In the 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 13 jurisdictions now have comprehensive privacy laws.

**Asia**

Privacy Laws in East, Central and South Asia and the Pacific

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. Thirteen jurisdictions in Asia now have comprehensive privacy laws: Australia, Hong Kong, India, Japan, Kazakhstan, Kyrgyzstan, Macao, Malaysia, New Zealand, the Philippines, Singapore, South Korea and Taiwan. New Zealand is the only jurisdiction in the region that has been recognized by the European Commission as providing adequate protection (13 WDPR 25, 1/25/13).

Notably absent from this list are countries such as China, Thailand, Vietnam and Indonesia. China is slowly moving toward a privacy regime, taking a piecemeal, sectoral approach to privacy, much like the United States. Thailand, Vietnam and Indonesia all have robust data protection regimes, but do not currently meet the criteria for EU adequacy decisions. (For a detailed discussion of the European Commission’s adequacy decisions, see 7 WDPR 107.12, 2/10/11).
This article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments.

Common Elements Found in Asian Laws

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

Choice
Every privacy law also includes some level of choice element. The level or type of choice varies significantly from country to country. For example, South Korea has a rather unique approach to alternative dispute resolution, and Thailand has no such system at all, while New Zealand has all of the laws in Asia include choice as a crucial element in the law.

Security
Restrictions: 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, or destruction. Some of the countries—particularly those in the EU—have very detailed rules regarding data security and data breach notification, and the appointment of a data protection officer (DPO), while others set limits on how long data may be retained or how long documents may be retained by an organization once the purpose for which the information was collected was achieved.

Access and 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 share with them significant rights to also ensure that their records are accurate, complete, and appropriate, access, update or correct that information. In contrast to their Latin American counterparts, registration is not required in all but three countries, South Korea—has very detailed rules regarding data security, data breach notification and the appointment of a DPO. The differences widen when comparing their respective rules on data breach notification, security and DPO obligations. For example, two-thirds of the countries in this region have drafted legislation but the bills have yet to be introduced to their respective legislatures. The governments of Thailand and Indonesia have not been successful in drafting any kind of data protection law or implementing any kind of data protection regulations.

The differences vary widely from each other and from laws in other regions of the world.

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

Differences in Approaches
While the core data protection principles and requirements are reflected in all of these laws, specific requirements vary widely from country to country. For example, South Korea has very comprehensive rules on data breach notification, and very comprehensive rules on data breach notification. The level or type of choice varies significantly from country to country. For example, South Korea has a rather unique approach to alternative dispute resolution, and Thailand has no such system at all, while New Zealand has all of the laws in Asia include choice as a crucial element in the law.


copyright 2023 by the bureau of national affairs, inc., washington, d.c. wdr issn 1473-3579
A country-by-country summary of the obligations in these key areas is provided below. Other noteworthy characteristics are also highlighted and, where applicable, the responsible enforcement authority is identified. In addition, a chart is provided at the end to show at a glance the countries with mandatory cross-border, DPO, data security breach notification and registration obligations.

**Trends**

**Enforcement:**

Violations of these laws can result in significant criminal and civil and/or administrative penalties being imposed; however, the enforcement approaches vary widely from one jurisdiction to another. Japan, New Zealand, Australia and Hong Kong encourage businesses and individuals to resolve disputes voluntarily without resorting to the imposition of fines, except in large data breach cases 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 the competent industry-specific regulators, so the level of enforcement, as well as the interpretations of the compliance obligations under the law, varies 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, albeit through higher financial penalties for non-compliance.

**Data Breaches:**

The growing number of data breaches in the region has resulted in legislative changes, such as in South Korea, to increase penalties and impose damages for data breaches, and increased enforcement efforts. In addition, some regulators have introduced mandatory breach notification requirements to encourage organizations to report data breaches in a timely manner.

---

### Asian/Pacific Privacy Laws

<table>
<thead>
<tr>
<th>Countries with Privacy Laws</th>
<th>Registration Requirement</th>
<th>DPO Required</th>
<th>Cross-Border Liabilities</th>
<th>Data Breach Notification Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiji</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Australia</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>India</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Japan</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Mongolia</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>New Zealand</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Philippines</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Singapore</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Taiwan</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1 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.

