as China, Indonesia, Thailand, and Vietnam. China has not yet enacted a comprehensive privacy law but late last year the country enacted a comprehensive Cyber Security Law (CSL) that went into effect June 1, 2017. In addition to regulating network security, the CSL includes broad provisions governing the protection of network data, including personal information and a data localization requirement that requires that operators of ''key information infrastructure'' (KII) to store in China both personal data and ''significant data'' collected and produced in the course of business operations in China.

Similarly, Indonesia does not have a comprehensive data privacy law but the country enacted regulations in December 2016 in connection with its Electronic Information and Transaction Law that established protections for personal data transmitted through electronic media. The government of Thailand has drafted legislation but it has not been approved yet by the legislature. Vietnam also appears to be moving slowly toward the development of privacy legislation.

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

 ISSN 1538-3423

Developments and Trends

Amendments to Existing Privacy Laws

Over the past year, Australia, Japan, and the Philippines either enacted or implemented changes to their data privacy laws. Japan's amendments to its Personal Information Protection Act were the most recent to enter into full effect, on May 30, 2017. Enacted in September 2015, these amendments made significant changes to the ways in which companies handle personal information, particularly with respect to disclosures to third parties, international transfers, anonymously processed information, and the collection and use of sensitive personal information. The amendments also provided for the creation of the Personal Information Protection Commission (PIPC), an independent authority charged with overseeing data protection compliance.

OVERVIEW OF DATA PRIVACY LAWS IN NON-EU/EEA COUNTRIES

Countries With Privacy Laws	Year Enacted (Amended)	Registration Requirement	DPO Required[1]	Cross-border Limitations	Data Breach Notification Requirement[2]
Asia (East, Central, and South) and the Pacific (14)		4	5	11	5
Australia	2000 (2012 and 2017)	No	No (recommended)	**Yes**	**Yes**
Hong Kong	1995 (2012)	No	No (recommended)	No	No (recommended)
India	2011	No	No	**Yes**	No
Japan	2005 (2015)	No	**Yes**	**Yes**	**Yes**
Kazakhstan	2013 (2015)	No	No	**Yes**	No
Kyrgyzstan	2008	**Yes**	No	**Yes**	No
Macao	2006	**Yes**	No	**Yes**	No
Malaysia	2013	**Yes**	No	**Yes**	No
New Zealand	1993	No	**Yes**	No	No (recommended)
Philippines	2012	**Yes**	**Yes**	**Yes**	**Yes**
Singapore	2012	No	**Yes**	**Yes**	No (recommended)
South Korea	2011 (2015)	No	**Yes**	**Yes**	**Yes**
Taiwan	2012 (2015)	No	No	No	**Yes**
Turkmenistan	2017	No	No	**Yes**	No

[1] In some jurisdictions, the appointment of a Data Privacy Officer (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.

Source: MORRISON & FOERSTER LLP

Bloomberg BNA

Asia Data Privacy Laws Chart

PVLR ISSN 1538-3423

Under the amended law, sensitive personal information is now defined and subject to different collection, use, and disclosure rules. In particular, organizations must obtain individuals' express consent at the time sensitive personal information is collected unless one of the limited exceptions applies. To transfer personal information to foreign third parties (including affiliated entities), express consent or a data transfer agreement (or intercompany rules in the case of affiliated entities) is required except where the transfer is to a third party in a country that provides equivalent protection or where the foreign third party has an internal personal information protection system equivalent to that which is required for domestic organizations under the amended law. In addition, organizations that disclose personal information to third parties using the opt-out notification procedure must now also notify the PIPC about such disclosures. Disclosures that rely on this opt-out notification procedure may no longer include any sensitive personal information.

In addition, the amended law and the rules issued by the PIPC create new requirements for the creation and use of anonymized processed information. If a company creates anonymized processed information in accordance with the amended law, the company may use anonymized processed information for any purposes and transfer such anonymized processed information to any third parties.

