Privacy laws in Asia

The GDPR deadline is certainly looming but, writes Courtney Bowman, companies would be well advised not to forget the data privacy laws of the other countries in which they operate.

With the impending enforceability of the GDPR on 25 May, all eyes are on the EU as it ushers in a sweeping new data privacy regime that promises to change many companies' data-handling practices. Although the GDPR understandably has occupied much of the data protection spotlight for the last year, it is far from the only landmark data protection law worthy of attention. In particular, the privacy landscape in Asia is shifting in ways that promise to affect how multinational companies collect, process, store, and transfer personal data in the region, especially as multiple countries have enacted new laws (or have amended existing ones) within the past few years. This article provides an overview of some of the region's more high-profile laws and their potential effects on businesses.

Japan

Japan's Act on the Protection of Personal Information ('APPI'), which went into effect in 2005, is thought to be one of Asia's oldest privacy laws. Not surprisingly given the pace of technological advancement – not to mention the evolution of privacy law around the world over the past decade – the Japanese government determined that the APPI was in need of an overhaul and enacted an amended version in mid-2017.

The amended law makes several significant changes to Japanese privacy law that will affect companies based in Japan, as well as those based outside of Japan that collect data from individuals in the country. Perhaps most importantly for multinationals, the law imposes restrictions on the transfer of personal information out of Japan, which will affect the many organisations that collect data from their Japan-based consumers or employees. Specifically, a company may only transfer personal information out of Japan if one of three conditions is met: the data subject consents to the transfer, the country in which the recipient is located has privacy laws that the Japanese Personal Information Protection Commission has determined are adequate in comparison to Japan's laws, or the recipient takes measures to ensure that it provides adequate measures for the protection of the data subject's privacy. Companies also are required to keep records of any transfers made to third parties outside the country. These changes mean that companies operating in the Japanese marketplace will have to evaluate the extent to which they collect the personal information of individuals in Japan and transfer it overseas. Assuming a company confirms it engages in such transfers, the company should then determine how it is ensuring the transferred data is treated in accordance with Japanese privacy law, including by evaluating how it and its vendors handle the personal data of individuals transferred from Japan, and how it keeps track of any data exports from the country to a third party. Internal policies may require revision, and contracts with third-party vendors may need to be amended as well.

Japanese privacy law imposes restrictions on the transfer of personal information out of Japan, which will affect the many organisations that collect data from their Japan-based consumers or employees.

Importantly, Japan is seeking an adequacy determination from the EU. Under current EU privacy law, as well as the soon-to-be-enforceable GDPR, companies generally cannot transfer personal data out of the EU unless they have ensured that the data will receive adequate protection in the non-EU jurisdiction. For most transfers – including transfers from the EU to the United States – that means companies must enter into mechanisms designed to impose EU-style privacy protections on the data being transferred (such as standard contractual clauses or binding corporate rules), or rely on the consent of the data subjects to transfer the information, which can be difficult to obtain and which data subjects may revoke. However, the EU has determined that a few countries have 'adequate' data protection regimes, meaning such safeguards are not required for transfers to those countries. Among the select 'adequate' jurisdictions are Switzerland, Argentina, and New Zealand; to date, however, no country in East Asia has been added to the list. That may change in the very near future, as Japan announced its intent to obtain adequacy status last year, and a decision is expected sometime in 2018. As part of any deal to that effect, Japan likely would grant the EU an adequacy determination of its own, meaning that personal information could be transferred from Japan to the EU without hassle. The news would be a boon for Japan, as it would

allow for a freer flow of personal information between the two jurisdictions, thereby saving companies the time and resources they otherwise would be spending on setting up the appropriate transfer mechanisms.

South Korea

When it comes to data privacy, South Korea has one of the most stringent legal landscapes in the region and, perhaps, the world. In addition to its omnibus privacy law, the Personal Information Protection Act ('PIPA'), it also has a number of sector-specific laws, including laws governing the use of personal information in the IT and financial services industries, as well as relating to the use of credit information. Moreover, potential fines for violating these laws are substantial, and the Minister of Security and Public Administration – who is charged with enforcing PIPA – has shown an increasing tendency to level criminal penalties against violators. The Minister also has the power to suspend data processors that violate PIPA, a remedy that is not as harsh as imprisonment but nevertheless may be at best disruptive, or at worst devastating, for some companies.