---

Asian/Pacific Privacy Laws

Source: BNA A BNA Graphic/apac25g1
In June 2015, the Japanese DPA entered into its first enforceable undertaking with Bridgestone Corp. Ltd., another of Japan's two largest telecommunications companies, all in a matter involving a data security breach. After a massive data breach involving three major Japanese credit card companies in January 2014, South Korea's Financial Services Commission (FSC) charged the companies with a data breach that affected 10.8 million customers of Shinhan Card Inc. (Shinhan), one of Korea's leading credit card companies. The companies failed to take appropriate security measures against the credit card companies' network breaches, which resulted in the loss of sensitive personal information. The FSC ordered the companies to cease and desist from all further violations of the Personal Information Protection Act (Act) and to pay a fine of 30 million won (approximately $27,300) each. These cases resulted in criminal convictions in 2015.

Data breaches also resulted in increased civil litigation, particularly in Japan and South Korea. For example, in late 2015, a large settlement was made to resolve a multi-plaintiff class action lawsuit brought by customers of Benesse Holdings Inc., a Tokyo-based company that provides educational courses for schoolchildren. In addition, hundreds of thousands of customers of South Korea's largest telecommunications company, SK Telecom Co. Ltd., have filed class action lawsuits against the company after it suffered three significant data security breaches. As a result of these breaches, the Ministry of Knowledge Economy in December 2015, South Korea enacted the Personal Information Protection Act (PIPA), which took effect in April 2013. The PIPA requires telecommunications and Internet service providers to pay fines of up to HK$500,000 ($64,343) and 3 years imprisonment, these cases demonstrated the effectiveness of the PIPA in deterring and prosecuting data breaches.

There has also been increased enforcement of direct marketing rules in Hong Kong. Since Hong Kong's new Data Protection Ordinance (Ordinance) took effect in April 2013, the Hong Kong Personal Data Protection Authority (DPA) has, as of January 2016, referred 53 cases for criminal investigation and prosecution. Four of these cases resulted in criminal convictions, including the conviction of a DPO for failing to comply with the Ordinance. In addition, the DPA has ordered three high-profile cases to pay fines of up to HK$500,000 ($64,343) for processing sensitive personal data and for the unauthorized collection of personal information. The DPA has also entered into its first enforceable undertaking with Singtel Optus Pty Ltd., Australia's second-largest telecommunications company, all in a matter involving a data security breach. After a massive data breach involving three major Australian credit card companies in January 2014, South Korea's Financial Services Commission (FSC) charged the companies with a data breach that affected 10.8 million customers of Shinhan Card Inc. (Shinhan), one of Korea's leading credit card companies. The companies failed to take appropriate security measures against the credit card companies' network breaches, which resulted in the loss of sensitive personal information. The FSC ordered the companies to cease and desist from all further violations of the Personal Information Protection Act (Act) and to pay a fine of 30 million won (approximately $27,300) each. These cases resulted in criminal convictions in 2015.

Requirements in this region related to cross-border transfers, registration, data security, data breach notification and the appointment of a data protection officer, vary widely and from time to time in other regions of the world.

In December 2015, the European Union's General Data Protection Regulation (GDPR) took effect, replacing the 1995 Data Protection Directive. The GDPR includes a number of significant new obligations for businesses, including a requirement to appoint a data protection officer (DPO) where necessary and to conduct data protection impact assessments before processing personal data for new or significant purposes. In addition, businesses must notify the relevant data protection authority of any data breach within 72 hours of discovery. The GDPR also introduces a number of new rights for individuals, including the right to access, rectify and erase their personal data, as well as the right to object to the processing of their personal data for direct marketing purposes.

The GDPR also introduces a number of new obligations for businesses, including a requirement to appoint a data protection officer (DPO) where necessary and to conduct data protection impact assessments before processing personal data for new or significant purposes. In addition, businesses must notify the relevant data protection authority of any data breach within 72 hours of discovery. The GDPR also introduces a number of new rights for individuals, including the right to access, rectify and erase their personal data, as well as the right to object to the processing of their personal data for direct marketing purposes.
An Australian citizen; the personal information was collected or held by the entity is the registered proprietor of trademarks in the entity includes Australia as one of the countries on which its business is conducted; the entity has a website that offers goods or services to the public and private sectors; the organization carries on business in Australia or an external territory, either directly or through a subsidiary or representative; or the entity conducts activities by which it is subject to a limitation as to time imposed by law.

Special Characteristics

Employee Records

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
- an employee record is compiled or used in Australia or an external territory.