Australia's Privacy Act 1988 (Cth) was amended in February 2017 to include mandatory breach notification requirements; the amended Act will take effect on Feb. 22, 2018, unless an earlier commencement date is proclaimed. Under the amendments, organizations must report an ''eligible data breach'' to the Office of the Australian Information Commissioner and notify affected customers immediately. An eligible data breach occurs where there is unauthorized access to, or unauthorized disclosure of, the information'' and ''a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.'' Failure to comply with the notification obligation is subject to civil penalties for serious or repeated interferences with privacy up to AU$360,000 ($273,100) for individuals and AU$1.8 million ($1.37 million) for organizations.

In September 2016, the Philippines finally issued in final form the Implementing Rules and Regulations (Rules) for its Data Privacy Act of 2012. The Rules introduced significant changes to or expanded upon the legal requirements set forth in the Philippine Law, particularly with respect to third-party disclosures, security, registration, data breach notification, and internal policy requirements. In addition, the exemption for outsourcing was narrowed. In December 2016, the Philippine data protection authority (DPA) issued additional rules for managing and reporting data breaches. These rules require, among other things, the creation of a data breach response team and outline the elements to be contained in a security incident management policy, preventive measures to be taken, and the internal documentation and DPA notification requirements.

New Data Privacy Laws Enacted and Under Development

In March 2017, Turkmenistan became the latest country in the region to enact a comprehensive data privacy law that regulates the processing of personal information by both the public and private sectors. The law, which takes effect on July 1, 2017, is largely a consent-based regime. In particular, written consent is required to collect, use, and disclose personal information unless one of the limited exceptions applies. While it does not require database registration, the appointment of a data protection officer, or notification to individuals in the event of a data breach, the law does restrict cross-border transfers, require organizations to take the necessary security measures, and provide access and correction rights. Organizations must respond to access and correction requests within one working day.

Even though they have not yet enacted comprehensive data privacy laws, China and Indonesian both recently enacted laws or issued regulations that alter significantly the privacy landscape in these countries. For example, when China's Cyber Security Law (CSL) and its implementing regulations took effect on June 1, 2017, there will be a number of privacy and data security provisions that are likely to apply to a wide range of organizations that either own or use a computer information network (and effectively to all personal information in electronic form). Under the CSL, the collection and use of personal information must comply with the principles of legality, legitimacy, and necessity and the purpose. The method and scope of the collection and use of personal information must be expressly disclosed, and the collection and use of personal information must be based on the individual's consent. Individuals can demand that personal information collected unlawfully be deleted and inaccurate personal information be corrected. No organization or individual may steal or acquire personal information by unlawful means, or unlawfully sell or unlawfully provide personal information to others. Moreover, the CSL restricts transfers of personal information to overseas parties by making such transfers subject to completion of a security review undertaken in accordance with standards mandated by the Cyberspace Administration of China and other departments of the State Council, with no exemption contemplated under the law. Operators of ''key information infrastructure'' are also required to store in China both personal data and ''significant data'' (undefined) collected and produced in the course of business operations in China.

Similarly, in December 2016, Indonesia issued new implementing regulations for its 2008 Electronic Information and Transaction Law which will greatly expand the privacy protections for electronic personal information. The Electronic Information and Transaction Law regulates all electronic transactions conducted inside or outside Indonesia. Among other things, the Law contains general privacy provisions such as the right to enjoy personal life and be free from any invasion, the right to communicate with others without surveillance, and the right to access information about one's personal life and data. Anyone whose privacy rights are infringed may lodge a claim for damages incurred under the law. As a result of the new implementing regulations, there are now requirements on the acquisition, collection, processing, analysis, storage, display, publication, transmission, dissemination, and destruction of personal information transmitted through electronic media. In particular, electronic systems operators have obligations with respect to notice, consent, access and correction, data security, breach notification, data quality, and data retention. Electronic systems operators are

broadly defined as individuals or organizations that provide, manage, and/or operate electronic systems individually or jointly, in the interests of the electronic system's users and/or the interests of other parties. Electronic systems operators have two years to comply with these new requirements. With the enactment of these new implementing regulations, Indonesia's Electronic Information and Transaction Law effectively has been transformed into a de facto data privacy law.

