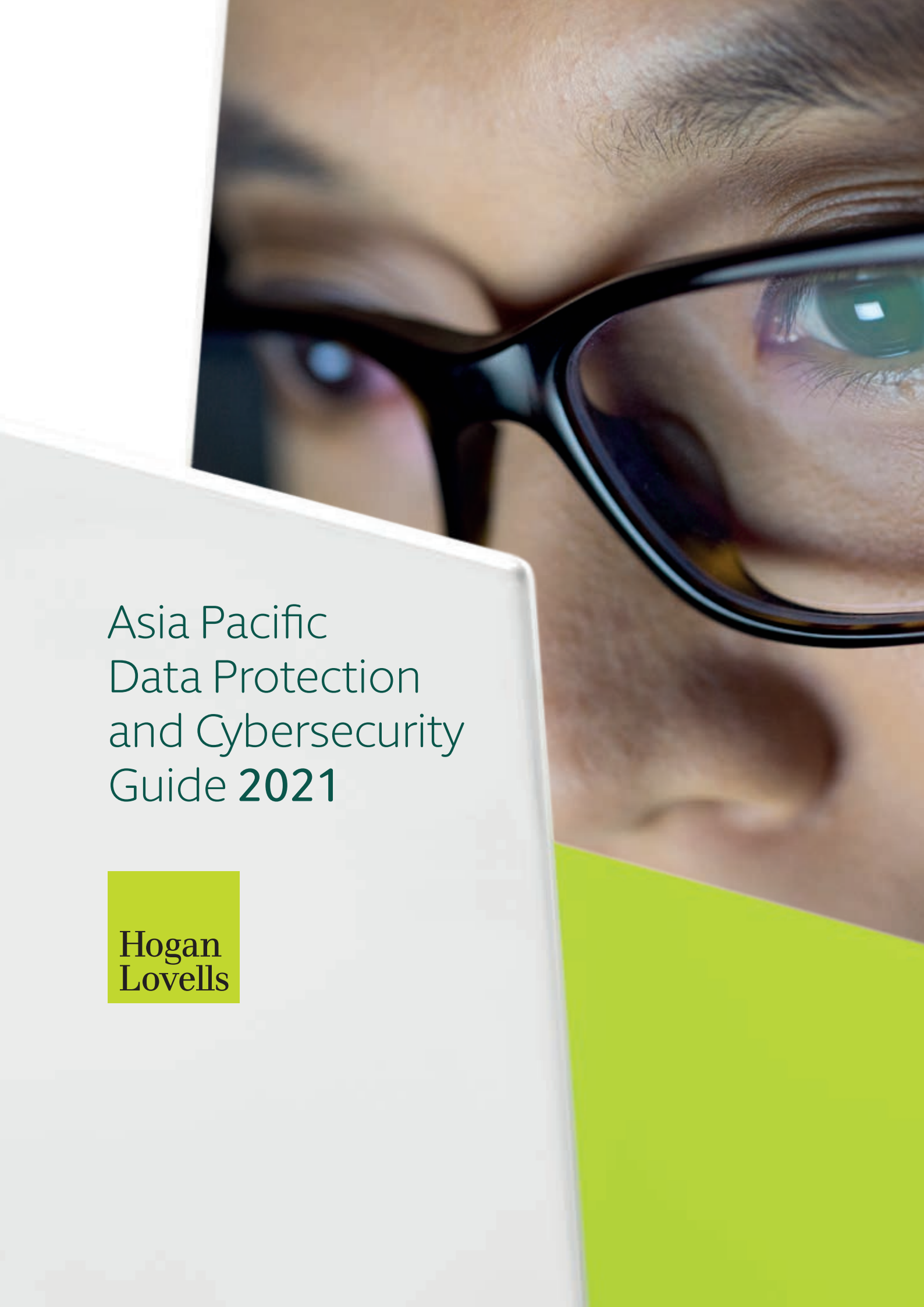


Asia Pacific Data Protection and Cybersecurity Guide **2021**

Hogan Lovells

Contents

Asia-Pacific data protection and cybersecurity regulation

2020 in review and looking ahead to 2021

The unprecedented challenges of the COVID-19 pandemic are still with us, not only in terms of the grim toll the virus has taken on individuals and families, but also in terms of wider implications for how people and societies live and interact. Data protection regulation emerged as a key regulatory pressure point during the pandemic in respect of a host of issues, from the collection of medical, biometric and contact tracing data, through to data protection and cybersecurity aspects of remote working as workers increasingly stayed home.

The data protection landscape in the Asia-Pacific region ("**APAC**") was already undergoing significant transformation in the run-up to the pandemic. Speaking in very general terms, the movement has been towards closer alignment with the European Union's General Data Protection Regulation ("**GDPR**"). The move towards this international "gold standard" has been seen as timely, as APAC economies continue to grow and become more digital. That said, the evolution of each national law in APAC necessarily reflects the specific policy aims of the lawmakers taking legislative reforms forward, with an eye to matters such as economic development goals, national security and a host of other issues unique to the jurisdiction.

In this context, it is becoming increasingly difficult to distil specific themes for recent developments in APAC and more challenging still to chart a likely course for regional regulatory developments. We would nevertheless point to the following as key developments of note for the region:

The impact of COVID-19

The focus of 2020 was undoubtedly on the impact of the pandemic. In APAC, the approaches taken by governments and authorities to respond to this threat have differed significantly. The pandemic has led to the deployment of various measures to contain the spread of the virus, such as track-and-trace technologies and, in some contexts, compulsory testing. Public support (and official enthusiasm) for these measures differed significantly from jurisdiction to jurisdiction, with public trust in government handling of personal data being a key consideration in this regard.

The pandemic has also significantly changed the way in which organizations work, forcing businesses to adapt working arrangements for employees unable to travel to their usual place of work. The pandemic has accelerated moves away from manual, paper-driven workflows and, at the same time, increased cybersecurity risks for businesses. Similarly, in the consumer realm, retailers and brands rushed to enhance their e-commerce channels to be better placed to make sales to consumers who were staying away from shops and malls. There is no question that part of the value proposition for digital interactions with consumers is in making profitable use of personal data, as retailers and brands struggled to maintain sales in recessionary consumer economies. This too has important data protection and cybersecurity implications.

The impact of the pandemic on data protection policy has not yet been fully understood, as policymakers across APAC look ahead to develop and implement measures to curb the spread of the virus and set the stage to prevent future pandemics. Many of these measures will involve the collection and handling of personal data, drawing a much sharper focus on the balance between privacy and public health considerations than we have seen since the wider adoption of comprehensive data protection laws began in the past five to ten years.

Post-pandemic, data protection regulation in the APAC region is a more complex and more urgent affair.

China's move towards comprehensive data protection regulation

The cornerstone for China's data protection and cybersecurity regulation is the Cyber Security Law which took effect in June 2017 ("**CSL**"). The CSL is framed in general terms with much of the detail left to be specified in implementing regulations. A complex interaction between overlapping laws and non-binding (but influential) standards has emerged in the months since. In the course of 2020, China amended the Information Security Technology – Personal Information Security Specification which is sometimes referred to as China's version of the GDPR, which is non-binding but has significant influence on official interpretations of the very general provisions found in the CSL. China also released two drafts of important new data protection laws, namely, the Data Security Law and the Personal Information Protection Law. These drafts are under consultation, but if implemented substantially as drafted would represent a significant move towards comprehensive data protection legislation in China. These legislative developments closely track many of the principles found in European data protection model. At the same time, China's efforts towards "cyber sovereignty" are a differentiating factor that casts GDPR innovations such as extra-territorial effect in a different light. As geopolitical tensions continue in 2021, China, like many other countries, is treating data protection and cybersecurity policy as a tool for international trade and national security policy. Also, in line with international developments, China is applying increasing regulatory focus to powerful digital platforms that are a mainstay for e-commerce, digital communications and content in China. Stronger data protection controls are a key feature of these domestic-focused regulatory initiatives.

"Data Protection 2.0" – continued regional advancement of data protection standards

The implementation of GDPR in 2018 continues to influence reforms of existing APAC data protection laws and the content of new laws now being enacted. Australia, New Zealand and Singapore have enacted GDPR-style enhancements to their laws, such as mandatory data breach notification obligations. Thailand's Personal Data Protection Act, which will come fully into effect 1 June 2021, and India's Personal Data Protection Bill 2019, also expected to be implemented in 2021, are examples of APAC jurisdictions lacking comprehensive data protection laws moving straight to regimes which are heavily inspired by GDPR. As noted above, China's latest draft data protection laws, are largely cut from the same cloth. The clear trend is towards the European model, with very significant consequences as data protection laws turn to EU-style extra-territorial effect and revenue-based fines. What is also clear from the implementation of new and amended laws is that the EU model, cast as it is in broad, principle-based terms, leaves significant room for local interpretation (or perhaps even misinterpretation) of GDPR principles. Superficially, there is clearly a harmonization of approach, but specific compliance requirements can vary significantly from jurisdiction to jurisdiction and we expect this to continue to be the case as each jurisdiction applies its own interpretation to broad-based GDPR principles. It is also important to note China's influence as an alternative source of policy inspiration for the region. China's localization measures (still not fully implemented), for example, have inspired Indian lawmakers to consider a provision that would force businesses to localize "critical personal information" notified by the authorities.

