Asia Pacific Data Protection and Cyber Security Guide 2017

Shifting landscapes across the Asia-Pacific region

Hogan Lovells

Introduction

The data protection landscape in the Asia-Pacific ("APAC") region looks vastly different today from ten, and even five, years ago. During 2016, the region witnessed significant legislative reform in China, Japan, the Philippines and Australia, with signs of new developments to come in Indonesia and Thailand. 2016 also witnessed a significant step-up in privacy enforcement action – a trend that is likely to continue in 2017 as data protection compliance matters feature in headlines more regularly and as more and more dedicated data protection authorities take office.

Critically, 2016 saw an important parallel development in cyber security regulation emerging across the region. Cyber security laws and data protection laws often share policy objectives, and so we see a reinforcing trend towards stricter technology risk management and cross-border data transfer restrictions.

A further trend to watch for in 2017 is the influence of Europe's General Data Protection Regulation ("**GDPR**"), which is scheduled for implementation in 2018. Hong Kong's influential Privacy Commissioner for Personal Data ("**PCPD**") has announced a study of the reforms with an eye to the possible implementation of parallel reforms in Hong Kong. One of the more striking developments in the region in 2016 was the Philippines' introduction of new data protection measures that borrow very heavily from concepts found in the GDPR, such as a mandatory 72 hour data breach notification requirement, a right to data portability and specific regulation of automated profiling. As Europe raises the bar further on data protection compliance and APAC regional competition for offshore services intensifies, we can expect to see law makers in the region reconsidering how their data protection laws stack up from a European adequacy point of view.

The common resolve to move forward with reforms in Europe draws attention to the question of whether or not data protection harmonisation or interoperability can and will be achieved in the APAC region any time soon. It remains to be seen whether the Asia-Pacific Economic Cooperation ("**APEC**") members will achieve their stated ambition in agreeing the APEC Privacy Framework, which is to raise data protection standards in order to encourage consumer confidence in e-commerce and cross-border data transfers with a view to spurring on economic advancement. Heading into a 2017 that, from the broader perspective, promises protectionist impulses and other threats to international collaboration, common ground on data protection policy is becoming all the more important.

Recent key developments

A stock take of 2016 data protection developments leaves much to consider. 2016 saw the introduction of more onerous regulatory requirements in several jurisdictions, while there were also some 'near misses' in other jurisdictions where reforms remain tabled and will likely come to fruition during the course of 2017.

The following are noteworthy developments:

- Japan's Personal Information Protection Commission was appointed on 1 January 2016, tasked with supervising enforcement and application of amendments to the Act on the Protection of Personal Information ("**APPI**") taking place in 2017;
- The Philippines appointed its National Privacy Commission ("**NPC**") in March 2016, which was closely followed by the introduction and passage of the Implementing Rules and Regulation ("**IRRs**") for the country's first comprehensive data privacy law, the Data Privacy Act of 2012;
- After years of delay, Australia finally passed amendments to the Privacy Act 1988 that will impose a mandatory breach notification requirement; and
- China adopted the Cyber Security Law in November 2016, to accompany the recently enacted National Security Law and Anti-Terrorism Law.

There was also a general trend towards more demanding compliance environments across the region. In particular, a number of high profile enforcement cases arose in relation to privacy breaches in Hong Kong, including, in one case, the Magistrate court imposing a community service order on an insurance agent for breaching direct marketing laws (an offence which had previously only been penalised with fines).

During 2017:

- we can expect to see a new comprehensive data protection law in Thailand, where the government confirmed that public hearings on the new law would begin in December, with full enactment expected in early 2017;
- the passage of Indonesia's data protection law is likely, a draft of which was published in 2015 and was expected to have been passed in 2016;
- the Singapore government is expected to introduce a cyber security bill to strengthen online defences; and
- Hong Kong's PCPD is expected to conclude his review of the Personal Data (Privacy) Ordinance ("**PDPO**").

Signs of APAC harmonisation?

With the data protection compliance burden growing so rapidly in the Asia-Pacific region, multinational organisations have good reason to hope for some measure of harmonisation of compliance standards across geographies, and easy, effective solutions for cross-border data transfers.

The APEC Privacy Framework has provided some rough signposts for a common approach to principles-based data protection regulation in the region. But while the common themes are well-evident in the national data protection laws that have come into force across the region, inter-operability has clearly not been achieved. In many cases, data protection authorities are very new to their posts, and so it is understandable that dialogue has not yet developed in this area. More fundamentally, we are still in a phase where new laws are being given meaning, often with unique cultural and political interpretations that are not readily transposable across borders.

APEC has seen some progress with its Cross Border Privacy Rules ("**CBPR**") system, a voluntary system endorsed in 2011 to facilitate data flows among APEC member economies. To date, the Canada, Japan, Mexico and the United States have acceded to CBPR, meaning that organisations may submit to a program certifying their data protection practices and procedures against specific CBPR specific program requirements. According to a survey conducted by the Vietnam e-Commerce and Information Technology Agency in 2016, Korea, Singapore and the Philippines "plan to join" the CBPR and Australia, Hong Kong, Russia, Taiwan and Vietnam are "considering" joining. Despite this progress towards common compliance standards, there is still no sign of real harmonisation, and in reality priorities for policy-making and enforcement vary significantly by jurisdiction. These differences reflect different levels of economic development and political agendas, as well as different cultures and experiences with data protection issues.

Looking forward to 2017 and beyond, there is some hope that the increasing importance of balanced data protection regulation to economic development and the increasing sophistication that the region's data protection authorities are bringing to the task of regulating will rejuvenate the discussions – and the spirit - that led to the APEC Privacy Framework and lead to greater inter-operability of national laws.

Cyber Security – the global threat

Cyber security issues dominated newspaper headlines around the world in 2016, with some dubbing 2016 the 'year of the hack'. There is no doubt that cyber incidents will continue to grow in number and scale in 2017, and the APAC region will not be spared. While not exclusively concerned with data protection, cyber security regulation has significant overlaps with data protection regulation and legislative developments on these two fronts need to be tracked hand in hand.

The passage of a new National Security Law, Anti-Terrorism Law and Cyber Security Law pushed China to the forefront of developments in cyber security regulation globally. It is clear that the legislative intent of these new laws encompasses a wider range of issues than just the security of critical infrastructure. China's cyber security policy is striking