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 or to signal the regulator's intent to actively enforce recently enacted rules. 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 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; however, Singapore has now begun to take enforcement actions against organizations. In the past year, Singapore has issued more than two dozen enforcement actions which included both warnings to organizations to correct their non-compliant privacy and data security practices and the imposition of fines ranging from SG$500 ($360) to SG$ 60,000 ($43,240). Most of the violations cited were for failing to implement adequate security measures.

In Japan, the number of enforcement actions on an annual basis has declined in recent years. The most serious case to date occurred in 2014 when the Benesse Corp., an education service provider, suffered a data breach that affected 48.6 million customers. Citing Benesse's lax security procedures and inadequate supervision of personnel, the Ministry of Economy, Trade, and Industry issued a recommendation requiring Benesse to take responsibility for the actions of its business partners, increase management attention to data security, and ensure that its data protection administrative structure was in place. Fines or other penalties were not issued. With the creation of the new data protection regulator, it is unclear whether the PIPC intends to take a similar enforcement approach.

In South Korea, the Ministry of the Interior (MOI), the authority with responsibility for enforcing South Korea's Personal Information Protection Act (the Act), announced in April 2017 that it had taken administrative enforcement action against a large number of companies for violations of the Act. The enforcement stemmed from on-site inspections of 162 companies that the MOI conducted between January and June 2016. As a result of the inspections, the MOI imposed monetary penalties and other corrective actions on 100 companies for violations of the Act, including fining 11 companies, which the MOI publicly named under its ''name and shame'' policy, over 10 million won ($8,800) each. Among the 11 companies on which the MOI imposed significant penalties, common violations included failure to encrypt sensitive personal information in transit and in storage, and failure to destroy personal information that was no longer necessary for the purposes for which it was collected. Other violations included collecting personal information that was not necessary for the stated purpose, failing to maintain appropriate access controls to the personal information processing system, and failing to obtain a separate consent for marketing uses.

In Australia, the DPA-initiated investigations have increased, largely in response to the growing number of data breaches in the region. The Australian DPA uses its own risk assessment criteria to determine whether to open an investigation, including: the number of people affected and the possible consequences for those individuals, the sensitivity of the personal information involved, the progress of an organization's own investigation into the matter and consideration of the actions taken by the entity in response, and the likelihood that the investigation will reveal acts or practices that involve systemic interferences with privacy and/or that are unidentified.

In 2016, the Australian DPA issued several determinations in connection with some of its investigations as well as in response to some unresolved privacy complaints. For example, in one case it ordered a credit reporting agency to pay the complainant AU$10,000 ($7,590) for failing to ensure that certain credit information the agency collected about the complainant was accurate, up-to-date, and complete. In another case, the DPA ordered a bank to pay a complainant AU$10,000 ($7,590) for using his personal information for a purpose other than the primary purpose for which the information was collected, and for failing to take reasonable steps to protect the complainant's personal information from misuse and loss and from unauthorized access, modification, or disclosure. The DPA also accepted three enforceable undertakings. Enforceable undertakings are accepted where the organization has cooperated with a DPA-initiated investigation, an inquiry into a data breach incident, or a privacy complaint investigation conducted by the DPA and it is believed that an enforceable undertaking would provide an appropriate regulatory outcome to the matter. The issues in these cases concerned data security breaches, inadequate security measures, and improper collection of personal information.

Direct Marketing

Enforcement activity in Hong Kong also increased in 2016, particularly in connection with direct marketing violations. Of the 112 cases referred to police for criminal investigation and prosecution, 109 were related to direct marketing violations. Since the new Direct Marketing regulatory regime took effect in April 2013, seven cases that were referred to the police for criminal investigation resulted in convictions as of December 2016. One of three convictions in 2016 was against a watch company that used an individual's personal data in direct marketing without proper notice or consent. The company was fined HK$16,000 ($2,050).