Enforcement? – call it a work in progress

2020 was notable for a significant increase in the enforcement of data protection laws in the region, but at the same time the enforcement activity underlined how small the fines for non-compliance are when compared to penalties being awarded under the GDPR. The contrast was most apparent in the summer of 2019 when two international airlines, British Airways and Cathay Pacific, faced separate enforcement action in respect of data security breaches. BA was fined GBP 22 million (reduced from GBP 183 million) by the UK Information Commission, whereas Hong Kong's Privacy Commissioner for Personal Data could only conclude its Cathay Pacific investigation by issuing an enforcement notice – no financial penalty was awarded. The picture is similar across the region, with fines continuing to be relatively low. A study by compliance technology provider Fenergo reported that data protection fines for the APAC region financial institutions totaled just USD 6.9 million in 2020 (compared to USD 5.1 billion in money laundering fines). The movement towards GDPR-style revenue-based fines will certainly change the picture on this front, particularly as the region's economies and public services become increasingly digitalized and there is much greater consumer focus on data protection and cybersecurity concerns.

"2020 was notable for a significant increase in the enforcement of data protection laws in the region, but at the same time the enforcement activity underlined how small the fines for non-compliance are when compared to penalties being awarded under the GDPR."

The impact of COVID-19 on data protection and cybersecurity

In 2020, the development of data protection and cybersecurity laws was largely overshadowed by the immediate challenges of the COVID-19 pandemic. A number of APAC jurisdictions turned to contact tracing technologies, some of which rely on real-time geo-location tracking, while others make use of Bluetooth or Wi-Fi-based geo-fencing technologies. Naturally, the privacy impact of these technologies varies, with some technologies being deployed on a voluntary basis, some collecting location data and others collecting sensitive health data. The urgency of the pandemic response tested positions on the appropriate balance between personal privacy and public health, with different resolutions of that balance in different jurisdictions.

With the risk of infection in the workplace, organizations faced a number of new operational challenges having important data protection implications, ranging from issues around the collection of employee health information through to data protection and cybersecurity risks of remote working. Many APAC data protection authorities issued guidance on topics such as temperature screening, the use of contact tracing technologies, obligations to report to health authorities and the scope of public health exemptions from consent requirements under data protection laws. The voluntariness of some forms of data collection exposed an important intersection with employment law.

Over the course of the year, we expect this organizational and workplace transformation to continue, meaning that organizations must continue to stay apprised of developments and conversations as the privacy implications of these new technologies continue to grow. On a regional level, we anticipate that the regulatory developments will continue to pick up steam, particularly with the various proposed legislative changes across the region in the pipeline.

China's progress towards clarity on its data protection approach

It is now over three years since China implemented the CSL, and yet critical areas of the law remain unspecified. Although progress has been made in specifying general requirements under the law through more detailed implementing measures, a number of key issues remain unresolved. The newly issued drafts of the Data Security Law and the Personal Information Protection Law represent China's first attempt to overlay its complex patchwork of laws dealing with data protection issues with comprehensive law. At present, sector-specific laws and the CSL set out general data protection requirements which are in practice fleshed out by reference to more specific language in a non-binding national standard, the Information Security Technology – Personal Information Security Specification.

China's data protection and cybersecurity landscape is discussed in more detail in the Individual Country Spotlight section, but key impacts to note are as follows:

Data localization

The CSL's provision for data export review or "data localization" continues to weigh heavily on international businesses operating in mainland China. Three years after the introduction of the CSL, the export review process has not yet been elaborated. A further draft of the export review measures was released in June 2019 but was not finalized. It is possible that the CSL's review measure will in part be superseded by the new cross-border transfer rules provided for in the draft Personal Information Protection Law. The draft Personal Information Protection Law would impose data export security assessments to data transferors which either: (i) are operators of critical information infrastructure; or (ii) undertake volumes of data processing that meet materiality thresholds to be set by the Cyberspace Administration of China. Other business operators intending to transfer personal data abroad would only need to engage a third party professional institution to conduct a certification or enter into a written agreement with data recipients which incorporates obligations ensuring the data will

> "More important to the evolution of laws in the APAC region, however, is the fact that there is far greater demand for data protection in the region now."

continue to be processed in accordance with the standards under the Personal Information Protection Law.

Countermeasures against discriminatory treatment

The draft Data Security Law and Personal Information Protection Law both authorize Chinese regulators to adopt countermeasures if foreign governments discriminate against or otherwise restrict Chinese businesses from making investments into or conduct trading activities in data-related sectors. The express incorporation of trade policy measures into Chinese data protection law would introduce an additional element of uncertainty for multi-national businesses doing business in China.

"Data protection 2.0": Continued regional advancement of data protection standards

The GDPR, implemented in the EU in May 2018, continues to generate shockwaves internationally. The immediate impact for businesses headquartered in the APAC region has been the extension of the scope of application of European data protection law from an "establishment" concept limiting the law's application to organizations with "bricks and mortar" operations on the ground in the EU to a broader set of criteria making the GDPR applicable to APAC businesses. The prospect of penalties reaching 4% of worldwide turnover has caught the attention of many APAC-based businesses, and so we see concerted compliance activity with a view to understanding the extent to which the new European requirements apply to businesses headquartered here. In some cases, organizations' operations and interaction with the EU and EU data subjects can be restructured so as to avoid "over-compliance" with EU requirements. In many cases, however, the international scope of business necessitates a GDPR compliance exercise in respect of at least some of the organization's operations.

The impact of the GDPR for APAC is much farther reaching than the compliance requirements for regional businesses with EU touchpoints. Lawmakers and data protection authorities across the region are studying the GDPR with a view to reforming their own regimes to reflect this "version 2.0" upgrade of comprehensive data protection regulation.

More important to the evolution of laws in the APAC region, however, is the fact that there is far greater demand for data protection in the region now, as citizens become increasingly immersed in a new digital reality brought about by widespread use of mobile devices and the emergence of the internet of things. At the same time, governments in the region are moving concertedly towards digital identity programs and more invasive approaches to electronic surveillance. On this view, the apparent "cherry-picking" of GDPR concepts is a reflection of the need for laws that are more protective.

One area where GDPR influence is particularly pronounced – and particularly impactful – is in relation to mandatory data breach notification obligations. One by one, Asia-Pacific jurisdictions have been moving from voluntary to mandatory notification regimes, with Hong Kong, Singapore and India all contemplating following the path of Australia, the Philippines, South Korea and Thailand in introducing mandatory notification laws.

The GDPR's influence is extensively seen in new laws which have recently been implemented or remain under discussion. India's draft Data Protection Bill 2019, which borrows liberally from GDPR, is a significant step for the APAC region, given that India is likely to be the region's most populous nation by 2025. The draft bill includes provisions concerning data anonymization, a right to be forgotten, rights in respect of automated decision-making and other GDPR-inspired innovations (please see the Individual Country Spotlight for India for a full discussion).

Enforcement? – call it a work in progress

It is clear that the volume of data protection enforcement activity is on the rise in the Asia-Pacific region, with important points to note for compliance programs.

The introduction of the CSL in China has led to round after round of highly publicized investigation campaigns, with a particular focus on online data collection by mobile apps. China's telecommunications regulator, the Ministry of Industry and Information Technology ("**MIIT**"), has launched several rounds of inspections against unlawful data collection by mobile apps. By the end of November 2020, MIIT has ordered in total 1,336 app operators to rectify non-compliance issues, publicizing 377 apps not appropriately rectified and ordering the removal of 94 apps from app stores, whose operators refuse to rectify. Despite that China's law enforcements in the realm of apps is hyperactive, enforcements in other fields remain quite silent. For instance, data processing activities via websites were largely unwatched. The Korean Communications Commission was also very active through 2019 with numerous enquiry letters being sent to operators of mobile apps, typically directed at improvements to online data protection policies. The pattern was that the KCC, or its agents, were pro-actively inspecting privacy policies available in app stores and sending email communications to app publishers requesting compliance.

The trend across the region is to expect pro-active engagement by regulators, particularly as data breach incidents become increasingly publicized in the press and public complaints continue to rise in number and breaches rise in severity. As mandatory data breach notification obligations become more common in the region, we can expect this trend to accelerate.

While regional businesses are often seeing more regulatory engagement and enforcement action, it is also clear that fines remain minimal. Amongst the largest reported fines in 2019 were those awarded by the Singapore Personal Data Protection Commission ("**PDPC**"), which fined Singapore Health S$250,000 (USD185,000) and Integrated Health Information Systems S$750,000 (USD550,000), both fines relating to failures to apply adequate security measures to safeguard Singapore's patient data system. The breaches contributed to a July 2018 cybersecurity attack that compromised the personal details of 1.5 million patients.