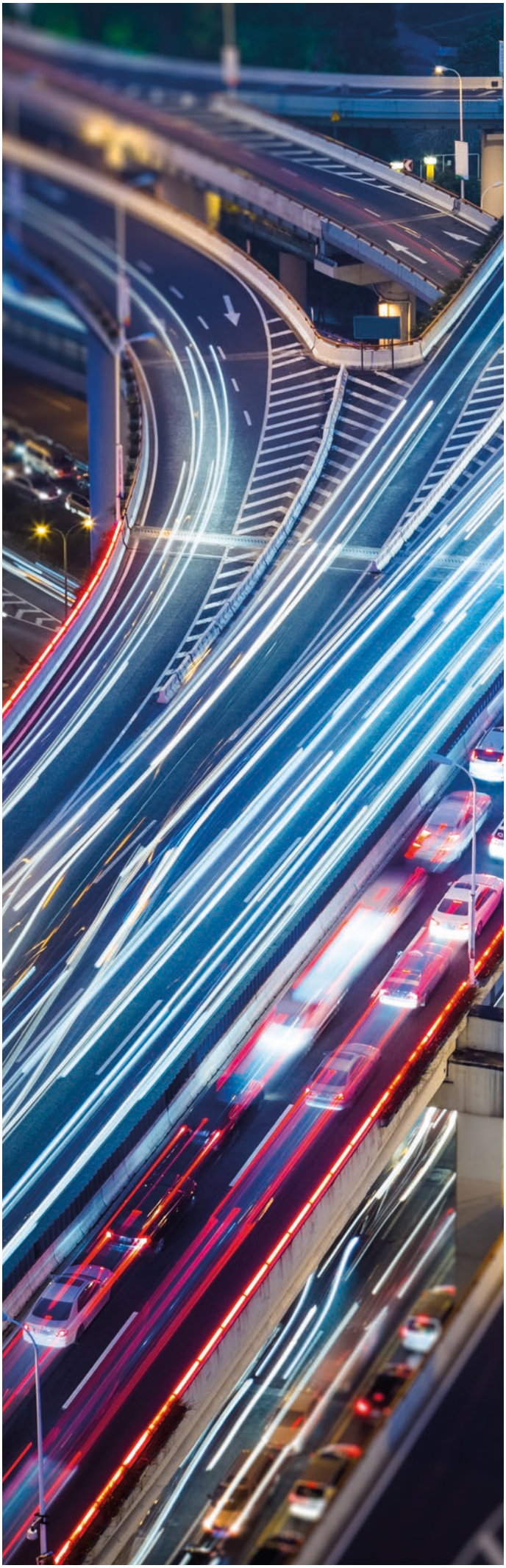
for its measures towards political control and trade regulation. From a data management point of view, China's cyber security laws mean extensive technology regulation (with pre-market certification for network technologies and measures for official access to systems and data) and obligations on critical information infrastructure operators to keep personal data and "important data" in mainland China, unless an export is necessary and the arrangements for export have passed a security review. These reforms will come into effect in June 2017, leaving businesses to struggle with the vagueness of the new laws in the meantime. It is no understatement that these new laws have forced multi-national businesses operating in China to re-evaluate their technology strategies for China.

More broadly, there have been important movements across the region towards a tightening of existing cyber security regulations. A well-publicised USD80 million bank heist in Bangladesh, in which the SWIFT interbank payments system was compromised through a malware attack, has precipitated a particularly sharpened focus on cyber security in the financial services sector. Banking regulators in Hong Kong and Singapore, two of the region's financial services hubs, have issued directions to their authorised institutions highlighting the increasing urgency of the need to address cyber security risks. The regulators are now calling for institutions to go above and beyond existing requirements and proactively develop solutions to the shifting nature and sources of cyber threats.

Biometrics, Big Data and the Internet of Things

As data protection regimes mature across the region, we are increasingly seeing lawmakers and regulators crafting regulation and compliance guidance that specifically address data protection aspects of advancing technologies in areas such as biometrics, big data and the internet of things ("**IOT**").

In the APAC region, as elsewhere, high tech solutions are promising individuals great benefits in terms of quality of life and productivity, but at the same time are raising important data protection and cyber security issues that can often run ahead of existing regulations.



Mobile health initiatives, for example, hold promise for improving the efficiency of healthcare delivery in increasingly costly environments of advanced economies and at the same time offer the means of extending the scope of healthcare to underserved populations in developing economies. These technologies, however, will typically involve the processing of extremely sensitive personal data, and so it goes without saying that data protection considerations are key for economies to realise the full benefit of the advances.

Biometric data is playing an increasingly prominent role in combatting cyber security risks, with increasing use of fingerprint, voice authentication and other technologies that seek to improve security controls. At the same time these technologies give rise to a need to seek a delicate balancing act with respect to data protection interests.

Regulators across the region are reacting to these developments:

- Japan introduced a concept of "sensitive personal data" that includes a data subject's medical history;
- Taiwan broadened its definition of sensitive personal data to include medical records;
- Hong Kong's Privacy Commissioner for Personal Data ("**PCPD**") published detailed guidance on the handling of biometric information, requiring that privacy impact assessments be carried out before such data is used, and that efforts be made to minimise its use in proportion to the objectives;

- A study conducted by the PCPD in Hong Kong in 2016 on fitness bands and other IOT devices led to the PCPD urging manufacturers to enhance data collection transparency and improve security measures;
- In July 2016, a joint development of a number of South Korean regulators, including the Ministry of Health and Welfare, the Korea Communications Commission and the Financial Services Commission introduced guidelines for the release and use of de-identified personal data through techniques such as pseudonymization, aggregation, reduction, suppression and masking techniques; and
- Singapore's 'Smart Nation' initiative has put a focus on promoting Singapore as a regional hub for developing data analytics and IOT, with the Personal Data Protection Commission calling for balance between compliance concerns and space for technological innovation. This balance is reflected in a number of respects under the Singaporean Personal Data Protection Act, which, for example does not apply to publicly available personal data.

We expect to see continuing tensions between the strong economic development case for advanced data analytics technologies and the data protection risks that these technologies raise, as regulators increasingly turn to issue detailed guidance with a view to drawing brighter lines for businesses and research organisations to navigate.

Biometric data is playing an increasingly prominent role in combatting cyber security risks

A right to be forgotten in APAC?

The right to request erasure of personal data and removal of links from search engines, now recognised under European law, has been coined the "right to be forgotten". There are some signs of APAC following suit, although potentially with different policy objectives in mind.