An organization, to whom or on whose behalf or at whose direction a data controller compiles or uses employee records, is subject to a limitation as to time imposed by law; or

- the employee record is compiled or used in Australia or an external territory; and
- the organization is:

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

The organization does not fall within one of the above categories will also have an Australian link where:

- an employee record is compiled or used in Australia or an external territory; and
- the organization is:

  - a body corporate incorporated in Australia or an external territory; or
  - a body corporate incorporated in Australia or an external territory and subject to a limitation as to time imposed by law.

In Brief

Like most of the jurisdictions in the region, the Australian Law has an opt-in data breach notification obligation set forth in the Bill will be deemed to be serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner (OAIC) and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches. Failure to comply with the privacy obligations set forth in the Bill will be deemed to be an infringement of the privacy of an individual by an organization. The Privacy Commissioner may take a variety of actions, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner and affected individuals of serious data breaches.
Before disclosing personal information to a recipient, organizations must take reasonable steps to ensure that the recipient does not breach the APPs. The following situations apply:

- The recipient is subject to a law or binding scheme that protects the information to a substantially similar level as the APPs, or the individual is expressly informed that, if he or she consents to the disclosure of the information by the organization.
- The individual is expressly informed, if informed, that the cross-border rules apply to transfers by the organization to its overseas affiliates but not an overseas office.
- The cross-border rules apply to transfers by the organization to its overseas affiliates and the individual consents to the disclosure of the information.
- There is no obligation to appoint a DPO; however, there is an exception under the law that covers the individual.

The cross-border rules apply to transfers by the organization to its overseas affiliates and the individual consents to the disclosure of the information by the organization.

**Data Protection Officer**

There is no obligation to appoint a DPO; however, there is a legal obligation to implement appropriate measures.

**Data Security Breach Notification**

There is no obligation to appoint a DPO; however, there is a legal obligation to implement appropriate measures.

**Data Protection Authority**

There is no obligation to appoint a DPO; however, there is a legal obligation to implement appropriate measures.

**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, it is not yet in force. The DPA has recommended the implementation of Section 33 and has also developed and subsumed recommended model data transfer clauses for such situations. The DPA has called upon the government to implement Section 33 and has also developed and subsumed recommended model data transfer clauses for such situations. The DPA has called upon the government to implement Section 33 and has also developed and subsumed recommended model data transfer clauses for such situations.
Marketing

One of the most significant changes was to more clearly regulate the use and protection of personal information. The Indian Privacy Rules provide that personal information "shall only be obtained or processed if the individual has expressed consent to the transfer of information to the recipient." This means that organizations must seek consent from individuals before transferring their personal information to third parties. The rules also require organizations to provide notice to individuals about the nature of the personal information to be processed, the purpose of the processing, and the intended recipient or category of recipient to whom the personal information is to be disclosed.

Special Characteristics

Data Protection Authority

The Data Protection Authority (DPA) is responsible for enforcing the Indian Privacy Rules. The DPA has the power to investigate complaints, conduct audits, and impose fines on organizations that violate the rules.

In Brief

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) provide guidelines for the handling of personal information in India, including provisions for the collection, storage, and processing of personal information.

In India, the Indian Privacy Rules do not apply to personal information that is in the public domain or that is accessible to the public.
Once the amended rules take effect, individuals’ personal information cannot be provided to third parties without prior consent of the individual unless an opt-out notice of third-party sharing has been provided prior to the personal information being collected. Once the amended rules take effect, individuals’ personal information will be treated as personal data 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 Internal Affairs and Communications (MIC), the Ministry of Justice, the Ministry of Health, Labor and Welfare (MHLW); the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) (a complete list of the guidelines and responsible ministries to be issued here).

Special Characteristics

Data Protection Authority

Under the 2015 amendments, the Personal Information Protection Commission (IPC), an independent governmental authority, has been established to make 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 Internal Affairs and Communications (MIC), the Ministry of Justice, the Ministry of Health, Labor and Welfare (MHLW); the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) (a complete list of the guidelines and responsible ministries to be issued here).

Each ministry issued guidelines detailing specific obligations and procedures. As a result, businesses operating in Japan have to carefully review the guidelines issued by the competent authorities in order to ensure compliance with the law. In addition, multiple guidelines governing, for example, the scope of data operations, the procedures to be followed, and the penalties for non-compliance may set out the same standard. In fact, they may actually conflict. When the conflicting provisions of the law come into force, the competent authority, has been established to unify authority relating to data protection under a single governmental agency. The determination which, until now, has been the responsibility of national administrative agencies and local governments, is part of their supervision responsibilities, these agencies have issued 39 data protection guidelines covering 27 different areas or sectors.