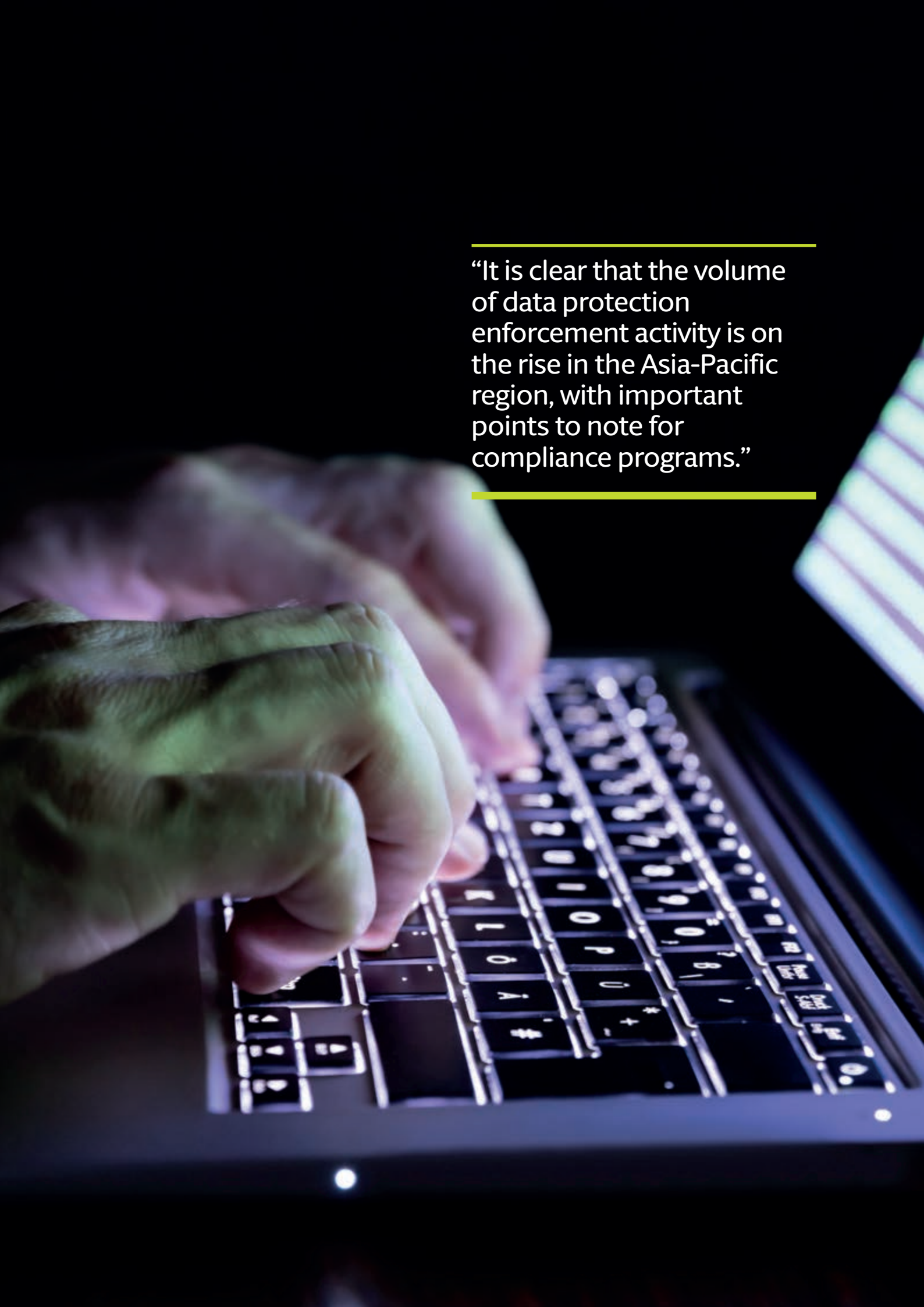
However, it is clear that fines of this scale are the exception, rather than the rule, even in Singapore. As reported by the Data Protection Excellence Centre in September 2019, the Singapore PDPC's total fines for the year at that time was S$1.28 million, levied against 26 organizations, meaning that the Singapore Health-related fines accounted for a significant majority of fines for the year.

It is likely that a reaction by lawmakers is coming, emboldened by the far larger scale of fines being awarded under the GDPR.

Proposed amendments to Australia's Privacy Act would increase penalties to AU$10 million, three times the value of the benefit obtained through the misconduct, or 10% of annual turnover.

The GDPR-inspired formulation of revenue-based fines has also found its way into India's draft data protection law, which is proposing maximum fines of the greater of Rs 15 crore (USD 2 million) or 4% of annual global turnover.

Proposals introduced to Hong Kong's legislative council in January 2020 also point to the prospect of revenue-based fines being introduced in relation to breaches of Hong Kong's Personal Data (Privacy) Ordinance.



"It is clear that the volume of data protection enforcement activity is on the rise in the Asia-Pacific region, with important points to note for compliance programs."

Revenue-based fines were introduced to Korea's Network Act some time ago, with fines of up to 3% of revenues derived from unauthorized overseas data transfers. Korea is generally understood to be one of the most challenging jurisdictions regionally in respect of data protection compliance. The bar was raised further in January 2020 when a Seoul District Court convicted and fined a tour operator for breaches of the Network Act arising from failures to prevent a data breach. The court also fined the company's privacy officer in his personal capacity, each being fined W10 million (USD 8,500). Prosecutors had apparently sought a custodial sentence, which was refused by the court. We understand that a number of similar cases are pending in the Korean court system, some of which may result in personal liability for individuals.

Data protection compliance strategies for APAC

With the data protection standards rapidly rising in the APAC region, and with lawmakers now showing greater resolve to punish those who fail to meet the mark, multinational organizations have a good reason to develop coordinated regional strategies for compliance.

GDPR compliance programs have provided a blueprint for organizations seeking a systemic approach to compliance, recognizing that the compliance effort is generally more extensive under the GDPR. Simply extending a GDPR-compliance program to operations in the APAC region would be "over compliance" in a number of key aspects and, at the same time, would miss important national law requirements that can, in some respects, exceed GDPR requirements or implement principles consistent with GDPR in different ways.

Smart data protection compliance in APAC, therefore, requires a local view. It also requires a regional view, given there is significant efficiency to be gained from developing a compliance program for APAC that reflects common requirements across the region and so avoids "re-inventing the wheel" for each jurisdiction.

Organizations take different approaches for different reasons, but there is now a proven process in taking a GDPR compliance program as the basis where it applies, then stripping out elements which have no application in the relevant APAC jurisdictions, and then finally adjusting the remainder to achieve compliance if most (if not all) jurisdictions, recognizing that there may be a need for "topping up" in APAC jurisdictions that have exceptional requirements in particular areas.

To give an example, direct marketing regulation in APAC remains a patchwork, with technical requirements that are specific to each jurisdiction, whether under the data protection law itself or under anti-spam laws, internet regulation or consumer protection laws. The result on this front is that some jurisdictions require discrete or unbundled opt-in or opt-out consents, sometimes with exemptions, sometimes without, some jurisdictions with "do not call" registries and some jurisdictions with specific formalities that must be adhered to in direct marketing communications, such as incorporating "ADV" or some equivalent form of indicator in message headings.

The recommended approach then is a two-pillar approach, with a GDPR compliant program in place where GDPR applies, and an APAC compliant approach for APAC.

The rapid pace of change across the APAC data protection regulatory landscape raises challenges for those seeking regional inter-operability and a consistent approach to compliance across the region.

The 2004 APEC Privacy Framework provided some rough signposts for a common approach to principles-based data protection regulation in the region. But while the common themes of the APEC framework are well-evident in national data protection laws across the region, it is clear that neither the APEC Privacy Framework nor any subsequent initiative has pressed for a strict harmonization of laws.

Offshore data collection and cross-border transfers have emerged as a particularly challenging area for multi-national organizations seeking to consolidate data processing arrangements centrally or in a regional hub. The data localization measures found in China's Cyber Security Law and Indonesia's Regulation

82 raise specific challenges for those jurisdictions, as does the requirement of an opt-in consent for international transfers from South Korea. Beyond these potential hard stops, the region's national data protection laws have come into effect, in many cases, with cross-border transfer restrictions in place that will typically allow for a range of compliance measures be taken, whether obtaining data subject consent, imposing contractual restrictions on transferees or exporting to a jurisdiction appearing on an official "white list".

The APEC Cross-Border Privacy Rules ("**APEC CBPR**") system was endorsed in 2011 as a development of the APEC Privacy Framework having an aim of alleviating these concerns. It is a voluntary, principles-based privacy code of conduct for data controllers in participating APEC member economies, based on the nine APEC Privacy Principles developed in the APEC Privacy Framework.

Recent years have seen the APEC CBPR gain momentum, with the Philippines announcing in September 2019 its submission of a letter of intent to become the ninth jurisdiction to participate in the system (alongside Australia, Canada, Japan, Mexico, Singapore, South Korea, Taiwan and the United States).

Organizations within these economies seeking certification under the APEC CBPR must have their data protection practices and procedures assessed as compliant with the program requirements by an APEC-recognised "Accountability Agent" in the jurisdiction in which they have their principal place of business (their "home" jurisdiction). Personal data from across the participating APEC membership may flow to the organization under the certification, subject to oversight by the Accountability Agent (which would have recourse by law or contract) and home privacy enforcement authority or the privacy enforcement authority in another participating jurisdiction (directly or through co-operation with the home jurisdiction authority).

However, it is important to be clear on the intended scope of the scheme, and its limitations. The CBPR scheme relates only to cross-border data flows. CBPR certification is a badge of compliance against the APEC Privacy Principles, but it does not represent compliance with applicable local privacy laws, so while participating economies recognize APEC CBPR certification as a means of achieving compliance with international transfer restrictions, the full range of remaining privacy issues still need to be considered by participating organizations in each applicable jurisdiction.

In a separate move to enhance co-operation between jurisdictions on the subject of data transfer in the region, in 2017, the Asia Business Law Institute's Board of Governors ("**ABLI**") launched a multi-stakeholder Data Privacy Project focusing on the regulation of international data transfers in a selection of Asian jurisdictions.

Hogan Lovells' Mark Parsons is among the group of data privacy experts appointed as a Jurisdictional Reporter to advise on the project.

A set of Jurisdictional Reports was published in 2018. In the second phase of the Project, the Jurisdictional Reporters and the wider Experts Committee will draft recommendations on key issues identified, aiming at a convergence of cross-border data transfer requirements across the region.