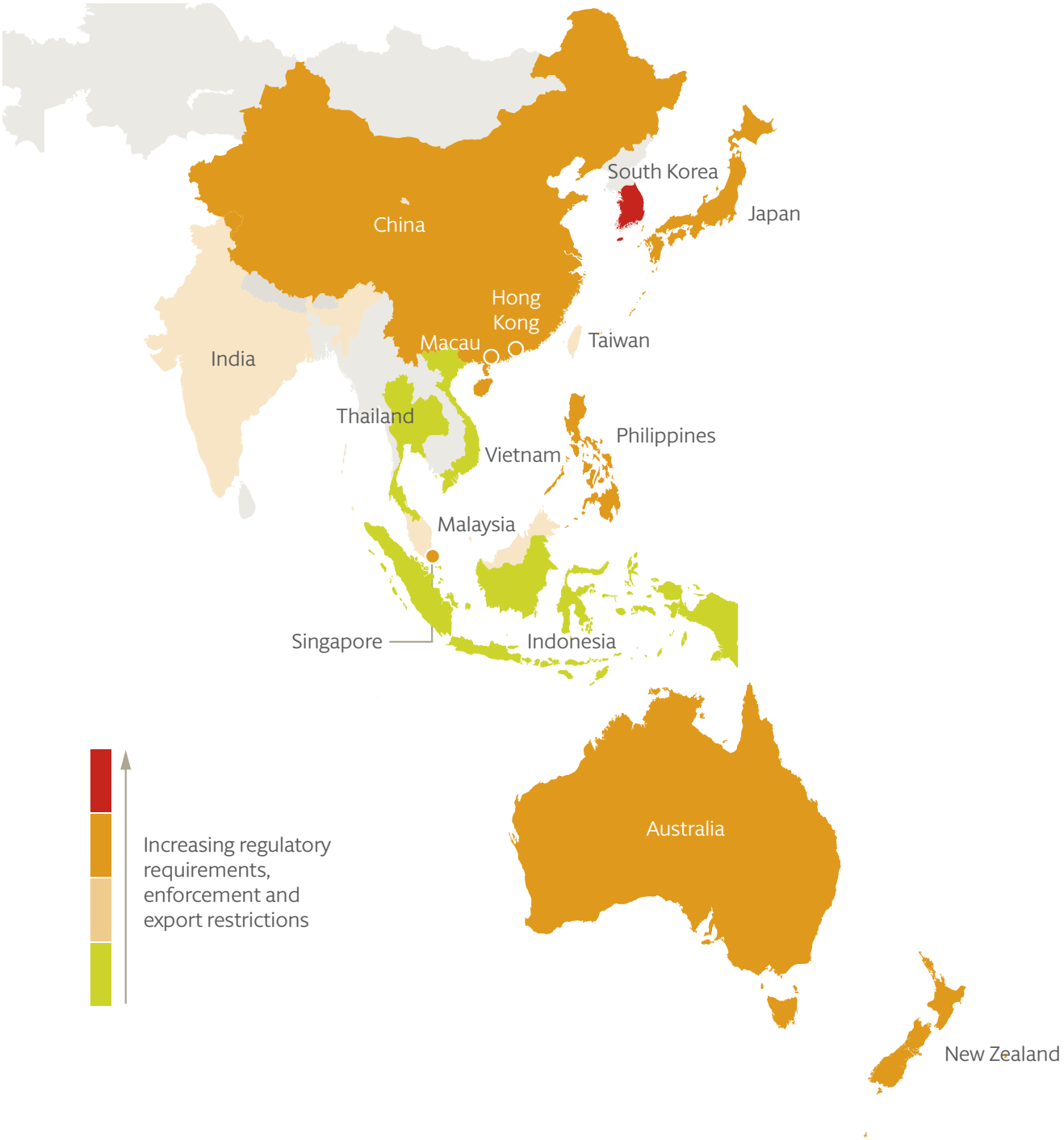
In March 2016, a Korean Communications Commission task force published draft guidelines which propose to give individuals the right to request that online posts and photographs concerning them be removed. Similar rights were also proposed for family members on behalf of a deceased individual. The proposals are yet to be formally implemented.

In Japan, a court recognised the right to be forgotten in a decision handed down in December 2015. The court ordered a search engine to hide news reports about a man convicted of child sex offences, taking the view that individuals should have the right to rehabilitate and have their private lives respected.

Some commentators have expressed concerns that the "right to be forgotten" may be co-opted by governments seeking to exercise greater control over the media. 2016 amendments to Indonesia's Electronic Information and Transactions Law, for example, allow citizens to petition for the removal of online materials. There are concerns that these rights may be abused for political purposes.

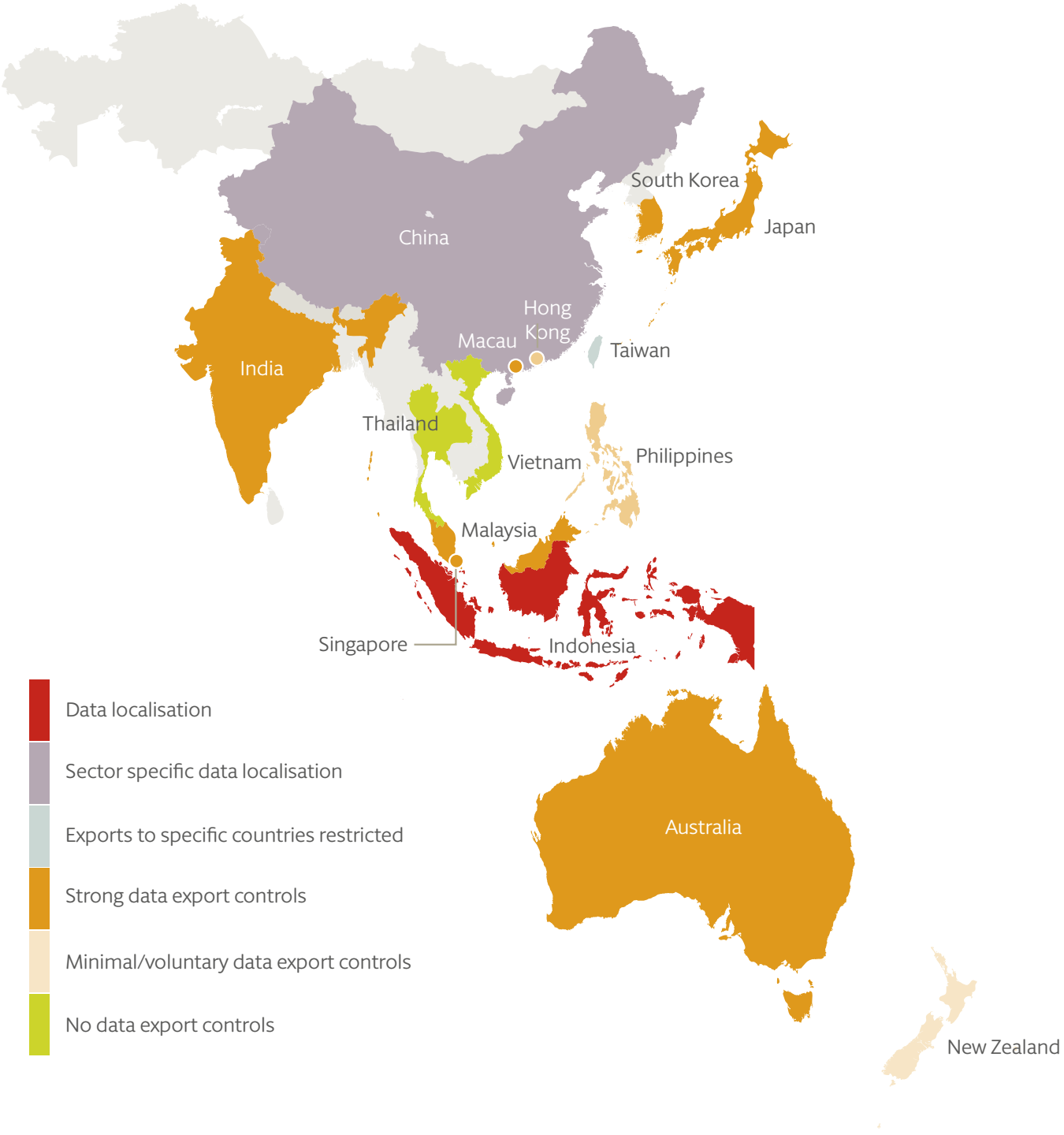
Asia-Pacific data protection regulatory heat map

Our Asia-Pacific Data Protection Regulatory Heat Map is a graphic representation of the relative stringency of the various data protection regulatory regimes across the region. The map below compares the various regimes in Asia-Pacific by grading jurisdictions against four criteria: 1) data management requirements; 2) data export controls; 3) direct marketing regulation; and 4) the aggressiveness of the enforcement environment. More challenging jurisdictions are represented as red, with less challenging ones appearing as green.