In 2016, South Korea introduced especially stringent penalties for information and communication service providers that illegally transfer personal information abroad. The amendment to the Act on the Promotion of IT Network Use and Information Protection states that if a service provider transfers personal information abroad without obtaining the consent of the data subject, it may be required to forfeit up to 3% of the revenue related to that transfer. That same amendment states that a service provider who suffers a major data breach as a result of an intentional act or its own negligence may be liable for 3% of the actual damages suffered by data subjects.

Like Japan, South Korea currently is seeking an adequacy determination from the EU. Once granted, South Korea can expect to receive the same benefits as Japan: namely, a largely unimpeded flow of personal data between South Korea and the EU.

China

China has long had a complicated privacy law landscape. Historically, Chinese privacy law has been sectoral, with a panoply of laws imposing different privacy-related requirements on various sectors – the Practicing Physicians Law, the Commercial Banking Law, and the Postal Law are just a few examples. While China still does not have anything that could be described as an omnibus privacy law, the recently-enacted Cybersecurity Law – which went into effect on 1 June 2017 – is a wide-ranging law that promises to have a significant effect on how companies both domestic and foreign handle personal data collected in China.

The Cybersecurity Law contains both privacy and cybersecurity-related provisions, and applies primarily to 'network operators' and 'critical information infrastructure ('CII') providers'. Both terms are defined broadly, especially 'network operators', which includes any company that owns or administers a computer network – a definition, in practice, that sweeps most companies into its ambit. CII providers, meanwhile, are defined as those who provide services that would damage China's national security or the public interest if the services were damaged. The Cybersecurity Law requires both types of companies to obtain data subjects' informed consent in order to collect their personal information, implement cybersecurity incident plans, and ensure the security of their network, among other things. CII providers are subject to additional requirements, including a mandate that they store personal information and 'important data' in China. This data localisation requirement is significant, particularly because the Chinese government has evinced an intent to expand this requirement to apply to network operators as well. Were the government to do so, it suddenly would be requiring a large number of companies of all sizes to store the personal data they collect in China, along with any 'important data' (a term that remains vague) in-country. For many companies, that would mean significant investment in the logistics and infrastructure required to keep the data in-country, such as buying or renting servers, and adopting the technology required to identify data collected in China and keep it stored in the country. At the other end of the spectrum, other companies (particularly smaller ones, or ones for which doing business in China does not represent an essential part of their business strategy) could decide that this requirement is too onerous and simply pull out of the Chinese market altogether. However, the growing importance of the Chinese market means that many companies understandably will be wary of taking the latter approach.

> When it comes to data privacy, South Korea has one of the most stringent legal landscapes in the region and, perhaps, the world.

In any event, companies that collect personal data in China are advised to keep themselves appraised of the latest developments in the interpretation and enforcement of the Cybersecurity Law, as companies with even minimal business ties to China may find themselves within the scope of the law. As the Cybersecurity Law is very complex and guidance still is forthcoming, it is in companies' best interests to consult with local counsel to develop an appropriate compliance strategy.

Conclusion

At a time when companies' privacy practices are coming under increasing scrutiny – both from regulators and the media – it is important for companies to understand the laws in each country in which they operate and focus their compliance efforts accordingly. Although the GDPR may be close to monopolising the attention of the privacy professionals worldwide, other jurisdictions' privacy laws demand attention as well. In particular, the privacy laws in the three major Asian jurisdictions described above have the potential to affect the operations of multinational companies that have offices in those countries, as well as companies who do not have any physical on-the-ground presence there but have customers or employees in those jurisdictions. ■

Courtney M. Bowman is a litigation associate in the Los Angeles office of Proskauer Rose. She specialises in international data protection law.

CBowman@proskauer.com