

```
..._array[a], u  
...[b.length - 1].b  
...reverse(); b = m(a  
(a, void 0); -1 <  
b && a.splice(b,  
...replace(RegExp("  
{ for (var c = 0  
c++; } ret  
d = 0; d <  
; } } ret  
b =
```

Asia Pacific Data Protection and Cybersecurity Guide 2020





Asia-Pacific data protection and cybersecurity regulation

2019 in review and looking ahead to 2020

It is no overstatement to say that 2019 saw a torrid pace of development of Asia-Pacific region data protection and cybersecurity laws.

Such was the rate and complexity of change that it is not straightforward to distil developments into simple themes. However, approaching data protection compliance from a regional perspective necessarily involves a quest to identify the bigger picture. We would point to the following as key developments of note:

- **Data protection with Chinese characteristics:**

China's progress towards clarity on its approach to data protection and cybersecurity regulation has not been straightforward. The cornerstone is the Cyber Security Law, which took effect in June, 2017 ("CSL"). But 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 2019, matters were further complicated by geopolitical trade tensions, with China's policies on data being an important point of contention. What is clear now, however, is that China is progressing towards a sophisticated model of private sector data protection regulation that draws from the European model, but at the same time implements China's cyber sovereignty imperatives in equal measure. It is also clear that there is growing public concern about data protection issues, such as the collection of biometric data and the harvesting of personal data from mobile devices. This development has started to influence regulatory developments and can be expected to continue to do so going forward.

- **Data protection 2.0:**

The European Union's introduction of the General Data Protection Regulation (the "GDPR") in 2018 continues to force a reassessment of the fitness for purpose of existing data protection laws in the region and, at the same time, provides a blueprint for jurisdictions introducing data protection laws for the first time. Established data protection regimes in the region, such as those in Australia, Hong Kong, New Zealand and Singapore, have been cherry-picking GDPR-led innovations, such as mandatory data breach notifications and obligations focused on ensuring greater accountability. Emerging data protection laws, such as those being introduced in India and Thailand, are poised to take a substantial leap from very limited regulation to GDPR-inspired comprehensive regulation. What is also clear from the implementation of new and amended laws is that the EU model, cast as it is in broad, principles-based terms, leaves significant room for local interpretation (or perhaps even misinterpretation) of GDPR principles. Superficially, there is now some harmonization of approach, but specific compliance requirements can vary significantly from jurisdiction to jurisdiction. 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 similar provision.

- **Enforcement? – call it a work in progress:**

2019 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 during the summer when two international airlines, British Airways and Cathay Pacific, faced separate enforcement action in respect of data security breaches. BA was fined 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, but the cracks are beginning to show. As the region's economies and public services are increasingly digitalized, the value and risk proposition for personal data changes dramatically. We are now beginning to see movement towards more proportionate regulatory action and accountability.

Data protection with Chinese characteristics

It is now over two and a half years since China implemented its Cyber Security Law, 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. It is clear enough that the impact on international business has been significant, and this is on-going. The uncertainty surrounding the law has in and of itself been sufficient to force businesses to make decisions now about their data processing and technology infrastructure in China.

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 Cyber Security Law's provision for data export review or "data localization" continues to weigh heavily on international business operating in mainland China. Two and a half years after the introduction of the Cyber Security Law, the export review process has not yet been elaborated. A further draft of the export review measures was released in June, but was not finalized. It is clear that the US-China trade tensions were brought to bear on the matter of data localization, and so we a respite through the second half of 2019. The potential extension of the data localization measure to "network operators", which was most recently intimated in the draft measures published in June, would effectively sweep in any and all businesses with operations on the ground in China. There had been some expectation that international businesses would continue to



have scope to connect HR and other internal systems to their international networks, and the export review could in the main be limited to self-assessment or reporting requirements, but none of this hoped for relief was apparent from the June 2019 draft of the implementing measures. The result has been a continuation of the “chilling effect” that has complicated compliance assessments for China since the Cyber Security Law was introduced, as some foreign businesses appear to be under the impression that the localization measures have already been implemented, forcing a localization of their data. We can only hope that 2020 brings greater clarity.

- **Exclusion of foreign technology:**

The intensive regulation of the information security of operators of critical information infrastructure is broadly in line with international developments in cybersecurity regulation. However, a key aspect for multi-national businesses is the extent to which regulations will (explicitly or by implication) close aspects of the Chinese market to foreign technology and services, at least in respect of key network infrastructure. Reports in December, 2019 that government agencies have been directed to replace foreign-supplied hardware and software by 2023 has heightened concerns in this area. At the same time, Chinese authorities have been publishing dozens of technical standards for network equipment, infrastructure and data management, amongst other data protection and cybersecurity-related topics. Concerns that China will impose specifications which only domestic technology providers can meet are a further concern.