Asia-Pacific data export controls

The map below is a graphic representation of the relative degree of regulation of cross-border data transfers across the Asia-Pacific region, with the colour applied to a jurisdiction representing the degree of cross-border restriction in accordance with the legend below.



Individual country spotlights

China

China has witnessed rapid developments in data protection regulation in recent years, although it still lacks a comprehensive cross-sector data protection law and instead relies on a combination of sector-specific laws, consumer protection laws and cyber security laws to regulate data handling practices. Abuses of privacy remain stubbornly widespread in China's massive and increasingly wired economy – a problem which the government is seeking to tackle through enhanced regulation and more stringent enforcement efforts.

Whereas data protection law came to the fore in China through telecommunications, internet and consumer protection regulation in the first half of this decade, the second half of the decade has seen a shift towards national security and cyber security as being the primary policy drivers. Following passage of the National Security Law and the Counter-Terrorism Law in 2015, the controversial Cyber Security Law was passed on 7 November 2016, forming the third 'pillar' of China's complex security regime. These laws are directed at a much wider range of issues than data protection, but at the same time introduce elements of data localisation and technology regulation that will have a significant impact on data collection and processing practices.

The new laws have been met with heavy criticism from multi-national businesses. Technology companies have expressed concerns that the requirement for businesses in China to adopt "secure and controllable" technologies could exclude foreign products from the market. Companies across a range of sectors fear that the policy direction could force them to establish separate operating platforms in China making use of local technology if foreign technology is incapable of achieving certification.

Critics have also stressed that the laws could lead to more pervasive cyber surveillance and enhanced online censorship, by requiring network operators to store internet logs for at least 6 months, block the dissemination of illegal content, and provide "technical support and assistance" to the authorities in national security and criminal investigations. Much will depend, however, on the content of the implementing

regulations to be issued by the Cyberspace Administration of China ("**CAC**"). The CAC issued a draft outline of its *Measures for Security Reviews of Network Products and Services* for public comment on 4 February 2017. The draft suggests that a high-level interdepartmental commission could be appointed to screen internet services and hardware being used in China, but gives precious little insight as to what the screening criteria will be.

Given the growing cyber threat globally, the Chinese move towards more rigorous cyber security regulation is, in very rough terms, in line with international trends. However, the specific approach to regulation being taken in China is a clear outlier, primarily for the use of broad and often imprecise terminology and also for the invasive and potentially discriminatory nature of the regulations.

In addition to enhanced cyber security regulation, the State Administration of Industry and Commerce's *Interim Measures for the Administration of Internet Advertising* came into effect on 1 September 2016. The new regulation sets out rules for online advertisement publishers and details on investigation measures and penalties for breaches.

Hong Kong

Data privacy regulation has a relatively long history in Hong Kong, with the PDPO dating back to 1995. After years of relatively lax enforcement, Hong Kong has stepped to the fore as a policy-making leader on data protection issues in the Asia-Pacific region, with 2016 continuing the recent towards the application of the PDPO's offence provisions.

The Hong Kong PCDP's enforcement statistics have tended to show a year-on-year escalation of complaints and enforcement action in recent years. However the latest figures show that the number of complaints could be starting to stabilise, though still remaining relatively high. During 2016, the PCPD received 1,838 complaints, which represented a 7% decrease from 2015.

Hong Kong saw several widely publicised convictions under its direct marketing offences in 2016, including one case in which an 80-hour Community Service Order was given, marking the first direct marketing conviction in which a non-financial penalty has been ordered. Though jail sentences have not yet been given for direct marketing breaches, these remain a very real possibility.

It is notable that the PCPD received 89 data breach notifications in 2016, despite the fact that Hong Kong's data breach notification regime remains a voluntary one, perhaps indicating the emergence of a more transparent culture in terms of data protection, or perhaps indicating that there simply are more data breaches taking place.

The data export restrictions set out in the PDPO are still not in force, meaning there are currently no legal restrictions on transferring personal data outside Hong Kong. While there are signs that the PCPD's office favours bringing the measure into force (see for example, the PCPD's publication of *Guidance on Personal Data Protection in Cross-border Data Transfer* in December 2014), a legislative amendment to the PDPO would be required in order to achieve this and we do not expect this will happen during the course of 2017.

The PCPD has announced that it will carry out a study of the European GDPR in 2017, the results of which will likely influence any legislative reform process.

Cyber security regulation has also become a feature of regulatory considerations in Hong Kong. In May 2016, Hong Kong's banking regulator launched a Cyber Fortification Initiative that will see institutions benchmarked against new industry standards and oblige them to share information about cyber incidents with each another. The initiative also promises to see the regulator administer cyber readiness simulation tests that will be based upon real time threat intelligence.

The HKMA is also exploring the possibility of using blockchain technology to enhance cyber security, since it provides a means of storing and sharing transaction data without revealing the data to a centralised body or any third party. The Hong Kong Monetary Authority commissioned a research project on blockchain (or "distributed ledger technology") during the course of 2016 to explore the potential applications and feasibility of adopting this technology in the financial sector. In the Whitepaper prepared by the Applied Science and Technology Institute (the government body commissioned for the project) and published in November 2016, data protection is identified as one of the key issues to be resolved if this technology is to be adopted by banks.

Japan

Japan's Act on the Protection of Personal Information ("**APPI**") dates back to 2003 and so stands as one of Asia's oldest laws in this area. In the wake of a series of high profile data security breaches and revelations of unlawful sales of personal data in Japan, the Japanese government passed extensive reforms to the APPI in September 2015:

The main changes include:

- the appointment of an independent, dedicated data protection regulatory authority;
- the expansion of the definition of "personal data" to include biometric data;
- the introduction of a concept of "special care-required personal information" (i.e. the concept of "sensitive" personal data) that will be subject to enhanced protections; and
- the introduction of restrictions on cross-border transfers of personal data, which will now require: (i) data subject consent; (ii) export to a jurisdiction having the benefit of an adequacy finding; or (iii) satisfaction of other criteria to be specified by the new regulatory authority.

The amended APPI will become fully effective in May 2017. There is no grace period for implementation, and the Personal Information Protection Commission has encouraged businesses to use the period leading up to implementation to prepare themselves for compliance.

It will be interesting to see how data protection issues in Japan will influence Japan's strategy for being the world's "Robotic Superpower". The government's latest artificial intelligence policies incorporate a number of related principles such as transparency, security, ethics and privacy.

Singapore

Singapore implemented its Personal Data Protection Act ("**PDPA**") in 2014. Since then, Singapore's Personal Data Protection Commission has been active in publishing a significant volume of explanatory guidance for businesses and consumers alike.

The PDPA has some of the stiffest penalties for data protection offences in the region, with fines of up to S$1 million (USD800,000), and while fines of this magnitude have not yet been imposed, 2016 marked just the start of the Commission's enforcement efforts. The Commission published the findings of 22 enforcement cases during the course of 2016, with the highest fine to date being S$50,000 for the failure of a karaoke house to implement adequate security measures, resulting in the disclosure of 317,000 members' personal data.