  PVLR ISSN 1538-3423

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, particularly South Korea, have very detailed rules regarding data security that may set the standard for the entire region and also influence the rest of the world.

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. In contrast to their Latin American counterparts, which require organizations to respond to access and correction requests in very short periods of time, many countries in Asia either do not specify time frames or provide organizations with a more reasonable time frames, similar to those found in European countries. Notable exceptions include Kazakhstan, Kyrgyzstan, Malaysia, South Korea, Taiwan, and Turkmenistan which have time frames that range from 1 to 21 days.

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.

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, three-quarters 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 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 three of the jurisdictions in the region.

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

Lastly, four of the countries, Kazakhstan, Singapore, South Korea, and Turkmenistan, 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, and data security breach notification and registration obligations.

Country-by-Country Review of Differences

AUSTRALIA

Australia's Privacy Act 1988 (Cth) (Australian Law) has been amended three times since it was enacted: 2000, 2012, and 2017. The most recent change to the law, which will take effect on February 22, 2018, imposes mandatory notification obligations in the event of a data security breach. Failure to comply with the notification obligation is subject to civil penalties for serious or repeated interferences with privacy up to AU$360,000 for individuals and AU$1.8 million for organizations.

In Brief

The Australian Law has detailed rules on cross-border transfers and requires notification in the event of a data security breach. Like most of the laws in the region, the Australian Law does not require database registration or the appointment of a DPO; however, the privacy commissioner recommends that organizations appoint a DPO. Other unique characteristics include an employee records exemption and the application of the law to cover all organizations with ''Australian links.''

Special Characteristics

Data Protection Authority

The Australian Law is administered by the privacy commissioner in the Office of the Australian Information Commissioner (DPA). 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.

Application of the Act

One of the significant changes to the Australian Law made in 2012 was the extension of the Australian Privacy Principles (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 APP guidelines, 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.

An entity merely having 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 relationship between the employer and the individual'' remains intact; the intention is to revisit this issue in the future.

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

Until February 2018, 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 that recommends that notice be provided to the DPA and affected individuals where the breach creates a real risk of serious harm to individuals. When the amendments take effect in 2018, organizations must report an ''eligible data breach'' to the DPA and notify affected customers immediately. An eligible data breach occurs where there is unauthorized access to, or unauthorized disclosure of, the information'' and ''a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.''

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. 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. 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

  PVLR ISSN 1538-3423

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.

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, that provision 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. 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. Organizations may also choose to notify the privacy commissioner.

Marketing

One of the most significant changes in 2012 was to more closely regulate the use and provision of personal information in direct marketing activities. Under these new direct marketing rules (guidance note on the direct marketing rules, here), 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.[1] ''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 ($64,108) and three years' imprisonment. In cases involving transfer of personal data for gain, a fine of HK$1 million ($128,217) 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. 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.

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.

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. 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., the organization 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. Written consent is required to process 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

In September 2015, Japan enacted legislation to amend the country's 2005 Personal Information Protection Act, which regulates the handling of personal information of natural persons by private sector organizations (Japanese Law). The amendments, which went into effect on May 30, 2017, made significant changes to the ways in which companies handle personal information, particularly with respect to disclosures to third parties, international transfers, anonymously processed information, and the collection and use of sensitive personal information. The amendments also provided for the creation of the Personal Information Protection Commission (DPA), an independent authority charged with overseeing data protection compliance. The creation of the DPA represents a significant change in the approach to enforcement which previously had been the responsibility of national administrative agencies and local governments.

In Brief

The Japanese Law imposes restrictions on cross-border transfers and sets forth special rules for sharing personal information with third parties and using anonymized information. The appointment of a DPO and data breach notification are required in the financial services sector and recommended in all other sectors.There are no registration requirements, however.