"With the data protection standards rapidly rising in the APAC region, and with lawmakers now showing greater resolve to punish those who fail to meet the mark, multinational organizations have a good reason to develop coordinated regional strategies for compliance."

What to watch for in 2021

We expect data protection and cybersecurity regulatory development to continue at a rapid pace during 2021.

Key initiatives to watch for:

- As the region's largest economy, China's fast-developing data protection landscape continues to be a key point of focus for business. A firm landing on international transfer regulation has been at the top of the wish list for three and a half years. The inclusion of extra-territorial measures in the new draft data protection laws raises another critical variable for multi-nationals. Continuing geopolitical tensions are very likely to influence China's program of regulatory reform, particularly now with the drafts' specific inclusion of countermeasures in response to discrimination against Chinese interests.
- With the legislative process in Hong Kong expected to run more smoothly, amendments to Hong Kong's data protection law – the Personal Data (Privacy) Ordinance – have become more likely in the course of 2021. We anticipate the amendments to cover areas, including mandatory data breaches, regulation on data processors and enforcement powers on doxing.
- Introduced to the Indian legislature in 2019, India's new data protection bill is currently under review by a Joint Parliamentary Committee, but it has been delayed several times due to the pandemic. This new data protection law would set the stage for this increasingly significant economy asserting its influence on regional policy developments for the first time. However, the draft bill has generated significant disagreement over what the right balance is for India between data protection, data sovereignty and the freedom for technological innovation that cross-border data transfers can support. Given this controversy, coupled with the impact of the pandemic, it is difficult to say if or when the bill will be enacted.
- We expect events, data breaches locally and multi-million Euro fines in the EU, in particular, to continue to heavily influence the development of "Data Protection 2.0" reforms. Lawmakers are increasingly taking the data protection agenda more seriously in the region, and with an increasing number of dedicated data protection authorities, we can expect to see enforcement action continue to rise.

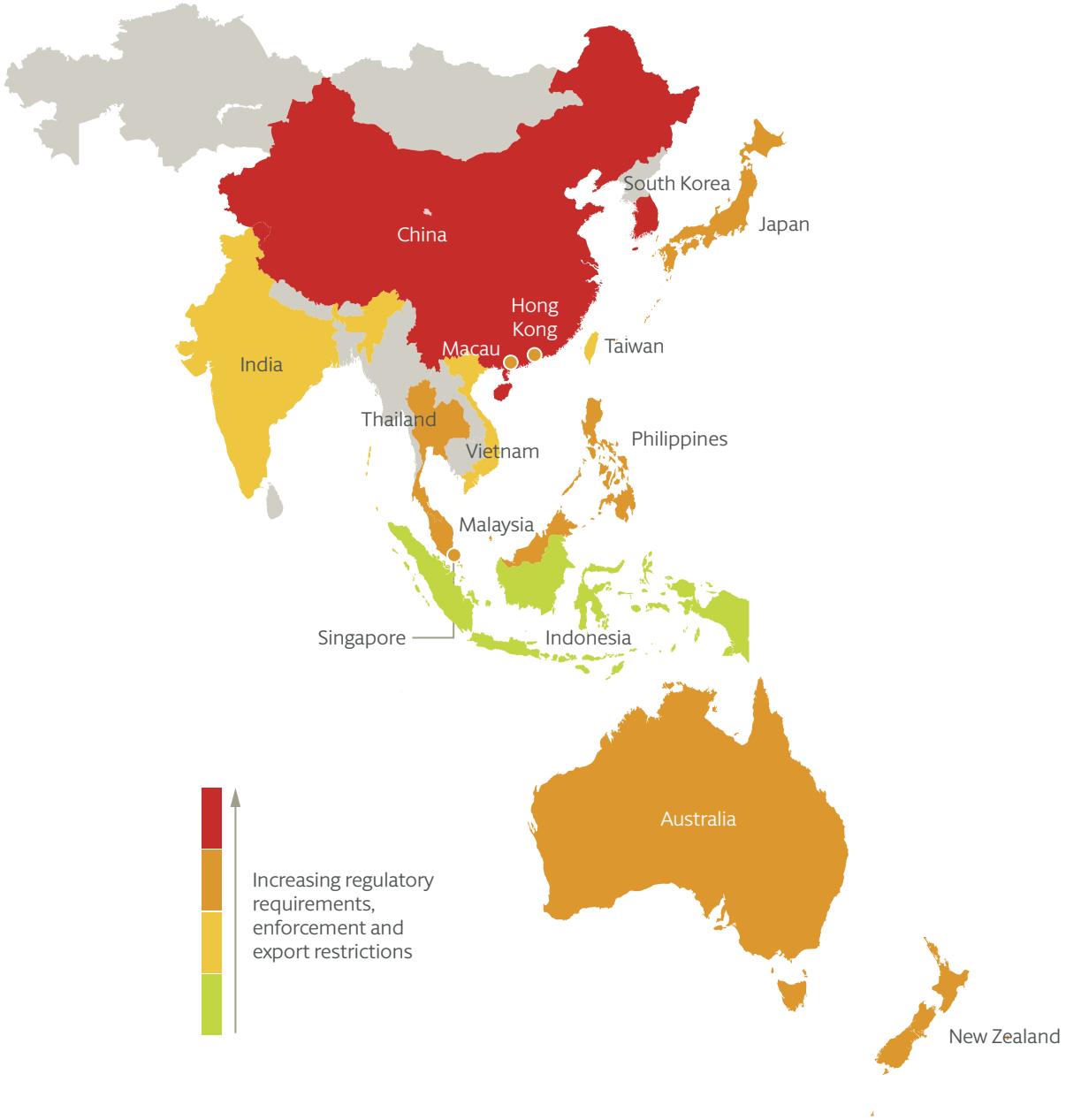
"We expect data protection and cybersecurity regulatory development to continue at a rapid pace during 2021."

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.



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. China instead relies on a combination of sector-specific laws, consumer protection laws and cybersecurity laws to regulate data handling practices, supplemented by a number of non-binding national standards. 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. Two new pieces of legislation, the Data Security Law and the Personal Information Protection Law, were released for public comment in 2020. Once finalized, these laws will form an overlay of comprehensive data protection law which will amount to a significant step forward for China.

The Cyber Security Law

China's controversial CSL came into effect on 1 June 2017. The focus under the CSL is not specifically on data protection, although the data protection measures found in the law are important. The wider remit of the law, which includes technology regulation and a vision of digital sovereignty, has prompted significant criticism from the international community. 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 law has led to more pervasive cyber surveillance and enhanced online censorship by requiring, for example, network operators to store internet logs for at least six months, block the dissemination of illegal content, and provide "technical support and assistance" to the authorities in national security and criminal investigations. Much still depends, however, on the content of the implementing regulations to be issued by the Cyberspace Administration of China ("**CAC**"), although the implementation of MPLS 2.0 (discussed in more detail below) may well have confirmed some of the worst fears for multi-nationals with operations in China.

Given the growing cyber threat globally, China's move towards more rigorous cybersecurity 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.

The Cyber Security Law regulates two types of organizations: (i) operators of critical information infrastructure ("**OCII**"); and (ii) network operators ("**NO**").

The scope of organizations falling into the category of OCII is not bounded by an exhaustive definition and is ultimately subject to designation by the authorities. The Cyber Security Law outlines the industries (including telecommunications, energy, transport and financial services) and state activities (public services and e-government) that form the law's focus. Prior to the law's implementation, the CAC published an "Examination Guideline" that laid out materiality thresholds for designating OCII based on considerations such as the number of users of a particular system or platform or the scale of likely impact resulting from a cybersecurity breach. This guideline has been useful in assessing whether or not a particular organization is an OCII under the law. OCII are subject to extensive technology regulation measures, including an obligation to only deploy network products and services that have completed a national security review. There are also far-reaching cybersecurity administration and reporting obligations under the law.

NO have a far more open-ended definition, essentially encompassing any organization that operates a computer network in China, even if that system is entirely internal to the organization. A key part of the concern over the expansive scope

of NOs relates to the Cyber Security Law's data export review measure.

Article 37 of the Cyber Security Law states that OCII are required to store personal data and "important data" (i.e., having importance in relation to China's national security or other state interests) in China unless it is necessary to send that data abroad and a security review has been completed. The first draft of the security review measures published by the CAC in May 2017 purport to extend the application of Article 37 to NOs.

Subsequent drafts, most recently the version published in June 2019, continue to propose an extension of Article 37 to NO. Few multi-national organizations would expect to be considered to be OCII, but most organizations with operations in China would expect to fall within the scope of NO, as currently elaborated.

Based on previous drafts of the implementing measures, there had been some hope that the security review measure would involve mandatory reviews for OCIIs, but NOs will be subject to a tiered arrangement in which NOs whose international transfers do not meet certain materiality thresholds will be subject only to a self-assessment process, with reporting to the relevant authorities rather than an official approval process.

However, the June 2019 draft of the implementing measures proposed to remove the self-assessment stream, proposing that each and every transfer of personal data from China be approved by the authorities. Provincial cybersecurity regulators receiving applications would be required to complete reviews within 15 days of receipt of a complete application, rejecting applications which would be potentially harmful to national security or the public interest or lacks effective safeguards. Assessments would need to be reviewed every two years or earlier if there is any change to the scope, volume or duration of the transfer.

However, this proposed data cross-border transfer regime does not appear to be aligned with the corresponding measures under the draft Personal Information Protection Law, which promises to scale back security assessments and adopt a more risk-based approach to cross-border transfer regulation (please see further details below).