There are economic motives informing the PDPA, and Singapore has gone so far as to draw an explicit link between the implementation of data protection regulation and its national ambitions to be a leading high tech hub in the region, including in areas such as data analytics. In January 2016, the government announced an intention to merge the Commission's office with the Infocommunications Media Development Authority, Singapore's telecommunications and broadcasting authority. This move may be seen as a subordination of data protection regulation to Singapore's ambitions to be a Smart City and a haven for technology development.

At the same time, the Singapore government is recognising that cyber security threats pose challenges for these national ambitions. The Ministry of Communications and Industry has announced that a new cyber security bill will be tabled in Parliament in 2017, as part of a program to manage cyber security risks. The bill, which is intended to complement the existing Computer Misuse and Cybersecurity Act, is expected to empower state authorities to manage cyber incidents and raise the standards of cyber security providers.

Australia

After a lengthy delay, in early 2017 the Australian parliament passed a bill that requires that the regulator and impacted data subjects be notified of data breaches.

The developments in Australia reflect growing concerns over cyber security, as reflected in the Telstra Cyber Security Report 2014, which reported that nearly one quarter of businesses surveyed had suffered a security incident in the preceding 12 months, and 60% had in the preceding five years.

2016 saw the Australian Attorney-General introduce a senate bill that would criminalise the re-identification of de-identified government personal data.

South Korea

South Korea has firmly established itself as one of the toughest jurisdictions for data protection and privacy compliance in the world. 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.

An amendment to the IT Network Act passed on 22 March 2016 and effective on 23 September 2016 has now made penalties for data protection breaches even more severe. Telecommunications and online service providers could now be liable to pay punitive damages, forfeit profits resulting from the breach, and, where the breach involves a prohibited overseas data transfer, pay a fine of up to 3% of revenue relating to the transfer. The amendment also holds senior officers of a company accountable for breaches, and they could be personally exposed to penalties.

Thailand

On 6 January 2015, the Cabinet of Thailand approved a draft data protection bill. Pressure on the government to ensure passage of the bill was intensified by reports in September 2016 that over 100 customer phone records had been sold by an executive of one of the country's main mobile operators.

The bill is one of a package of proposed new laws forming part of Thailand's Digital Economy and Society policy implementation. The government confirmed in November 2016 that public hearings on the data protection bill would commence, with full enactment said to be expected in early 2017.

One criticism of the bill is its lack of distinction between a data controller and a data processor. Without this separation, any third party collecting, using or disclosing personal data on behalf of a data controller could share the same liability and duties of the controller. This approach to regulation would clearly be discouraging for internet service providers, cloud service providers and other participants in the digital economy who process data on behalf of others.

Malaysia

Malaysia issued its Personal Data Protection Standards dealing with data security, integrity and retention requirements in 2015. Detailed direct marketing guidelines have also been published in draft form, and if implemented these would introduce controls similar to those in Hong Kong, where specific categories of goods and services and cross-marketing partners need to be identified in the direct marketing consents.

On 15 March 2016, the Commissioner issued the Personal Data Protection (Compounding of Offences) Regulations 2016, which define a number of offences as "compoundable". The Commissioner can offer data users the opportunity to pay a fine in respect of compoundable offences, and if payment is not made within a specified period, the data user will be prosecuted for the offence.

The Philippines

The Philippines' first comprehensive data protection law, the Data Privacy Act of 2012 (the "**DPA**"), took effect in September 2012, but it was not until March 2016 that the National Privacy Commission ("**NPC**") (the body responsible for enforcing and monitoring compliance with the DPA) was formed. The NPC's implementing rules and regulations (the "**IRRs**") came into effect in September 2016, giving specific meaning to the general requirements of the DPA.

It is fair to say that the IRRs represent a striking move forward for Asia-Pacific data protection laws. Some of the key features of the IRRs are:

- Consent, accompanied by data subject disclosures, is required for any private sector data sharing, and a form of data sharing agreement must be entered into with any transferee. These agreements are subject to review by the NPC;
- The IRRs require that organisations appoint a data protection officer or other person accountable for ensuring the protection of data privacy and security; and
- When data processing is outsourced, the personal information controller must use "contractual or other reasonable means" to ensure that proper safeguards are in place to protect personal data. The IRRs specify the types of clauses that are required in outsourcing contracts with personal information processors.

The most overt borrowings from the GDPR found in the IRRs are a 72 hour data breach notification requirement, data subjects' right to be informed of profiling and automated decision-making and a right to data portability.

With the implementation of the IRRs, the Philippines has now set one of the highest bars for data protection compliance in the Asia-Pacific region.

Indonesia

Indonesia has yet to adopt a comprehensive data protection law, but amendments to Government Regulation No. 82 of 2012 regarding the Provision of Systems and Electronic Transactions have introduced a measure of data protection regulation to the country, multi-nationals paying particular attention to the data localisation measures that will come into effect during 2017. Regulation 82 threatens the continued use of regional operating platforms that have, to date, tended to host Indonesian data processing operations in jurisdictions such as Singapore, where a more advanced data centre and telecommunications sector can be found.

With a population of over a quarter billion and one of the highest economic growth rates globally, Indonesia is an increasingly important target for multi-national businesses. Foreign access to this market is being challenged by an increasingly restrictive regulatory environment for data and technology.

Data Protection and Cyber Security regulation in Asia: A guide to making (and keeping) your business compliant

The tightening of Asia's data protection regulatory environment and the emergence of cyber security regulation comes at the same time as personal data has developed into an increasingly valuable business asset. It also comes as regional businesses seek to turn more to outsource data processing and transfer data across borders with a view to improving operational efficiency and leverage economies of scale.

An effective data protection and cyber security compliance program begins with a comprehensive look at the personal data being used within the business and then proceeds to map applicable regulatory requirements to this processing.

At a high level, the steps towards developing an effective compliance plan are as follows:

- What personal data does the business hold and use, how was it obtained and for what purposes is it being processed?
- Is the data being transferred to any other group companies or to unrelated third parties for any purpose? If so, into which jurisdictions is the data being sent?
- What future plans does the business have for processing data, in particular having regard to new business lines, new jurisdictions, new technologies, new business models and other potential new avenues to monetising data?
- What data protection and cyber security regulatory regimes apply to the organisation's personal data holdings, bearing in mind both the location in or from which the data was collected and the location or locations where it is being processed?
- Are the business's existing policies and procedures compliant? Where are the gaps and what are the practical options for achieving compliance?

Each of these steps is explored in more detail below.

A Personal Data Audit

The first step towards developing an effective compliance plan is to understand what personal data the business uses.

Customer Data

Customer databases are one of the more obvious holdings of personal data, particularly for consumer facing businesses. The practical issue for identifying the full extent of an organisation's customer data holdings is that databases are not always clearly marked out as such, particularly now in the era of cloud computing and widespread use of mobile devices.

Engaging with sales, marketing, business development and technology teams is often the key to successfully auditing customer data holdings. Care needs to be taken to understand the specific technologies being used by the business and whether data is being collected or extracted online or through mobile handsets, whether directly or through third party service providers.