Special Characteristics

Data Protection Authority

The Personal Information Protection Commission (DPA), an independent government authority, has been established to unify authority relating to data protection under a single governmental agency. Up until now, the data protection rules have been enforced and interpreted by the ministries responsible for enforcement in their individual sectors: 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, Labor, and Welfare (MHLW); and the Ministry of Land, Infrastructure, Transport, and Tourism (MLIT).

Anonymized Information

The recent amendments and the rules issued by the PIPC create new requirements for the creation and use of anonymized processed information. If a company deletes certain information that may identify individuals from personal information and creates anonymized processed information in accordance with the amended law, the company may use anonymized processed information for any purposes and transfer such anonymized processed information to any third parties. There are also specific rules for companies that anonymize data, including when transferring anonymized information to a third party, publicly announcing the items of information included in the anonymized information to be provided and the method of the provision, and notifying the third party that the transferred information is or contains anonymized information.

Cross-Border Transfers

Prior to the 2015 amendments, the Japanese Law did not impose limitations on cross-border transfers; however, the rules for disclosures to third parties did apply. Now, under the amendments, express consent or a data transfer agreement, or intercompany rules in the case of affiliated entities, are required to transfer personal information to foreign third parties (including affiliated entities) except where the transfer is to a third party in a country that provides equivalent protection or where the foreign third party has an internal personal information protection system equivalent to that which is required for domestic organizations under the amended law.

Data Protection Officer

Although the Japanese Law does not require the appointment of a DPO, a DPO is required in the financial and credit sectors and, in all other sectors, the PIPC recommends that organizations appoint a person in charge of handling personal data as part of their security measures.

Data Security

Organizations must 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 breach notification is not explicitly addressed in the recent amendments but is addressed in guidelines for the financial sector. These guidelines which remain in force require business operators in this sector to report to the regulators information regarding data breaches and remedial measures taken in the event of a

   ISSN 1538-3423

leakage of personal information. In addition, the PPC has issued guidance applicable to all sectors that recommends that business operators report relevant facts and remedial measures to the PIPC (or competent minister if so specified by the PIPC) in the event of a leakage, loss, or damage of personal information, except for some minor incidents (e.g., if there was no substantial harm because the leaked information was retrieved before it could be reviewed by third parties). Data breach reporting forms will be available on the PIPC website in the near future.

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 reported to the individuals or publicly announced.

Opt-Out Notification

Organizations may disclose non-sensitive personal information to third parties without obtaining opt-in consent if the organizations provide the requisite prior notice to individuals and notify the PIPC. The requirement to notify the PIPC is one of the changes under the amendments. In addition, the use of this opt-out notification procedure for disclosures involving any sensitive personal information is now prohibited.

Sensitive Information

Under the amended PIPA, sensitive personal information is now defined and subject to different collection, use, and disclosure rules. In particular, organizations must obtain individuals' express consent at the time sensitive personal information is collected unless one of the limited exceptions applies.

KAZAKHSTAN

The Law on Personal Data and Protection (Kazak Law), which went into effect in November 2013, protects all personal information of natural persons and applies to both the private and public sectors. The law was amended in November 2015 to impose new data localization requirements, effective January 2016.

In Brief

The Kazak Law restricts cross-border transfers to countries that do not protect personal information. It also imposes data localization requirements and exceedingly short timeframes for responding to access and correction requests. However, there are no data breach notification, special security, DPO, or registration requirements.

Special Characteristics

Data Protection Authority

There is no independent data protection authority responsible for enforcement of the Kazak Law. In practice, the General Prosecutor's Office and its territorial bodies are authorized to investigate and initiate administrative cases involving data protection law violations; the Ministry of Internal Affairs and the Ministry of Finance are responsible for investigating and initiating criminal cases involving data protection law violations.

Access and Correction

Access requests must be acted upon within three working days; correction requests must be acted upon within one day.

Cross-Border Transfers

Personal information may be transferred without restriction to a country that protects personal information. However, to transfer personal information to a country that does not provide such protection, consent or another one of the very limited exceptions must apply.