In Brief

Under the 2015 amendments, the Personal Information Protection Commission (IPC), an independent governmental authority, has been established to make authority relating to data protection under a single governmental agency. Effective Jan. 1, 2016; the remaining provisions will take effect in August 2017. The creation of the PIPC represents a significant change in the approach to enforcing data protection. In addition, the creation of a centralized DPA, an independent governmental authority, has been established to make authority relating to data protection under a single governmental agency. Under the 2015 amendments, the Personal Information Protection Commission (IPC), an independent governmental authority, has been established to make 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 Internal Affairs and Communications (MIC), the Ministry of Justice, the Ministry of Health, Labor and Welfare (MHLW); the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) (a complete list of the guidelines and responsible ministries to be issued here).

Each ministry issued guidelines detailing specific obligations and procedures. As a result, businesses operating in Japan have to carefully review the guidelines issued by the competent authorities in order to ensure compliance with the law. In addition, multiple guidelines governing, for example, the scope of data operations, the procedures to be followed, and the penalties for non-compliance may set out the same standard. In fact, they may actually conflict. When the conflicting provisions of the law come into force, the competent authority, has been established to unify authority relating to data protection under a single governmental agency. The determination which, until now, has been the responsibility of national administrative agencies and local governments, is part of their supervision responsibilities, these agencies have issued 39 data protection guidelines covering 27 different areas or sectors.

In Brief

Under the 2015 amendments, the Personal Information Protection Commission (IPC), an independent governmental authority, has been established to make authority relating to data protection under a single governmental agency. Effective Jan. 1, 2016; the remaining provisions will take effect in August 2017. The creation of the PIPC represents a significant change in the approach to enforcing data protection. In addition, the creation of a centralized DPA, an independent governmental authority, has been established to make authority relating to data protection under a single governmental agency. Under the 2015 amendments, the Personal Information Protection Commission (IPC), an independent governmental authority, has been established to make 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 Internal Affairs and Communications (MIC), the Ministry of Justice, the Ministry of Health, Labor and Welfare (MHLW); the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) (a complete list of the guidelines and responsible ministries to be issued here).

Each ministry issued guidelines detailing specific obligations and procedures. As a result, businesses operating in Japan have to carefully review the guidelines issued by the competent authorities in order to ensure compliance with the law. In addition, multiple guidelines governing, for example, the scope of data operations, the procedures to be followed, and the penalties for non-compliance may set out the same standard. In fact, they may actually conflict. When the conflicting provisions of the law come into force, the competent authority, has been established to unify authority relating to data protection under a single governmental agency. The determination which, until now, has been the responsibility of national administrative agencies and local governments, is part of their supervision responsibilities, these agencies have issued 39 data protection guidelines covering 27 different areas or sectors.

In Brief
Special Characteristics

Data Protection Authority

There is no independent data protection authority responsible for the enforcement of the Kazakh Law. In practice, the General Prosecutor’s Office and its territorial bodies are authorized to investigate and initiate administrative and criminal cases involving data protection law violations. The Ministry of Internal Affairs and the Ministry of Finance are responsible for overseeing and ensuring compliance with data protection laws.

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 Jan. 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) (available in Russian here), 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 data-base registration (not yet in force), and imposes 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

The Kyrgyz Law requires the government to designate a specific state body to regulate the collection and use of personal information, handle applications, maintain records of personal data files and holders of such files, and make international agreements on the transferability of personal data files and holders of such files, the public authorities responsible for, among other things, implementing the country’s information law policies, and supervising business activities and government activities that involve personal data files.

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 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 or the processing is necessary to pursue a legitimate interest of the organization (legitimate interests).

Registration

Companies must register with their personal data files with the DPA; however, as of April 2016, the government has not yet designated 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 sectors.

In Brief

The Macao Law requires the government to designate a data protection authority and requires organizations to have a legal basis for processing personal information, handle applications, maintain records of personal data files and holders of such files, and make international agreements on the transferability of personal data files and holders of such files, the public authorities responsible for, among other things, implementing the country’s information law policies, and supervising business activities and government activities that involve personal data files.
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 that are processed in Malaysia and 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.