- **Data and the commercial Internet in China:**

While the risk of data localization and the firewalling of the Chinese internet are the most eye-catching aspects of Chinese data protection policy from an international perspective, focus should also be given to China’s emerging policy in relation to data collection through the commercial internet. There is concern amongst online businesses in China that regulators may require a complete “unbundling” of data protection consents for non-essential data processing in areas such as analytics, profiling and retargeting, giving users the option to accept this processing or opt out from it. There can be no question that many online business models that drive the internet economy (in China and elsewhere) are based on “non-essential” data processing activities. For some time, the move towards unbundling was reflected only in the influential - but non-binding - national standard GB/T 35273-2017. On 30 December 2019, however, the unbundling requirement was introduced as binding law under directions to officials investigating mobile app compliance with the general data protection measures under the CSL. Watch this space.

Data protection 2.0

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 world-wide turn-over 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 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, 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 2019 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 Cyber Security Law in China has led to round after round of highly publicized investigation campaigns, with a particular focus in 2019 on online data collection by mobile apps. China’s telecommunications regulator, the Ministry of Industry and Information Technology (“MIIT”), launched a campaign against unlawful data collection by mobile apps in November 2019, ordering a first batch of 41 app operators to rectify non-compliance issues in December 2019. A second batch of 15 mobile app operators were ordered to rectify issues concerning personal information infringement in January 2020.

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 (“PCPD”), 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 PCPD’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 law-makers is coming, emboldened by the far larger scale of fines being awarded under the GDPR.

In March, the Australian government tabled proposals to increase maximum penalties for breaches of the Privacy Act, from A\$2.1 million (USD 1.4 million) for serious or repeated breaches, to the greatest of: (i) A\$10 million (USD 6.9 million); (ii) three times the value of any benefit obtained through the misuse of information; and (iii) 10% of annual domestic 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.

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 ₩10 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 co-ordinated 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 sign-posts 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.

What to watch for in 2020

We expect data protection and cybersecurity regulatory development to continue at a rapid pace during 2020.

Key initiatives to watch for:

- There is much anticipation surrounding the finalization of China's data export review measures as part of its implementation of the Cyber Security Law. There remains some optimism that the regime will provide scope for self-assessment of international data transfers below certain materiality thresholds and that there will be some form of a transition period allowing organizations time to achieve compliance. Given the importance of China's economy globally, clarity in this area would be highly beneficial.
- India's legislative debate towards a new data protection law will 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.
- 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. Law-makers 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.

