The compliance challenges that can no longer be ignored

There has been an explosion of new data privacy regulation across the Asia Pacific region in recent years, and the challenge now facing multi-national businesses operating there, is to find practical compliance solutions to satisfy the myriad rules and requirements now in force across the region. Mark Parsons and Peter Colegate, Partner and Associate respectively at Hogan Lovells, Hong Kong, provide insight on recent legislative changes and the ways in which businesses can meet their compliance obligations.

Introduction

Although Asia's data privacy laws draw from a common set of guiding principles, each law is unique. Moreover, as freshly minted regulators come to grips with these new laws, differences in interpretation and underlying policy are becoming apparent. As a consequence, there is now a 'patchwork' of compliance requirements across the region. Depending on the country, sector specific laws, consumer protection laws, employment laws and laws in emerging areas such as cybersecurity, also complicate the compliance picture for Asia, and there is no common framework for any of these laws.

The growth of data privacy in Asia

Australia, New Zealand, Hong Kong and Japan were the region's earliest movers, passing comprehensive data privacy laws in 1988, 1993, 1995 and 2003 respectively. Since 2005, the Asia-Pacific Economic Co-Operation (APEC) Privacy Framework has been the formal catalyst for continued regulatory development across the region. The policy rationale for APEC is decidedly economic and trade-related, as Asian governments seek to continue the impressive growth of e-commerce across the region and to provide businesses both regionally and globally with greater confidence in processing their data in Asia's offshore and regional service hubs.

APEC members Singapore, Malaysia, the Philippines, South Korea and Taiwan, have all passed comprehensive data privacy regimes in the past five years. India enacted an IT law in 2011, which tracks a similar principle-based approach to data privacy. Perhaps most significantly, China has also passed a whole raft of legislation in this area in recent years, both industry specific and of more general application.

Privacy hotspots in Asia

China

Perhaps against expectation, a rapid sequence of legislative reforms in China in recent years show a serious resolve to move the country towards a more comprehensive data privacy regime. However, without the unifying force of a law to provide a framework, there has been a tendency to approach the issue in a somewhat piecemeal fashion. Specific offences in relation to misuse of personal data were introduced to the criminal law in 2009. The following year saw the introduction of specific privacy-related torts. Since then, the pace has accelerated, with a series of legislative developments commencing in 2011 concerning the processing of personal data collected through the provision of internet and telecommunications services. The most significant reforms directed at the processing of electronic personal data came into force in March 2012, followed in February 2013 with non-binding guidelines and in September 2013, with further rules specifically addressed at telecommunications and internet content providers. March 2014 saw the first significant set of amendments to the consumer protection law in the last 20 years, many of which relate to data privacy and which apply the rules to a much wider universe of all business operators in China.

The general shape of the new requirements draws from the same principle-based regulation that underlies other privacy laws in Asia, but analysing data privacy issues in China now requires a careful assessment of various overlapping laws, decisions and guidelines against the specific type of personal data involved and the circumstances of its collection and processing. The thicket of potentially relevant laws, regulations and guidelines that has grown up around this area cannot be viewed in isolation. There is a need to consider industry-specific regulation, sensitive areas of regulation, such as anti-bribery and state secrecy laws, and potential reputational issues where an issue becomes publicised in the media.

While the hardest thrust to legislative reform has been directed at curing abuses of personal data by online fraudsters and data merchants, recent high profile prosecutions have underlined the growing importance of data privacy in the Chinese legal and regulatory landscape. Multi-national businesses can no longer afford to put data privacy regulation in China on the back burner.

South Korea

South Korea is now widely understood to be amongst the most challenging jurisdictions in Asia in terms of data privacy regulation. Provisions of the over-

arching Personal Information Protection Act and the IT Network Act are supplemented by sector-specific laws, creating a very difficult compliance environment.

South Korea has extensive registration and disclosure requirements, and a need for separate specific data subject consent in areas such as the processing of sensitive personal data, data transfers and data exports. From November 2014, data subject consent is now also required by any business transmitting advertising information by email. Businesses are obliged to disclose the identities of third party data processors and must report all data security breaches to data subjects and the authorities. The legislation is backed up with extensive enforcement measures, including provision for class action suits against offenders.

Businesses are finding the requirements to be difficult to meet in practice. Some requirements, such as the obligation to disclose the identities of third party data processors, appear to many to be counter-productive to achieving data security. The official view is that these requirements must be met and substantial public resources are now being spent on official investigators. Any business with operations in South Korea needs to take these regulations into account.

Singapore

Singapore is one of Asia's most recent movers towards comprehensive data privacy regulation, with the Personal Data Protection Act fully in force from 2 July 2014.

Singapore's new law contains general requirements for data subject consent, data export controls and other measures which are now increasingly common across the region. The new Personal Data Protection Commission has been very active in undertaking public consultations about specific requirements under the law and publishing extensive explanatory guidance for businesses and consumers alike.

As regulators across the region develop policy requirements and test their enforcement tools, the risk of failing to comply with data privacy laws in Asia can no longer be ignored

Singapore has gone so far as to draw an explicit link between the implementation of data privacy regulation and its national ambitions to be a leading high tech hub in the region. While these statements should be somewhat reassuring to businesses, the law has been enacted with some of the stiffest penalties for data privacy offences in the region, with fines of up to S$1 million (USD800,000). It is clear that the new Commission will be resourced to enforce the law, a view reinforced by the announcement in November 2014 that the Commission is looking to appoint a panel of digital forensic experts to help with data breach investigation. With a strong culture of compliance in Singapore, we expect to see the island state at the fore of policy development across the region going forward.

Hong Kong

Data privacy regulation has a relatively long history in Hong Kong, with the Personal Data (Privacy) Ordinance (the PDPO) dating back to 1995. However, after many years of relatively lax enforcement, recent times have seen a regulatory environment substantially in flux.

In 2013, Hong Kong introduced one of the world's most challenging direct marketing regulatory regimes. Much of the complexity relates to requirements that direct marketing notifications be increasingly specific as to the kinds of personal data that will be used and the classes of goods and services that will be marketed. The 'opt out' standard adopted by Hong Kong also requires that data subjects affirmatively indicate that they have opted out. Silence is not sufficient. The new regime has come forward backed up by substantially increased fines and an increased willingness by the authorities to 'name and shame' offenders.

The Privacy Commissioner for Personal Data is very much an activist regulator. He has published a substantial volume of guidance on topics as diverse as data security breach notifications, cloud computing, mobile app development and public domain data. He publicly comments on developments in privacy law abroad and continues to press for wider ranging regulation and heavier enforcement powers under the PDPO. It is very likely that Hong Kong will see further development in coming years, as consumer awareness of privacy issues continues to grow.

Compliance is critical

Data privacy compliance is now a critical business issue across the region. Failure to comply can have consequences that go far beyond simply monetary fines and other regulatory sanctions: very often reputational issues are also in play. In the latest published figures for 2013, Hong Kong's Privacy Commissioner reported a 48% increase in complaints and a doubling of enforcement notices.

As regulators across the region develop policy requirements and test their enforcement tools, the risk of failing to comply with data privacy laws in Asia can no longer be ignored.

Mark Parsons Partner
Peter Colegate Associate
Hogan Lovells, Hong Kong
mark.parsons@hoganlovells.com
peter.colegate@hoganlovells.com