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, investment, 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 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 must with 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 other European laws, such as:
- if the individual has consented to the transfer;
- if the transfer is necessary to perform a contract with or at the request of an individual;
- if 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;
- if the transfer is necessary to satisfy an official duty to protect the vital interests of the individual;
- if 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 April 2016, 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 hospitality, transportation, retailing, credit rating, credit bureaus (such as legal, audit, accounting, engineering or architecture) and credit or withholding dealers as defined under the Credit Reporting Agencies Act 2009.

New Zealand
New Zealand was the first country in the region to enact a data protection law. The Privacy Act 1993 (New Zealand Law), which regulates the processing of personal information 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 to New Zealand.

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.
The Philippine Law applies to the processing of all personal information of individuals by public and private sector organizations with some important exceptions.

**Personal Information**

- The Philippine Law applies to the processing of all personal information of individuals by public and private sector organizations with some important exceptions.

**Application of the Law**

The Philippine Law establishes the National Privacy Commission (the Commission) as a DPA located within the Department of Information and Communications Technology (DICT). The Commission, whose leadership was appointed in March 2016, will be vested with the power to directly impose penalties; it can only recommend prosecution and penalties to the Department of Justice.

In Brief

- The Philippine Law came into compliance with the law. Implementing regulations have yet to be issued; however, with the President's appointment of the three members of the National Privacy Commission in March 2016, the expectations are that the implementing rules and regulations will be issued soon.

**Special Characteristics**

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

- Data Protection Office
  - A DPO must be appointed regardless of the size of the organization, if the DPO is appointed by the President in March 2016, will be vested with the power to directly impose penalties; it can only recommend prosecution and penalties to the Department of Justice.

**Data Security Breach Notification**

While registration is not required for private sector organizations, organizations must designate one or more Data Protection Officers (DPOs) for information collected as part of data processing operations relating to personal information received from outside the Philippines.

- Data Security Breach Notification
  - Data Protection Officer
    - The Office of the Privacy Commissioner (DPA) regulates and administers the New Zealand Law.

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

**Data Protection Officer**

While registration is not required for private sector organizations, organizations must designate one or more Data Protection Officers (DPOs) for information collected as part of data processing operations relating to personal information received from outside the Philippines.

- Data Security Breach Notification
  - Data Protection Officer
    - The Office of the Privacy Commissioner (DPA) regulates and administers the New Zealand Law.
In Brief
The Personal 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. It is the primary privacy law in South Korea, and regulates the processing of personal information in the context of services provided by telecommunications carriers, banking institutions, financial institutions, and other types of organizations. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal 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. The 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. The Personal Data Protection Act (PIPA or Korean Law), which took effect in September 2011 and was subsequently amended in 2 Data Protection Officer
Organization must designate one or more data protection officer(s) responsible for ensuring the organization’s compliance with the Singapore Law.

In Brief
The Singapore Law restricts cross-border transfers and requires the appointment of a DPO and data security breach notification. It also prohibits the sending of certain marketing messages as spam.

Special Characteristics
The following summarizes the special characteristics of data protection rules coming into force in January 2014 and the DNC Registry provisions contained in the Singapore Law: The Singapore Law restricts cross-border transfers and requires the appointment of a DPO and data security breach notification. It also prohibits the sending of certain marketing messages as spam.

In Brief
The Singapore Law restricts cross-border transfers and requires the appointment of a DPO and data security breach notification. It also prohibits the sending of certain marketing messages as spam.

Special Characteristics
The following summarizes the special characteristics of data protection rules coming into force in January 2014 and the DNC Registry provisions contained in the Singapore Law: The Singapore Law restricts cross-border transfers and requires the appointment of a DPO and data security breach notification. It also prohibits the sending of certain marketing messages as spam.
Cross-Border Transfers

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

Data Protection Officer

Organizations must appoint a DPO with specified responsibilities.

Data Security

The Korean Law and subsequent guidance issued by the regulatory authorities also impose significant data security obligations. These data security requirements are among the most thorough 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 organization’s data security breach notification officer, and when the leak involves personal information of one hundred or more individuals, also notify the relevant data protection authority. Individuals must be notified when their personal information has been stolen, divulged or altered in any way. If the leak involves personal information of one thousand or more individuals, the organization must also notify the relevant data protection authority. If the leak involves personal information of ten thousand or more individuals, the organization must also notify the media.

TAIWAN

Taiwan’s Personal Data Protection Act (Taiwanese Law) entered into effect in October 2012 (12 WDPR 25, 9/21/12). 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 processed on any medium, including personal data stored on computer media, and personal data in transit. The Taiwanese Law entered into effect on May 20, 2012.

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 has the authority to 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 in any way.