With all the focus on the implementation of the CSL, it has been possible to overlook the fact that China has a patchwork of data protection regulations with a wide range of legal sources, most significantly the Consumer Law, the E-Commerce Law that took effect on 1 January 2019, and regulations applicable to the collection of personal data through the internet and telecommunications services. The data protection requirements applicable in any specific context will depend on the specific activity in question, the types of personal data involved and the manner and source of collection.

Another important feature of the Chinese data protection landscape is the non-binding data protection standard titled the Information Security Technology – Personal Information Security Specification issued by the Standardization Administration of China ("**GB/T 35273-2020**"), which initially came into effect on 1 May 2018 and was later replaced by an amended version on 1 October 2020. The 2020 amendments retained the original framework for the standard, but added new provisions dealing with matters such as user profiling, personalized displays, automated decision making and the handling of personal biometric data.

GB/T 35273-2020 provides a series of best practices for the collection, processing, retention, use, sharing and transfer of personal information and for the handling of information security incidents. The standard has been read by regulators and law enforcement officials as important elaboration of a number of the general principles concerning data protection stated in the CSL, adding some important glosses on expected best practice:

- a definition of explicit consent (required where sensitive personal data is collected), which includes: (i) a written statement (whether through physical or electronic media); (ii) a ticked box; (iii) registration; (iv) sending a consent message; or (v) the data subject continuing to communicate with

the organization collecting the data (a form of implied consent);

- a requirement that encryption be applied to the transmission and storage of sensitive personal data;
- a requirement that when collecting personal data indirectly, the data controller should: (i) require the third party providing the information to explain the source of the personal data; (ii) investigate whether or not the third party obtained data subject consent to the sharing of their data; (iii) clarify the scope of consent, including what data-related activities are covered (i.e. transfer, sharing, disclosure, deletion, etc.) and whether the purpose of use of such personal data is covered by such consent; and (iv) if the data processing activities being conducted are not covered by the consent, explicit consent of the data subject should be obtained either before the data processing or reasonably after the acquisition of such data;
- a requirement that when personal data is transferred as part of a merger, acquisition or restructuring transaction, the data controller must notify the data subject of this fact and the successor to the controller must assume the obligations and responsibilities of the original controller; and if the purpose of use of personal data is changed post-transaction, the successor must obtain a new explicit consent from the data subject; and
- a requirement that data controllers formulate a contingency plan for security incidents that involve personal information and conduct emergency drills at least once a year.

One of the most controversial areas of review under GB/T 35273-2020 is the distinction it draws between collection of data for "core" versus "non-core" purposes, with "core" purposes being the obvious purpose of collection, for example, for the provision of a service or functionality through a mobile app. "Non-core" purposes include the commercialization of personal data through marketing, profiling and retargeting activity.

The App Privacy Methods

The move to implement the "core" versus "non-core" distinction in mandatory law has now begun. On 30 December, 2019, the CAC, together with the MIIT, the Ministry of Public Security ("MPS") and the State Administration for Market Regulation ("SAMR"), jointly issued a detailed set of data protection requirements for mobile app operators, the Methods on the Identification of Illegal Collection and Use of Personal Information by Apps (the "App Privacy Methods"). The App Privacy Methods set out directions Chinese regulators should apply when they investigate mobile app operators' compliance with broadly worded – but mandatory – data protection requirements under the Cyber Security Law, in particular, a very broadly framed obligation under the law to collect and use personal data as lawful, appropriate and necessary in line with consents obtained from data subjects. Of particular relevance here, the App Privacy Methods direct regulators to consider whether personal data collected through a mobile app significantly exceeds what is necessary for the services provided by the app and whether users are forced to consent to the use of their personal data for purposes such as user experience enhancement, research and development or the personalization of push advertising.

The implementation of the App Privacy Methods represents a critical regulatory development for cookie use in China. It is clear that the distinction between "core" and "non-core" data processing introduced in GB/T 35273-2017 has now been implemented in a mandatory regulatory requirement. It is, as yet, too early to understand how the App Privacy Methods will be enforced in practice, given the potential disruption it would mean to the operation of commercial internet services in China if taken literally, but it is clear that regulatory scrutiny of the internet economy is on a tightening trend in China.

MLPS 2.0

2019 saw the implementation of a revamped version of China's cybersecurity framework, the Multi-Level Protection Scheme ("**MLPS**"). "MLPS 2.0", as it has become known, is the first significant update to MLPS since the introduction of the Cyber Security Law. MLPS 2.0 comprises a new set of MLPS regulations, together with three new national standards. MLPS began in 2006 as a self-certification regime for network security. MLPS 2.0 is a far more potentially invasive upgrade of the regime, with key changes, including the need for organizations having a risk rating of 3 and above now being required to implement cybersecurity monitoring, detection and response programs, and make incident notifications to relevant bodies, amongst other requirements. MLPS 2.0 introduced annual inspections by government officials and, in a move that has raised significant concern for multi-nationals operating in China, the revised rules empower MPS to perform remote access inspections of network equipment, including cloud services.

The clear trend in China is towards an ever more tightly regulated internet, both in terms of data regulation and cybersecurity. We understand that in the course of 2020, few multi-national corporations were asked to undergo a MPLS 2.0 program assessment, but this position may change in 2021.

Draft Data Security Law

On 3 July 2020, the National People's Congress published a consultation draft of the Data Security Law ("**Draft DSL**").

This Draft DSL provides a set of high-level national data security principles and policies, and the main elements of which are: (a) the establishment of basic mechanisms for data security management, such as data classification and management, data security risk assessment, monitoring, warning and emergency response; (b) the data security protection obligations of organizations and individuals carrying out data-related activities; (c) measures to support the promotion and development of data security; and (d) the establishment of mechanisms to guarantee the security of government data, and promote the openness of government data.

Notably, the Draft DSL extends the geographic scope of Chinese data laws, applying to organizations or individuals outside China if they carry out data activities in such a way that may undermine national security, other public

"Rapid international developments and recent events in Hong Kong have moved the government and the PCPD to work towards improvements to the Personal Data (Privacy) Ordinance"

interests of China or the legitimate rights of any citizens or organizations in China. As drafted, the Draft DSL would introduce extraterritorial regulation of data processing activities, a dimension not yet seen under the CSL, which has been understood to apply only to systems and technology physically located in mainland China.

Similar to the CSL, many of the provisions in the Draft DSL are very general in nature, and so it is likely that the implementation of the Data Security Law will largely rely on subsequent supporting regulations and measures.

Draft Personal Information Law

On 21 October 2020, China's National People's Congress published a consultation draft of the Personal Information Protection Law ("**Draft PIPL**"). Drawing extensively from the GDPR, the law would set a high bar for Chinese data protection, taking revocable consent as its principal basis for processing (without GDPR's legitimate interests basis for processing), introducing extraterritorial effect and restrictions on international data transfers and imposing revenue-based fines as the principal penalty for non-compliance:

- Basis for Processing: consent would be the principal basis for processing personal data, with specific exemptions for conclusion or performance of contracts with data subjects, compliance with applicable laws, public health and public interest processing. Notably, the Draft PIPL does not follow GDPR in providing for legitimate interests processing.
- Extraterritorial Effect: where offshore data processing activities are for the purpose of (i) providing services or products to individuals resident in China, or (ii) analyzing or evaluating the behavior of individuals resident in China, the Draft PIPL would be applied extraterritorially.
- International Data Transfers: Security assessment would be mandatory for data transferors that are either OCIIs (as defined above under the CSL) or undertake a volume of data processing that meets materiality thresholds to be set by the CAC. Non-OCII transferors falling below the CAC's materiality thresholds could meet the international transfer restrictions by (i) a certification by a third-party professional institution; or (ii) an agreement between the Chinese data transferor and the offshore data recipient with obligations sufficient to ensure the transferred data will continue to be processed in accordance with the standards under the Draft PIPL.
- Imposing Revenue-based Fines: Under the Draft PIPL, fines of up to RMB 1,000,000 could be imposed on companies, with fines of RMB 10,000 to 100,000 imposed on responsible individuals. In more serious cases, the fine could be increased to RMB 50,000,000 or 5% of the company's total turnover in the preceding year, with fines of RMB 100,000 to 1,000,000 imposed on responsible individuals.

Hong Kong

Hong Kong's Privacy Commissioner for Personal Data (the "**PCPD**") remains a policy-making leader in the region. Rapid international developments and recent events in Hong Kong have moved the government and the PCPD to work towards improvements to the Personal Data (Privacy) Ordinance (the "**PDPO**"), a comprehensive data protection law which has only been amended once since its introduction in 1995.

In January 2020, the PCPD, together with the Constitutional and Mainland Affairs Bureau ("**CMAB**"), presented a discussion paper outlining topics for reform of the PDPO to the members of the Legislative Council (the "P**DPO Review Paper**"). The PDPO Review Paper sets out some important areas of legislative reform which would modernize the PDPO, bringing the law closer in line with international trends.

Proposed Legislative Changes

The PDPO Review Paper focuses on the following areas:

- **Mandatory Breach Notification Obligation:** At present, the PDPO requires data users to take all practicable steps to prevent unauthorized or accidental access of personal data. However, unlike an increasing number of laws internationally, the PDPO does not include an obligation to notify

the PCPD or impacted data subjects if this provision has been breached. This lack of a breach notification requirement was heavily publicized following the PCPD's investigation of a substantial data breach by Cathay Pacific Airways. The PDPO Review Paper proposes a mandatory breach notification, which would require further formulation on: (i) how a "personal data breach" is defined; (ii) the threshold for notification; (iii) the timeframe for notification; and (iv) the method of notification. A key challenge for the proposed notification obligation is to strike a balance between alerting the PCPD of data breaches whilst avoiding "notification fatigue".