Data Localization

Effective January 1, 2016, companies established in Kazakhstan as well as representative offices and branches of foreign companies that own or operate databases containing personal information must store personal information in Kazakhstan. It is unclear, however, if this storage requirement applies to foreign companies without any legal presence in Kazakhstan whose operations are aimed at Kazakhstan and whose websites are accessible in the territory of Kazakhstan (e.g., Internet companies).

KYRGYZSTAN

The Law on Personal Data (Kyrgyz Law), which went into effect in April 2008, protects all personal information of natural persons and applies to both the private and public sectors.

In Brief

The Kyrgyz Law restricts cross-border transfers, requires database registration (not yet in force), and imposes exceedingly short timeframes for responding to access and correction requests. In addition, similar to laws in the EU, the Kyrgyz Law requires organizations to have a legal basis for processing personal information such as consent, legitimate interests, vital interests, or legal requirements. However, the Kyrgyz Law does not impose data breach notification, special security, or DPO requirements.

Special Characteristics

Data Protection Authority

The Kyrgyz Law requires the government to designate a specific state body to regulate the collection and use of personal information, handle registrations, maintain records of personal data files and holders of such files, and make international agreements on the cross-border transfer of personal information. The State Registration Service, the public authority responsible for, among other things, implementing the country's informatization policy and supervising business activities and programs in this sector, has some but not all of the DPA functions set forth in the law. In particular, the State Registration Service has not been given authority over the registration process for personal data holders.

Access and Correction Requests

Access and correction requests must be fulfilled within seven days.

Cross-Border Transfers

Personal information may not be transferred to countries that do not provide an adequate level of protection unless one of the limited exceptions applies such as consent or vital interests.

Legal Basis for Collection and Use

Similar to EU law, the Kyrgyz Law requires organizations to have a legal basis for processing personal information such as: the individual has consented to the processing (consent); the processing is necessary to pursue a legitimate interest of the organization (legitimate interests), the processing is necessary to protect the vital interests of the individual (vital interests), or the processing is necessary to comply with a legal requirement (legal requirement).

Registration

Companies must register with their personal data files with the DPA; however, as of May 2017, the government has yet to designate a state authority responsible for registration.

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. 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.

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; organizations were given three months (until Feb. 15, 2014) to comply. 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.

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 2017, 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

  PVLR ISSN 1538-3423

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. 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.

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.

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. While the law entered into force Sept. 8, 2012, the Implementing Rules and Regulations (Rules) were not issued until September 2016. The Rules introduced significant changes to or expanded upon the legal requirements set forth in the Philippine Law, particularly with respect to third-party disclosures, security, registration, data breach notification, and internal policy requirements. In addition, the exemption for outsourcing was narrowed. In December 2016, the Philippine National Privacy Commission issued additional rules for managing and reporting data breaches. These rules require, among other things, the creation of a data breach response team and outline the elements to be contained in a security incident management policy, preventive measures to be taken, and the internal documentation and DPA notification requirements.

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. The Philippine Law does not require registration. In addition, the Philippine Law contains an exemption for outsourcing providers.

Special Characteristics

Data Protection Authority

The National Privacy Commission (DPA), established in March 2016, is responsible for administering, implementing, and monitoring compliance with the Philippine Act, as well as investigating and settling complaints. Located within the Department of Information and Communications Technology (DICT), the DPA does 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; however, data controllers and processors remain subject to the requirements of implementing data security measures under the Philippine Law and Rules. 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 (except for data security) 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 processing that is done or engaged in by an organization with links to the Philippines that uses equipment located in the Philippines, maintains an office, branch, or agency in the Philippines for processing personal data, has entered into a contract in the Philippines, provides its parent or affiliate with access to the personal data, carries on business in the Philippines, or collects or holds personal data 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 a resident. 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

As part of the required organizational security measures, controllers and processors must designate an individual or individuals who will function as data protection officer (DPO) or compliance officer or otherwise be

accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security. In March 2017, the DPA issued advisory guidelines on the designation of data protection and compliance officers. The guidelines set forth detailed rules in a number of areas including the data protection officer's duties and responsibilities, appointment status, and degree of independence, and the controller's and processor's obligations vis-a-vis their data protection and compliance officers.