Data that has been anonymised or aggregated for profiling or analytics purposes may not, strictly speaking, be "personal data", but this data should nevertheless be included as part of the audit. Data protection laws generally look at data from an entity-wide or group-wide perspective, meaning that de-personalised data sets that can be linked to identities will not avoid compliance requirements. With the proliferation of social media and online public data sources, the risk of "re-identifying" individuals from anonymised or aggregated datasets has never been higher. Assessing data protection compliance will involve assessing the procedures for creating and maintaining the de-personalisation of these datasets.

Employee Data

As Asia region businesses grow in scale and geographic reach, we see a trend towards increased consolidation of human resources databases and increased use of external service providers to administer HR processes and procedures. This development has been running up against stricter data privacy laws in general and, in particular, the imposition of data export controls in a number of jurisdictions – hence the need to be more vigilant and ensure that data holdings have been properly identified and audited.

An important aspect of employee data is that it almost invariably includes "sensitive personal data" such as information about health and ethnic background. Sensitive personal data is subject to enhanced privacy protection under a number of the region's laws.

Other Personal Data

Many organisations will also hold personal data about individuals who are not their direct customers, such as shareholders, directors and company officers of corporate customers and suppliers, as well as family members and other individuals who are connected to customers or employees. In the context of social media and cloud services businesses, there are often holdings of user contacts or "refer a friend" data that has not been directly obtained from the business's customers. This personal data will nevertheless be subject to regulation.

It can very be important to identify data holdings of individuals of this type, given that the business may not have any direct contractual relationship with the individuals concerned, and so find it more challenging to obtain data subject consents and otherwise be sure that compliance requirements have been met.

Assessing the Means of Collection and the Purposes for Processing

Once the various personal data holdings within an organisation have been identified, the next task will be to identify how the data was obtained and the purposes for which each group of data is being processed. This will likely again be a matter of engaging with appropriate individuals within functions such as sales and marketing, HR, technology and operations who understand the business processes involved.

As noted above, the pace of technology deployment within an organisation may well run ahead of the legal and compliance teams' immediate understanding of what sort of collection and processing is taking place across the business. Data analytics, for example, is an increasingly valuable business tool across a wide range of industries. It is too often the case that these technologies have been deployed without proper compliance checks.

Another area that can raise difficulties is the use of publicly sourced data. In some jurisdictions, such as Singapore, privacy laws do not in general apply to publicly sourced data. In others such as Hong Kong, regulators have made clear that publicly available data may only be used in compliance with general data privacy principles.

We would recommend a holistic approach to analysing purposes be applied, with references to appropriately stress-tested checklists. New purposes for processing data may develop unexpectedly. For example, it may be a rare occasion that a business has a need to consolidate data on the servers of an e-discovery service provider as part of multi-jurisdictional litigation, but it is much better to be prepared for such an eventuality if it is a practical possibility. Likewise, if personal data may be subject to demands by foreign regulators, care will need to be taken to understand this risk in order to factor in appropriate data subject consents and policies and procedures around data handling if the business is in the position to make the disclosure.

Mapping Data Transfers

A related task in the fact gathering process is to understand where personal data is being transferred to from its points of collection, both in terms of transfers to entities within the wider business group and transfers to unrelated third parties. The geographic transit of personal data will also be important given the proliferation of data export controls across the Asia-Pacific region.

Data transfers can broadly be of two types – (i) transfers to affiliated companies and business partners who collaborate in determining the purposes for data processing or have the discretion to pursue different purposes of processing data (i.e., "controller to controller" transfer scenarios); and (ii) "controller to processor" scenarios in which the transferee simply processes the data in accordance with the transferor's instructions with no discretion to pursue new purposes for processing.

Both types of transfer will be relevant, although the compliance requirements will differ significantly in each case.

Cross-border transfers of personal data raise an additional layer of complexity in many jurisdictions in the Asia-Pacific region which now have data export controls.

Data Maintenance and Retention

Databases constantly evolve through their use, and so an understanding of how a database is updated, corrected and augmented is key to an effective regulatory analysis.

As the Asia-Pacific region's data protection laws are all consent-based, a key consideration is what procedures are in place to ensure that requests from data subjects that processing cease are appropriately addressed.

Similarly, many of the regimes across the region have express data subject access and correction rights. Businesses will be expected to have policies and procedures in place to manage these requests.

As a general rule, the region's laws also oblige businesses to cease processing personal data once the purposes for which it has been collected have been exhausted. There are few prescriptive data retention periods under general purpose data protection laws, but businesses will need to undertake an appropriate analysis to determine how long data should be kept. Likewise, it will be important to evaluate approaches to securely erasing personal data once the purposes for having it have been fulfilled.

An Eye to the Future

While much of the personal data audit process is a forensic one aimed at generating a clear snapshot of the current state of data process across a business organisation, a well-executed review will also consider planned extensions of the purposes for processing of data and changes to business operations, such as plans to consolidate databases and deploy new technologies, such as the introduction of remote access by employees to cloud based services, the "bring your own device" policies and the introduction of behavioural profiling technology to company web sites and apps.

Assessing Regulatory Requirements

Once the organisation's personal data holdings and processing have been understood as a factual matter to a sufficient level of granularity, an analysis against applicable data protection and cyber security regimes can be undertaken.

Leveraging what's already there

The regulatory analysis will not necessarily be a matter of re-inventing the wheel, in particular for European-based multinationals who have invested years of effort in constructing policies and procedures that meet European standards. European standards often (but do not always) meet or exceed national requirements across many jurisdictions in the Asia-Pacific region, and so it is often efficient to leverage global or regional policies from elsewhere in the organisation if they are transportable having regard to the nature of the business and the data processing taking place. As Asia's data protection and cyber security regimes proliferate and develop, however, there are more and more local distinctions that will need to be taken into account.