- **Data Retention:** The PDPO's data protection principles require data users to ensure personal data is not kept longer than necessary for the fulfilment of the purposes of collection but does not specify when the personal data is "no longer necessary". The PDPO Review Paper recommends amending the PDPO to require data users to develop clear personal data retention policies, covering the maximum retention period for different types of personal data, the legal requirements that may affect those retention periods and how those retention periods are calculated.
- **Fines and Sanctions:** At present, the PCPD may issue an enforcement notice requiring a data user to remediate its breach of the data protection principles. A breach of an enforcement notice may result in a Level 5 fine (HK$50,000) (approx. USD 6500) and imprisonment for two years on first conviction. To increase the deterrent effect of these fines, the PDPO Review Paper proposes to increase these fines and to allow the PCPD to issue administrative fines.
- **Regulation of Data Processors:** Currently, the PDPO only regulates data users and not data processors, but the PDPO does require data users to ensure that data processors adopt measures to protect personal data. The PDPO Review Paper goes further and proposes regulatory oversight directly over data processors.

- **Definition of Personal Data:** The PDPO Review Paper proposes to expand the definition of "personal data" to include data that relates to an "identifiable" natural person as opposed to the current definition of an "identified" natural person. This would cover more categories of data, for example, tracking and behavioral data generated by big-data tools.
- **"Doxing":** A significant focus of the PDPO overhaul is to address "doxing" – i.e. the practice of disclosing personal data for the purpose of shaming or intimidation – a phenomenon which intensified during the political unrest in Hong Kong over the past two years. The Hong Kong government is currently considering conferring statutory powers on the PCPD to require the removal of doxing-related content and to bestow criminal investigations and prosecutions powers under the PDPO.

The PCPD has stated that amendments to the PDPO will be her priority in the coming year.

Enforcement

Over the past year, we have also seen the PCPD step up its enforcement actions, especially in relation to doxing activities. As of 31 December 2020, the PDPO had referred 1,461 doxing cases to the police for criminal investigation and consideration of prosecution, 17 of which resulted in individuals being arrested by the police on suspicion of contravening the PDPO. In 2020, Hong Kong also saw the first conviction for a doxing offence under the PDPO where the defendant was sentenced to 24 months' imprisonment. In recent months, PCPD have also strengthened its monitoring on online platforms and have worked with local and foreign private entities to tackle doxing-related materials.

India

India's parliamentary cabinet approved the Personal Data Protection Bill 2019 ("**2019 Bill**") in early December 2019, taking India one step closer to implementing comprehensive data protection regulation for the first time.

A legislative committee tabled the first draft of the law to the Ministry of Electronics and Information Technology ("**MEITY**") in the summer of 2018. At the time, the scope and complexity of the draft law surprised many observers, charting a course for India that would involve its first data protection legislation incorporating many advanced data protection concepts found in the GDPR. There has been much discussion of the bill since, with the result that the 2019 Bill retains many of the core elements of the 2018 version, but with some important changes. That said, reports from government sources emerged in December 2020 that the 2019 Bill was unlikely to be passed in its current form and that significant amendment was needed. We have not yet seen the output of these further deliberations. As India's population is expected to be the largest in APAC in a few years and the country is likely to emerge as a significant economic force regionally, its data protection framework will be a critical bellwether for regional policymaking.

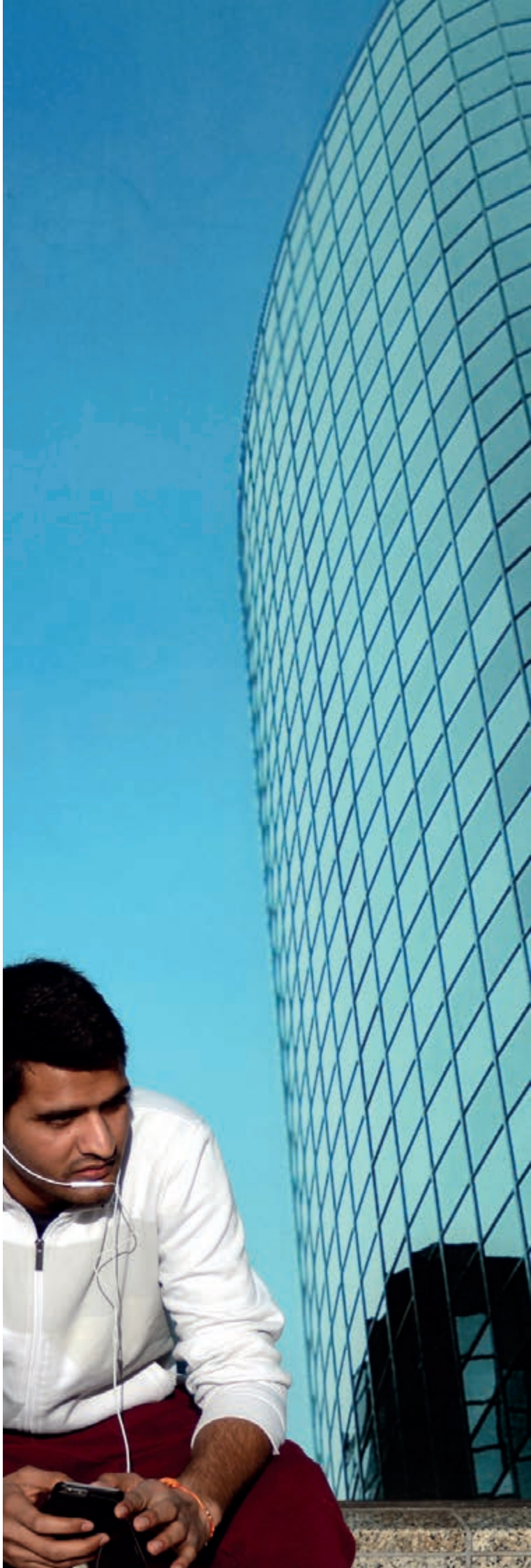
Key elements of the 2019 Bill include:

- **A dedicated authority:** The 2019 Bill would establish the Data Protection Authority of India (the "**Indian DPA**"), which would serve as a dedicated data protection regulator (a key indicator for measuring the likely seriousness of intent for a new data protection regime).
- **Extra-territoriality:** Drawing inspiration from GDPR, the 2019 Bill would regulate all personal data collected or processed within the territory of India, processed by any Indian organization oro the processing of personal data by organizations not present within India, if such processing is: (a) in connection with any business carried on in India, or any systematic activity of offering goods or services to data subjects within the territory of India; or (b) in connection with any activity which involves profiling of data principals within the territory of India.
- **"Significant data fiduciaries" and data protection officers:** The 2019 Bill would require that "significant" data fiduciaries (organizations controlling the processing of personal data) appoint a data protection officer responsible for advising the organization on its compliance with the law and for being a principal point of contact in relation to compliance matters, amongst other accountability obligations. The 2019 Bill sets

out general criteria as to the scale or nature of data processing that would be "significant" and so trigger this requirement. The intention appears to be that the Indian DPA will notify organizations or classes of organization that will be considered "significant". "Social media intermediaries" (discussed in more detail below) exceeding published materiality thresholds and whose actions have or are likely to have a "significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India", will be designed by the central government, in consultation with the India DPA, as "significant". It is also noteworthy that significant data fiduciaries would be required to have its policies and its conduct in processing personal data audited annually by an independent data auditor.

- **Basis for processing:** The 2019 Bill requires informed data subject consent to the processing of personal data, subject to prescribed exceptions. Consent is revocable under the 2019 Bill, and the provision of goods or services (or the provision of any quality of goods or services) cannot be made conditional on receiving a data subject's consent.
- **Sensitive personal data and personal data of children:** The processing of "sensitive personal data" would require explicit consent, with unbundled consent required so as to create optional levels of processing. "Sensitive personal data" is very broadly defined, including "financial data" in addition to health data, official identifiers and other categories of personal data. The 2019 Bill separately includes measures directed at processing personal data of children (defined as those under the age of 18), requiring the consent of a parent or guardian and prohibiting profiling, tracking and behavioral monitoring of children.
- **"Reasonable purposes" processing:** The 2019 Bill provides that consent is not required for "reasonable purposes" of processing which are prescribed by regulation. These "reasonable purposes" are non-exhaustively defined to include purposes such as the prevention and detection of unlawful activity, whistle blowing, mergers and acquisitions, credit scoring, the processing of publicly available personal data and the operation of search engines. The Indian DPA may prescribe safeguards concerning "reasonable purposes" processing.
- **Data subject rights:** In addition to rights to access and correct personal data, the 2019 Bill would provide data subjects with rights of erasure and portability.
- **Privacy by design policy:** The 2019 Bill requires all data controllers to prepare a "privacy by design policy", which would be an internal data protection policy augmented by an accountability program. The privacy by design policy involves the implementation of organizational systems and procedures intended to anticipate, identify and avoid harm to data subjects, formulated in such a way as to balance the legitimate interests of the business against privacy interests and ensure transparent processing. The 2019 Bill provides for voluntary certification of privacy by design policies by the Indian DPA, enabling the data controller to publish the policy and the certification.
- **Mandatory data breach notification:** The 2019 Bill would require organizations to notify the Indian DPA as soon as possible and not later than the time period specified by regulations, following any personal data breach that is likely to cause harm to any data subject. Upon receipt of a notification, the Indian DPA is required to determine whether data subjects should also be notified of the breach, having regard to the prospect of harm and the scope for mitigating action. The Indian DPA may also publish details of the breach on its website.