Data Security Breach Notification

The controller must notify the DPA and affected individuals within seventy-two hours when the controller or the processor has knowledge or a reasonable belief that a personal data breach requiring notification has occurred. Notification of a data breach is required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the controller or the DPA believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected Individual. These rules require, among other things, the creation of a data breach response team and outline the elements to be contained in a security incident management policy, preventive measures to be taken, and the internal documentation and DPA notification requirements.

SINGAPORE

Singapore's Personal Data Protection Act 2012 (Singapore Law) came into force in January 2013. 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.

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.

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 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, email 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 Breach Notification

There is no express obligation under the Singapore Law on any entities to give notice in the event of a data security breach. However, in May 2015, the DPA issued a Guide to Managing Data Breaches, which recommends that individuals whose personal information has been compromised be notified immediately if a data breach involves sensitive Personal Data. The DPA should be notified of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals.

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 Korean Data Protection Act (PIPA or Korean Law), which took effect in September 2011 and was subsequently amended in 2015, regulates public and private sector processing of personal information of natural persons. 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. 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. The Korean Law also imposes extensive obligations in such areas as notice, consent, and data security. Registration is not required, however.

  PVLR ISSN 1538-3423

Special Characteristics

Data Protection Authority

The Ministry of the Interior (MOI), formerly the Ministry of Government Administration and Home Affairs, is the authority responsible for enforcing the Korean Law.

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 it intends to provide personal information to a third party across the national border, an organization 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 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. In addition, under the recent amendments, organizations that process ''Particular Identification Information'' (i.e., resident registration numbers, passport numbers, driver's license numbers, and alien registration numbers) will be subject to regular inspections by the Minister of the Interior (or a designated specialized agency) to determine whether they have implemented measures necessary to ensure the security of the Particular Identification Information.

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. Individuals who suffer damages resulting from a data breach caused by an organization's willful misconduct or gross negligence may be entitled to punitive damages of up to three times the actual damages. In addition, individuals whose personal information has been lost, stolen, or leaked due to a data breach caused by negligence or willful misconduct may request statutory damages of up to 3 million South Korean won ($2,632).

TAIWAN

Taiwan's Personal Data Protection Act (Taiwanese Law) entered into effect in October 2012. The Taiwanese Law, which 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, now provides protection to personal information of natural persons across all public and private entities and across all sectors. In December 2015, the Taiwanese Law was amended to address concerns about the rules for processing sensitive personal data and the notice requirements for processing personal data collected prior to the entry into force of the PDPA. Those amendments went into effect on March 15, 2016.

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.

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.

TURKMENISTAN

In March 2017, Turkmenistan enacted a privacy law (Turkmenistan Law) that regulates the processing of personal information by both the public and private sectors. The Turkmenistan Law, which takes effect on July 1, 2017, is largely a consent-based regime. In particular, written consent is required to collect, use, and disclose personal information unless one of the limited exceptions applies.

In Brief

The Turkmenistan Law restricts cross-border transfers but does not require registration, the appointment of a DPO, or data breach notification.

Special Characteristics

Data Protection Authority

The Turkmenistan Law authorizes the government to establish a privacy regulator to work with the State Prosecutor's Office to oversee and enforce the law.

Access and Correction

Individuals have the right to access and correct their personal information. Organizations must respond to access and correction requests within one working day.

Cross-Border Transfers

Personal information may not be transferred to countries that do not provide protection unless one of the limited exceptions applies, such as written consent or where necessary to protect the life or health of the individual.

Links to all of the data privacy laws and data protection authorities discussed in this article are available Morrison & Foerster's online Privacy Library at https://www.mofo.com/privacy-library/.

PVLR ISSN 1538-3423