A regional approach to compliance

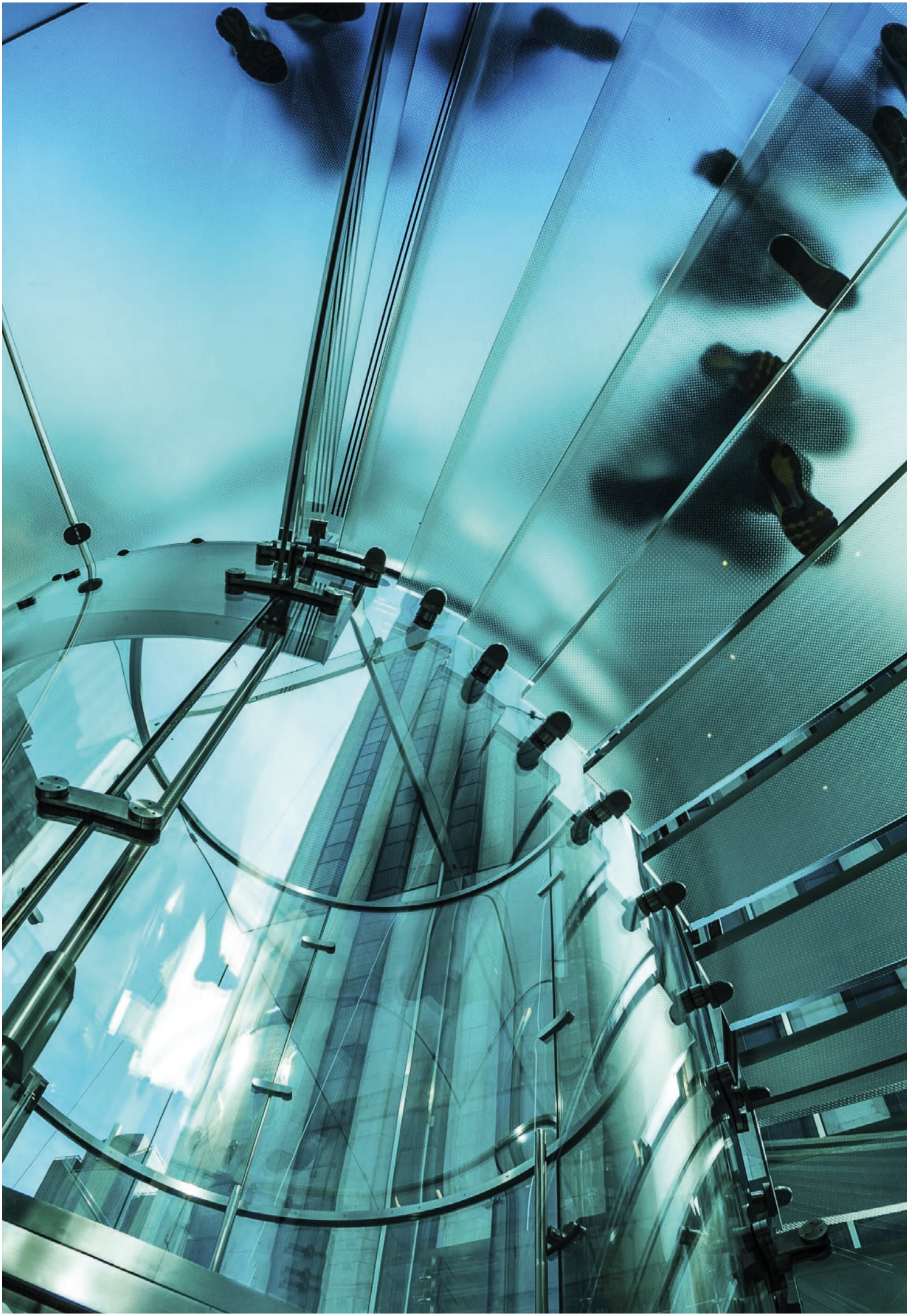
Irrespective of the starting point a business finds itself in, we generally counsel clients with regional footprints to take a regional view of Asia-Pacific's data protection and cyber security compliance requirements. Although there are important differences at every turn, there is a degree of general conformity, at least, around the principles set out in the APEC Privacy Framework.

"Levelling up" to APEC standards in jurisdictions without data protection laws often makes good business sense, given the obvious trend towards comprehensive regulation. We expect, for example, new laws to emerge in Indonesia and Vietnam in the coming years, and it is a virtual certainty that the new national laws there will take approaches to regulation that are similar to that taken by their neighbours.

There is also, of course, good business sense in having a strong brand for data privacy wherever the business may be. In the area of electronic and mobile commerce and payments, borderless data transfers, cloud computing and remote access to databases, a global or regional approach to managing data security and data privacy is becoming increasingly a business necessity.

While Asia has a number of jurisdictions that are yet to implement legislation tracking the requirements of the APEC Privacy Framework, Asia also has a number of jurisdictions sitting at the other end of the compliance spectrum. South Korea, for example, has marked itself out as being one of the world's most challenging jurisdictions for data privacy compliance. There are other challenges across the region, such as Hong Kong's direct marketing controls and Indonesia's data export requirements. China raises a unique overlay of difficult laws and regulations that pose compliance challenges on a number of fronts. The "new normal" for Asia-Pacific data privacy compliance is setting an ever increasing bar for compliance.

Cyber security regulation is steadily introducing new variables to approaches to data management in the Asia-Pacific region. China's move to require that businesses use "secure and controllable" technology is beginning to drive businesses in regulated sectors in particular to localise technology and data to the mainland. Indonesia's Regulation 82, due for implementation in 2017, is forcing the same considerations there.



Typical Compliance Considerations

The typical range of compliance measures that most businesses will need to turn to will include:

- **Personal information collection statements (PICS)** prepared either as consents or notifications, as applicable, incorporated into customer terms and conditions, privacy policies for web sites and apps, employment terms and conditions and other interfaces with data subjects.
- **Data processing policies and procedures** for internal stakeholders to understand and administer, including policies and procedures dealing with:
  - Data collection and capture, including policies concerning the use of appropriate PICS and the mechanics of collecting consents and the usage of third party data sources;
  - Direct marketing, including alignment of PICS with direct marketing activities, implementation of "opt in"/"opt out" mechanisms, prior consultation with applicable "Do Not Call" registries and compliance with direct marketing formalities, such as consumer response channels and any required "ADV" indicators;
  - Human resources management, including policies dealing with job applicant data, retention of and access to employee files, notification and consent to data privacy policies, employee monitoring, management of sensitive employee data and the use of external vendors for functions such as payroll and counselling;
  - Data analytics, including policies specifying the types of profiling data that may be used, anonymisation/aggregation principles and policies around "enhancing" datasets through the use of publicly available data or third party datasets;
  - Data commercialisation, which looks more broadly for the potential use of the organisation's data to collaborate with other businesses in marketing initiatives and consumer profiling;
  - Security, including technical standards applicable to various types of internal and external data processing, data access and permissioning, the use of encryption technologies and policies around the use of data in cloud services and other technologies;
  - Business continuity and disaster recovery, including data back-up procedures, the use of redundant storage and contingency planning;
  - Data subject access, including procedures for assessing and verifying requests, considering the legal implications of requests and managing costs of responding to requests;
  - Complaints handling, including complaints from customers, employees and other affected individuals;
  - Data quality management, including procedures for updating and correcting databases and determining if data is to be erased;
  - Data processing and outsourcing, including vendor due diligence policies and standard contract clauses and templates for onshore and offshore processing;
  - Data retention, including policies for determining how long data of various types are to be retained and how it is to be securely destroyed;
  - Cyber threat assessments and incident response planning, including programs to identify and review cyber threats across the organisation, allocation of responsibilities for escalation of and response to incidents;
  - Data breach management, including policies for escalating, containing and remediating data breaches and evaluating the need for regulatory or data subject notifications, as well as procedures for assessing any need for change to policies and procedures following the occurrence of a breach; and
  - Privacy impact assessment, which includes a general framework for the organisation to assess privacy impacts due to proposals for organisational, technological or policy change.

Management oversight and review

Developing effective data protection and cyber security risk management policies and programs will involve engagement with the right stakeholders across the organisation and creating an effective governance regime for approving, overseeing, implementing and reviewing the various policies. The appointment of official roles such as a Data Protection Officer is becoming more common as best practice in the region, even in jurisdictions where the designation is not required by law.