- **Social media intermediaries:** The 2019 Bill incorporates specific regulations for "social media intermediaries", including the requirements in respect of data protection officers noted above. Social media intermediaries are under specific obligations to undertake data protection impact analyses before introducing processing involving new technologies or large-scale profiling or use of sensitive personal data such as genetic data or biometric data or other processing which carries a risk of significant harm.
- **Data protection impact analysis:** The 2019 Bill provides that the Indian DPA may specify circumstances in which organizations are required to carry out data protection impact analyses, with an obligation on the organization's data protection officer to review and submit the assessment to the Indian DPA. On receipt of an assessment, the Indian DPA may direct the organization to cease the processing or continue with it subject to conditions.
- **Data localization:** Much focus had been drawn to India's proposals to restrict transfers of data in the 2018 draft of the bill. The 2019 Bill relaxes these requirements somewhat, with restrictions applying only to "sensitive personal data" (which must be stored in India but may be copied offshore) and "critical personal data", which may only be processed in India, subject to a "vital interests" exception or approval by the central government. International transfers of sensitive personal data require data subjects' explicit consent plus the controller's reliance on one of the following: (i) a contract or intra-group scheme, in either case, approved by the Indian DPA; (ii) a "white list" of export jurisdictions published by the central government; or (iii) as otherwise permitted by the Indian DPA. Given the breadth of the definition of sensitive personal data, which includes financial information, and given that the Indian central government has discretion as to how information is designated as "critical", the localization aspect of the 2019 Bill has generated significant concerns.



Singapore

Singapore's push to be a leading regional innovation economy is reflected in the rapid pace of regulatory development of the Personal Data Protection Act (the "**PDPA**") and the thought leadership of the Personal Data Protection Commission (the "**PDPC**"). Most significantly, the Personal Data Protection (Amendment) Bill (the "**Bill**") was passed by Parliament on 2 November 2020.

The Bill proposes significant changes to the PDPA, being focused on four key themes: (1) strengthening accountability; (2) enabling meaningful consent; (3) increasing consumer autonomy; and (4) increasing deterrence and strengthening enforcement powers. We expect the Bill to come into force in early 2021, with different parts of the Bill being implemented in phases.

The key areas of reform under the Bill are as follows:

Mandatory data breach notification regime

At present, the PDPC adopts a voluntary regime. In order to strengthen accountability, the Bill formalizes much of the existing guidance into legislation by introducing a mandatory data breach notification requirement. The regime will cover data breaches which result in, or are likely to result in, significant harm to an affected individual, or which is of a significant scale. The organisation concerned will be required to notify the PDPC and, if necessary, affected individuals following a data breach. There are various scenarios in which an organisation need not notify the individual, including where sufficient remedial action has been taken, or the data is sufficiently encrypted.

Data breaches that constitute significant harm will be clarified in later regulations but will likely include those which compromise sensitive categories of personal data, such as social security numbers, drivers' licence numbers, credit/debit card numbers, health insurance information and medical history information. A numerical threshold will be used to determine whether a breach is of a significant scale. The PDPC currently notes that data breaches that affect 500 or more individuals would be an appropriate threshold.

Extended deemed consent provisions

The PDPC has recognized that technological developments are causing significant challenges for consent-based approaches to data protection. It is often not practical for organisations to anticipate the specific purpose for each collection of data at the outset, nor always practical to seek express consent. The Bill therefore expands the concept of deemed consent in two ways – deemed consent by contractual necessity and deemed consent by notification.

Under the first limb, consent will be deemed to have been given where data has been disclosed to, and used by, a third party organisation and it is reasonably necessary to conclude or perform a contract or transaction between the individual and the disclosing organisation.

Under the second limb, consent will be deemed to have been given where individuals have been notified of the purpose of the intended collection, given a reasonable opportunity to opt-out, and have not opted out.

Exceptions to the consent requirement

The Bill will also introduce two entirely new exceptions to the consent requirement, covering situations where there are substantial public or systemic benefits and where obtaining individuals' consent may not be appropriate.

A "legitimate interests" exception will be introduced to enable organisations to collect, use or disclose personal data where it is in the legitimate interest of the organisation and where the benefit to the public outweighs any adverse effect to the individual. This is very similar to the legitimate interest concept enshrined in the GDPR and will work to ensure IT and network security, as well as prevent illegal activities such as fraud and money laundering.

In a pragmatic move, businesses will also be able to use (but not collect or disclose) personal data without having to obtain consent for "business improvement" purposes, where such purposes cannot be achieved using aggregated data and a reasonable person would consider such use to be appropriate. These broad criteria include ensuring better operational efficiency, improved services for product or service developments and to get to know customers better. This exception cannot be used for marketing messages.

Data portability obligation

The Bill will introduce a new data portability obligation aimed at making it easier for consumers to switch service providers and avoid being "locked in" with a single provider. At an individual's request, an organisation will be obliged to transmit all data about the individual that is in their possession to another organisation in a commonly used machine-readable format. This measure will facilitate movement of consumer data from one service provider to another in order to improve competition.

A number of exceptions to the data portability obligation will be introduced. These will mirror the exceptions to the Access Obligation under Schedule Five to the PDPA. One of the key exceptions will relate to data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation. The right will also be limited to "white-listed datasets", being specific categories of personal data specified by the PDPC in consultation with industry.

Increased deterrence

The Bill will strengthen the accountability of individuals who handle or have access to personal data through the introduction of three new offences: (1) knowing or reckless unauthorized disclosure of personal data; (2) knowing or reckless unauthorized use of personal data for a wrongful gain or a wrongful loss to any person; and (3) knowing or reckless unauthorized re-identification of anonymized data.

Whilst the PDPC will remain focused on holding organisations accountable for data protection, this move to directly criminalize the mishandling of personal by data by individuals is an important development in the safeguarding of personal data. Individuals found guilty of an offence will be liable upon conviction to a fine of up to SGD 5,000 and/or imprisonment for up to two years. This would include employees who act in contravention of an employer's policies or act outside their scope of employment; as such, the role of the Data Protection Officer (mandatory for all entities in Singapore, regardless of size or operations), along with staff training and protocols, are likely to be given far more thought by Singapore organisations.

The maximum financial penalty under the PDPA will also be increased to the greater of 10% of an organization's annual turnover in Singapore where such turnover exceeds S$10 million, or in any other case, S$1 million. These penalties are significant, although it should be noted that they are still comparatively low compared to some other regimes (the maximum penalty under the GDPR, for example, is the greater of 4% of worldwide turnover, or €20 million).

Australia

In April 2019, the Australian Federal Government announced major changes to the Privacy Act, including additional powers for the Information Commissioner and tougher penalties for misuse of personal information.

The new regime will increase the maximum penalties for misuse of personal information by entities covered by the Privacy Act, from $2.1 million for serious or repeated breaches, to the greatest of:

a) $10 million;

b) three times the value of any benefit obtained through the misuse of information; or

c) 10% of a company's annual domestic turnover.

The updated penalties will bring Australia more in line with the GDPR, under which the maximum penalty for an entity's breach of privacy is €20 million or 2% of that entity's annual global turnover. These proposed penalties (delayed due to the COVID-19 pandemic) have not yet been passed by parliament.

In March 2020, the Office of the Australian Information Commissioner (the "OAIC") launched proceedings against Facebook for serious and/or repeated breaches of the Privacy Act, in particular, using and disclosing personal information other than for the purpose for which it was collected and having inadequate security measures in place. The proceedings are the first of its kind in the Australian legal landscape and have not yet been decided.

In January 2021, Kogan Australia Pty Ltd, operator of an online shopping platform, agreed to a court-enforceable undertaking and paid $310,800 in fines for breaches of the Spam Act 2003 (Cth). Following investigation by Australian Communications and Media Authority, Kogan were found to have sent 42 million marketing emails to consumers without adequate unsubscribe functions. This penalty highlights the importance for companies to implement adequate opt-out mechanisms in their communications.

Alongside the OAIC, the Australian Competition and Consumer Commission continues to progress its Consumer Data Right ("CDR") initiative. The CDR will first apply to the banking sector in phases, followed by the energy sector and telecommunications sector. Consumer data relating to credit and debit cards, deposit accounts and transaction accounts were made available from 1 July 2020 followed by consumer data relating to mortgage and personal loans in November 2020. Other sectors impacted by privacy reforms, including the health and medical, communications (relevant to telehealth services), financial services and markets sector (including health insurance business), data storage or processing (such as cloud service providers) and food and grocery sector. On 10 December 2020, the Security Legislation Amendment (Critical Infrastructure) Bill 2020 ("Bill") was introduced and read into Parliament only a month after its release. The Bill aims to strengthen the cybersecurity of infrastructure by introducing additional positive obligations, including sector specific risk management programs, mandatory cyber incident reporting, enhanced cybersecurity obligations for systems of national significance and the introduction of government assistance in responding to significant cyber attacks.

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 ("**PIPA**") and the IT Network Act are supplemented by sector-specific laws, creating a very difficult compliance environment.

Amendments to PIPA, the IT Network Act and the Credit Information Use and Protection Act were made in August 2020. Key amendments seek to help support South Korea's drive to continue to be an innovation economy. A key amendment narrowed the scope of the definition of "personal data" under PIPA to provide that information must be such that it may be "easily combined" with other information to identify a specific individual in order to be personal data. An express exclusion of anonymized personal data from the scope of personal data has been added.

