The Asia-Pacific region has seen the most rapid development in privacy laws in recent times. Companies that operate in the region and that collect, store, and use personal information can expect increasing compliance challenges in the face of new and evolving data protection regimes. Specifically, key trends across the region include the following:

**Countries increasingly are adopting data protection rules.** A number of countries throughout the Asia-Pacific region recently adopted or are planning to adopt new data privacy regulations, including Malaysia, the Philippines, and Singapore. Additional countries, such as Hong Kong, Australia, and New Zealand, among others, are seeking to tighten their privacy rules or already have done so.

**Penalties for noncompliance are increasing.** Recent amendments to data protection rules in Hong Kong and Australia drastically increase penalties for noncompliance and/or data breaches.

**Cross-border transfers of personal data are unevenly regulated.** Similar to the European Union (EU), some Asia-Pacific jurisdictions, including South Korea and Australia, only permit cross-border transfers of personal data where the destination country has "adequate" data protection laws in place or where prior consent is obtained. Other countries have adopted cross-border transfer rules that are not yet in force, such as Hong Kong and Singapore. Finally, cross-border transfer is not explicitly regulated by law in some Asia-Pacific countries, such as Japan.

**Data privacy rules in the Asia-Pacific region are, for the most part, less stringent than EU standards.** To date, New Zealand is the only jurisdiction that is considered to have "adequate protection" by the EU.

Below, we highlight recent privacy developments in Singapore and Hong Kong. As multinational companies strengthen their presence in Asia, it is increasingly important that they be aware of new privacy requirements in these countries.

**Singapore**

Compared to data protection laws in the EU, Singapore law favors commercial flexibility and a business-friendly approach. Prior to 2012, Singapore did not have overarching legislation on data protection. On October 15, 2012, the Singapore Parliament passed the Personal Data Protection Act 2012 (PDPA). The PDPA has two objectives: (i) to enhance an individual’s control over his or her personal data, defined as "information about an identified or identifiable individual"; and (ii) to enhance Singapore’s competitiveness and strengthen its position as a trusted business hub. Unlike the EU laws, the PDPA does not reference a fundamental right of privacy.

The PDPA does not offer a particularly detailed or exacting framework for the protection of personal information. Instead, the PDPA takes a high-level approach and leaves more detailed rulemaking to sector-specific efforts by industry regulatory agencies. The PDPA addresses: (i) the collection, use, and disclosure of personal data; (ii) the transfer of personal data outside of Singapore; (iii) the protection and retention of personal data; (iv) the right to access and correct personal data; and (v) sanctions and enforcement mechanisms. The PDPA also provides for the creation of a Data Protection Commission with the authority to fine an organization an amount not exceeding $1 million for rule violations. A private right of action for persons suffering loss or damage resulting from a violation of the PDPA also is available.

The PDPA will take effect in three phases, with the main data protection provisions becoming enforceable on July 2, 2014.

**Hong Kong**

Hong Kong’s Legislative Council amended its main data protection regulation, the Personal Data (Privacy) Ordinance (Cap. 486), in June 2012 after it had remained largely unchanged since its adoption in 1997. Like the PDPA, the ordinance sets forth principles related to: (i) the purpose and manner of collection of personal data; (ii) the accuracy and retention of personal data; (iii) the use of personal data; (iv) the security of personal data; (v)
information that should be made generally available; and (vi) access to personal data. Although the ordinance prohibits the transfer of personal data outside of Hong Kong except in specified circumstances, these cross-border transfer rules are not yet in force.

The 2012 amendment drastically increases penalties and introduces new offenses particularly focused on direct marketing and unauthorized disclosure of personal data. Malicious disclosure of personal data without consent, for example, now carries a maximum penalty of up to HK$1 million and imprisonment for up to five years. The amendment also enhances the authority of the Privacy Commissioner for Personal Data and introduces a new scheme whereby the commissioner may provide legal assistance to individuals.

* * *

Data protection regulations will continue to develop throughout the Asia-Pacific region. It is critical that businesses that operate throughout the region develop their compliance positions to avoid regulatory investigations, fines, and other sanctions.

For more information, please contact Umair Javed at 202.719.7475 or ujaved@wileyrein.com.