Regulators in the region are becoming increasingly conscious of the degree to which data protection and cyber security policies have been prepared under senior management and board direction. Input from such high levels lends credibility to the compliance effort. Effective implementation of data privacy policies will need to consider appropriate channels for reinforcement of new policies following their publication. Training of individuals within the organisation will be necessary in order to lend context and emphasise the importance of compliance to the business. The policies will need to be seen to have been acted upon in order to be evidence of due compliance, and so enforcement procedures will be critical. Policy breaches will need to be examined after the fact with a view to understanding whether or not any organisational change is needed in response.

In order to be effective, an organisation's data privacy policies will need to be under regular review, reflecting changes in law and regulation, changes in the data being collected and used and changes in technologies and operating procedures. The benefit of experience must also be brought to bear.

Our Asia-Pacific practice

An international perspective

At Hogan Lovells we bring an international perspective to advising clients on Asia's data protection and cyber security laws and the ongoing development of policy across the region. Our Asia Pacific team includes practitioners who practised data privacy law in Europe, and so bring a depth of experience to interpreting Asia-Pacific laws that have a common origin in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. At the same time, our experts are on the ground in the region and rooted in the local law and language, sensitive to the important emerging local nuances.

Integrated support

Our Asia team is closely integrated with our international team of data protection and cyber security practitioners, and so benefits heavily from a wider team of market-leading lawyers who are at the forefront of policy developments in Europe and the United States, advising clients on the most critical mandates on a world-wide basis.

Where Hogan Lovells does not have offices in the Asia-Pacific region, we have strong working relationships with local counsel experts. These relationships have developed over the course of the effective lifetime of these emerging laws, supporting the delivery of a uniformly consistent and high quality work product and practical solutions for business.

Our Asia data protection and cyber security team is also closely integrated with other relevant specialists, in particular lawyers engaged in commercial arrangements concerning data commercialisation and processing and employment law specialists. Our seamlessness on this front means that we bring a very practical, solutions-based approach to counselling that is well informed by market practice.

Key points

Our advice covers all aspects of data protection and cyber security compliance, including:

- Conducting data protection and cyber security compliance audits and developing policies, including integrating Asia policies with existing international policies;
- Helping clients structure and allocate risk in relation to cross-border data transfers, including as part of outsourcing, shared services and cloud arrangements;
- Advising on the acquisition of personal data as an increasingly important part of merger and acquisition and joint venture activity;
- Advising on data protection issues arising from online data capture, whether as part of electronic and mobile commerce, behavioural profiling or otherwise;
- Advising on commercial arrangements, such as marketing, distribution and sponsorship agreements, where securing rights to use personal data is a key business objective;
- Advising on cyber-security regulation and cyber-readiness planning;
- Advising on data breach notification requirements when data is hacked or lost;
- Advising on data subject access requests;
- Defending companies against enforcement actions; and
- Bringing to bear the knowledge and experience of our extensive and market-leading data protection and cyber security management team across the world in finding solutions that work in Asia based on lessons learnt elsewhere.

Key contacts in Asia

Hong Kong

Mark Parsons
Partner
mark.parsons@hoganlovells.com
T +852 2840 5033

Eugene Low
Partner
eugene.low@hoganlovells.com
T +852 2840 5907

Louise Crawford
Registered Foreign Lawyer
louise.crawford@hoganlovells.com
T +852 2840 5014

Beijing

Jun Wei
Partner
jun.wei@hoganlovells.com
T +86 10 6582 9501

Roy Zou
Partner
roy.zou@hoganlovells.com
T +86 10 6582 9488

Japan

Hiroto Imai
Partner
hiroto.imai@hoganlovells.com
T +81 3 5157 8166

Shanghai

Philip Cheng
Partner
philip.cheng@hoganlovells.com
T +86 21 6122 3816

Andrew McGinty
Partner
andrew.mcginty@hoganlovells.com
T +86 21 6122 3866

Singapore

Stephanie Keen
Partner
stephanie.keen@hoganlovells.com
T +65 6302 2553

Vietnam

Jeff Olson
Partner
jeff.olson@hoganlovells.com
T +84 8 3825 6370

Our global Privacy and Information Management practice

Realizing the true value of data

Finding the right balance between the most fruitful use of data and the protection of privacy is one of the greatest challenges of our time. Personal information is an extremely valuable asset and its responsible exploitation is crucial for the world's prosperity. For that reason, our approach is to look at privacy compliance and information governance as part of our clients' strategic vision for success.

Embracing privacy, data protection, and cyber security can be crucial in order to gain competitive advantage, because it will promote employee and customer loyalty, encourage consistency and efficiency, and facilitate international expansion. In addition, we believe that privacy is not only compatible with innovation, but can make a valuable contribution to it.

With its depth of knowledge and global presence, Hogan Lovells' Privacy and Information Management team is uniquely placed to help clients realize this potential. We have extensive experience of assisting clients with multi-jurisdictional projects and understand the complexities involved in dealing with laws and regulators across the world.

What we offer

- A true specialist practice focused on privacy, cyber security, data protection, and information management
- Thought leadership and close involvement in the development and interpretation of the law
- Seamless global coverage through our well established and continuously developing team
- Advice which goes beyond achieving compliance and adds value to the information held by organizations
- A one stop shop for all of your data privacy needs around the globe.

Our focus and experience

The Hogan Lovells Privacy and Information Management practice spans the globe and all aspects of privacy, data protection, cyber security, and information management.

- No other team in the world has our track record of BCR approvals. We have advised on and successfully secured approvals of BCRs for nine applicant companies and are currently working on several BCR projects.
- We have worked with numerous multi-nationals on other data transfer solutions, including adoption of model clauses, intra-group agreements and Safe Harbor.
- We have advised numerous global companies with respect to complying with their notification obligations across the EU.
- We have drafted and advised on many global data processing contractual arrangements to ensure practical and effective compliance with security related obligations.
- We have liaised with policy makers throughout the world and contributed to the legislative process in the EU and other jurisdictions.
- We have assisted clients in devising and implementing regulator cooperation strategies, including liaising closely with EU data protection authorities.
- We have surveyed in detail the laws and regulations impacting employee monitoring practices in over 60 countries, including important markets in Europe, the Americas, Asia, the Middle East and Africa.
- We advised a number of global companies on data privacy questions arising from their migration of HR and customer data of their European subsidiaries to cloud service providers.
- We have advised many multi-nationals on localising website privacy policies.
- We have assisted leading global companies to adopt and implement a pan-European strategy in respect of the EU cookie consent requirements for their website and mobile application offerings.
- We provided strategic advice to a number of clients on data breach notification requirements throughout the world.

– We have advised on complex matters ranging from the use of biometrics to the collection of mobile device data, including making submissions to multiple data protection authorities to facilitate the

How we can help

We have had a team specializing in Privacy and Information Management for over 25 years. Today Hogan Lovells has one of the largest and most experienced Privacy and Information Management practices in the world, spanning the United States, Europe, and Asia. We assist clients with all of their compliance and risk management challenges, drafting policies and providing advice on legal issues, risk management strategies, and strategic governance. With our global reach, we are able to provide a 24-hour global privacy hotline to respond to data emergencies. We play an important role in the development of public policy regarding the future regulation of privacy. Additionally, we provide the latest privacy and data protection legal developments and trends to our clients via our blog,

Chronicle of Data Protection

(http://www.hldataprotection.com)

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com