A concept of "pseudonymized" personal data has also been introduced, allowing the processing of such information for statistical and research purposes without data subject consent. A form of legitimate interests processing has also been introduced, allowing organizations to process personal data for purposes "reasonably related" to the original purposes of processing without data subject consent where to do so would not result in disadvantage to the data subject or compromise data security.

The legislative amendments also included the elevation of the Personal Information Protection Commission ("**PIPC**") to the status of a central administrative agency reporting directly to the prime minister. The PIPC now has consolidated authority over data protection matters, assuming various areas of authority from the Korea Communications Commission and the Ministry of Public Administration and Security, including responsibility for investigating data breaches. Although the legislative reforms signal a clear move towards greater support for South Korea's digital economy, the compliance stakes have been raised further. In January 2020, a Seoul District Court convicted and fined a tour operator for breaches of the Network Act arising from failures to prevent a data breach. The court also fined the company's privacy officer in his personal capacity, each being fined □10 million (USD 8,500). Prosecutors had apparently sought a custodial sentence, which was refused by the court. The prospect of individual liability for data protection breaches has not been a feature of the landscape

in the Asia-Pacific region, meaning that this and other similar cases will be closely followed.

Japan

On June 12, 2020, the Japanese government announced substantial amendments to the Japanese Act on the Protection of Personal Information ("**APPI**"), requiring companies to take certain additional measures to protect personal data of data subjects. The amended version will likely come into force in the first half of 2022. The exact date is not determined yet. Guidance from the regulator on the provisions is expected to be published later this year. The amendment aims to broaden data subjects' powers to exercise control over their data and to establish a system to facilitate corporations' internal use of "big data". The update comes as part of the Japanese government's commitment to update Japan's privacy law every three years.

Key provisions include:

- **Expanding rights of data subjects:** The update aims to broaden the right of data subjects, making it easier for data subjects to request that a data handler cease use of or delete stored data. Further, the amendments broaden the scope of retained data which a data handler must disclose to a data subject upon request regardless of the retention period (at present, data retained for less than six months is subject to fewer restrictions).
- P**seudonymization:** The amended APPI introduces the concept of "Pseudonymously Processed Information", as the conditions to anonymize personal information are very strict under the APPI so that it is hardly feasible to rely on anonymization. Data handlers can utilize pseudonymized data in limited circumstances, while obligations of dealing with data subjects' rights, such as for disclosure and cease of utilization, will be eased.
- **Mandatory breach reporting:** The updated APPI makes it mandatory for data handlers to report a data breach to the PPC and the affected data subjects.
- **Revising and strengthening of penalties:** The amendment is partially effective since December 2020 regarding penalties. An entity may now be punished with a fine of up to 100,000,000 JPY (about USD 1 million) in case of violation of an order from the authority or illegitimate use of data.
- **Extraterritorial applicability:** The PPC will be granted authority to request foreign entities which supply goods or services in Japan and handle personal information of individuals in Japan to submit reports or to issue orders in case of violations of the APPI by foreign entities, which can be enforced with a penalty.

Data protection and cybersecurity regulation in APAC

A guide to making (and keeping) your business compliant

The tightening of the APAC region's data protection regulatory environment and the emergence of cybersecurity 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 mobile and cloud-based operating platforms and transfer data across borders with a view to improving operational efficiency and leverage economies of scale.

An effective data protection and cybersecurity 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 of 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 monetizing data?
- What data protection and cybersecurity regulatory regimes apply to the organization'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 organization'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 anonymized 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-personalized 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 anonymized or aggregated datasets has never been higher. Assessing data protection compliance will involve assessing the procedures for creating and maintaining the de-personalization of these datasets.


8
9
O
I
O
P
K
L
Ñ
M
alt gr

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 most of the region's comprehensive data protection laws and in jurisdictions where it is not subject to explicit enhanced protection (such as Hong Kong and Singapore), data security obligations will nevertheless be proportionately higher in respect of these data.

Other personal data

Many organizations 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 organization 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 organization 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. As organizations increasingly move to e-commerce and social media platforms to market and sell their products, collecting, sharing and processing personal data through these "ecosystems" requires careful scrutiny, particularly as increased regulatory focus comes to these platforms in the EU and other jurisdictions.

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 it clear that publicly available data may only be used in compliance with general data privacy principles.

We would recommend a holistic approach to analyzing 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 APAC region and the introduction of localization measures in some jurisdictions.

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.

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 APAC region's data protection laws are generally 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 APAC 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 organization, 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 behavioral profiling technology to company web sites and apps.

Assessing regulatory requirements

Once the organization'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 cybersecurity regimes can be undertaken.

1. Leveraging what's already there

The regulatory analysis will not necessarily be a matter of re-inventing the wheel, in particular for EU-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 APAC region, and so it is often efficient to leverage global or regional policies from elsewhere in the organization if they are transportable having regard to the nature of the business and the data processing taking place. As the APAC region's data protection and cybersecurity regimes proliferate and develop, however, there are more and more local distinctions that will need to be considered.

"Irrespective of the starting point a business finds itself in, we generally counsel clients with regional footprints to take a regional view of the APAC region's data protection and cybersecurity compliance requirements."

2. 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 the APAC region's data protection and cybersecurity compliance requirements. With the introduction of the GDPR in 2018, many organizations have started a "global upgrade" of their data protection compliance programs. However, simply rolling out an EU-based compliance program in the APAC region will likely represent "over compliance" in a number of areas. Our recommended approach is to carefully distinguish where the GDPR applies (and where it does not) and craft an efficient compliance solution that involves consistency of approach with EU standards, where appropriate, but fixes a general "APAC standard" that applies with limited exceptions across the region.

"Levelling up" to the "APAC standard" in jurisdictions without data protection laws often makes good business sense, given the obvious trend towards comprehensive regulation across the region. 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 neighbors.

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 the APAC region has a number of jurisdictions that are yet to implement comprehensive data protection legislation, the region 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 and, more recently, the introduction of the Cyber Security Law. The "new normal" for APAC region data protection compliance is setting an ever-increasing bar for compliance.

3. Cybersecurity regulation: ready to respond

Cybersecurity regulation is steadily introducing new variables to approaches to data management in the APAC region. The introduction of a comprehensive Cyber Security Law in China is an important development. Indonesia's Regulation 82 is forcing the same considerations there. India's draft data protection legislation contains a similar measure, allowing onshore-offshore "mirroring" of sensitive personal data, but requiring localization in specific cases of information considered critical by the central government.

These developments notwithstanding, cybersecurity regulation is still at an early stage of development in the APAC region and currently tends to focus only on regulated industries and critical infrastructure. Organizations focusing on cybersecurity will of course see it as an aspect of data protection (and potentially cybersecurity) compliance, but more fundamentally it is a matter of business risk across a range of risk areas: in particular operational, financial and reputational.

As data security breaches become more and more commonplace, and increasingly damaging to businesses, we see organizations moving towards greater formality in their cybersecurity preparations, including through undertaking detailed threat assessments, implementing preventive measures and preparing and testing incident response plans.

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, anonymization/aggregation principles and policies around "enhancing" datasets through the use of publicly available data or third-party datasets;

- Data commercialization, which looks more broadly for the potential use of the organization'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, addressing both data protection and cybersecurity concerns;
- 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 organization, 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 organization to assess privacy impacts due to proposals for organizational, technological or policy change.

Management oversight and review

Developing effective data protection and cybersecurity risk management policies and programs will involve engagement with the right stakeholders across the organization 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 cybersecurity 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 organization will be necessary in order to lend context and emphasize 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 organizational change is needed in response.

In order to be effective, an organization'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 APAC data protection and cybersecurity practice

An international perspective

At Hogan Lovells we bring an international perspective to advising clients on the APAC region's data protection and cybersecurity laws and the ongoing development of policy across the region. Our APAC region team includes practitioners who practiced data privacy law in Europe, and so bring a depth of experience to interpreting APAC region 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 APAC region team is closely integrated with our international team of data protection and cybersecurity 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 APAC 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 APAC region data protection and cybersecurity team is also closely integrated with other relevant specialists, in particular, lawyers engaged in commercial arrangements concerning data commercialization 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 cybersecurity compliance, including:

- Conducting data protection and cybersecurity compliance audits and developing policies, including integrating Asia policies with existing international policies;
- Helping client's 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, behavioral 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 cybersecurity 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 cybersecurity management team across the world in finding solutions that work in Asia based on lessons learnt elsewhere.

Key contacts in APAC

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

Tommy Liu
Senior Associate
T: +852 2840 5072
tommy.liu@hoganlovells.com

Anthony Liu
Registered Foreign Lawyer
T: +852 2840 5907
anthony.liu@hoganlovells.com

Sherry Gong
Partner
T: +86 10 6582 9516
sherry.gong@hoganlovells.com

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

Mandi Jacobson
Partner, Sydney
T: +61 2 9093 3502
mandi.jacobson@hoganlovells.com

Our APAC data protection and cybersecurity 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 cybersecurity 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 Cybersecurity 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, cybersecurity, 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 Cybersecurity practice spans the globe and all aspects of privacy, data protection, cybersecurity, 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 localizing 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 deployment of new data-driven technologies.

How we can help

We have had a team specializing in Privacy and Cybersecurity for over 25 years. Today Hogan Lovells has one of the largest and most experienced Privacy and Cybersecurity 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 Hogan Lovells Engage.

www.engage.hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
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
Riyadh*
Rome
San Francisco
Sao Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Centre: Berlin

www.hoganlovells.com