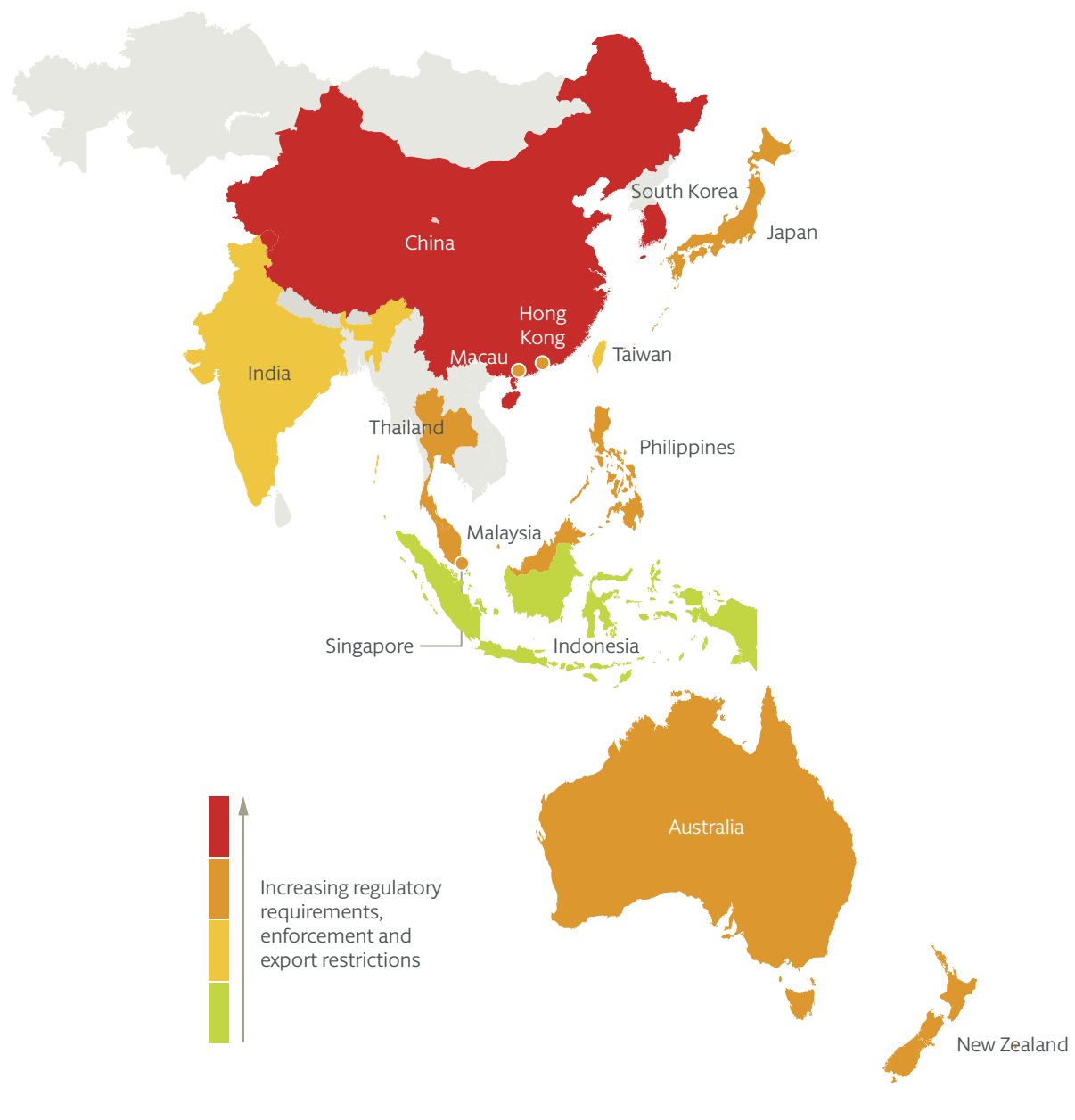


Asia-Pacific data protection regulatory heat map

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.

The Cyber Security Law

China's controversial Cyber Security Law came into effect on 1 June 2017. The focus here 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 OCII, 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.

The June 2019 draft of the implementing measures was not finalized and so significant uncertainty remains with respect to the scope and impact of Article 37. An administrative approval of each and every transfer of personal data from mainland China seems utterly infeasible. The necessity for such approvals has also not been made out.

With all the focus on the implementation of the Cyber Security Law, it is possible to forget 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.

Standard GB/T 35273-2017

Another important feature of the Chinese data protection landscape is the non-binding data protection standard issued by the Standardization Administration of China ("**GB/T 35273-2017**"), which came into effect on 1 May 2018. GB/T 35273-2017 provides a series of best practices for the collection, 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 Cyber Security Law, 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 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; and (ii) investigate whether or not the third party obtained data subject consent to the sharing of their 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.

GB/T 35273-2017 appears to be under near constant review by the authorities, with its third revision being considered at the end of 2019.

One of the most controversial areas of review under GB/T 35273-2017 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

1 December 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 introduces 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. In 2020 we can expect to see some important tensions play out, as China's technology sector presses for balance between data protection compliance and a viable commercial internet, and as the full extent of China's ambitions for its surveillance apparatus is made clear.

Hong Kong

Hong Kong's Privacy Commissioner for Personal Data (the "PCPD") remains a policy-making leader in the region. 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.

A data breach involving Hong Kong-headquartered Cathay Pacific Airways led to a highly publicized investigation by the PCPD in the summer of 2018. The fact that the airline had no obligation under the PDPO to report the data breach bolstered calls for the introduction of a mandatory data breach notification under the PDPO.

Hong Kong's protracted period of civil unrest through the second half of 2019 generated close to 5,000 reports of "doxxing", the unauthorized publication of individuals' personal data with the intent of intimidating or causing humiliation. Calls for granting the PCPD better tools to combat doxxing also supported the growing movement to reform the PDPO, in particular, to add new provisions directly addressing doxxing as misconduct under the PDPO, as well as related measures such as regulating data processors, which are currently not directly regulated under the PDPO, and introducing stiffer penalties for those who breach the PDPO, potentially with revenue-based fines tracking the GDPR.

The proposals for reform were presented to Hong Kong's Legislative Council in January 2020. Specific legislative reforms are expected to follow later in the year.





India

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

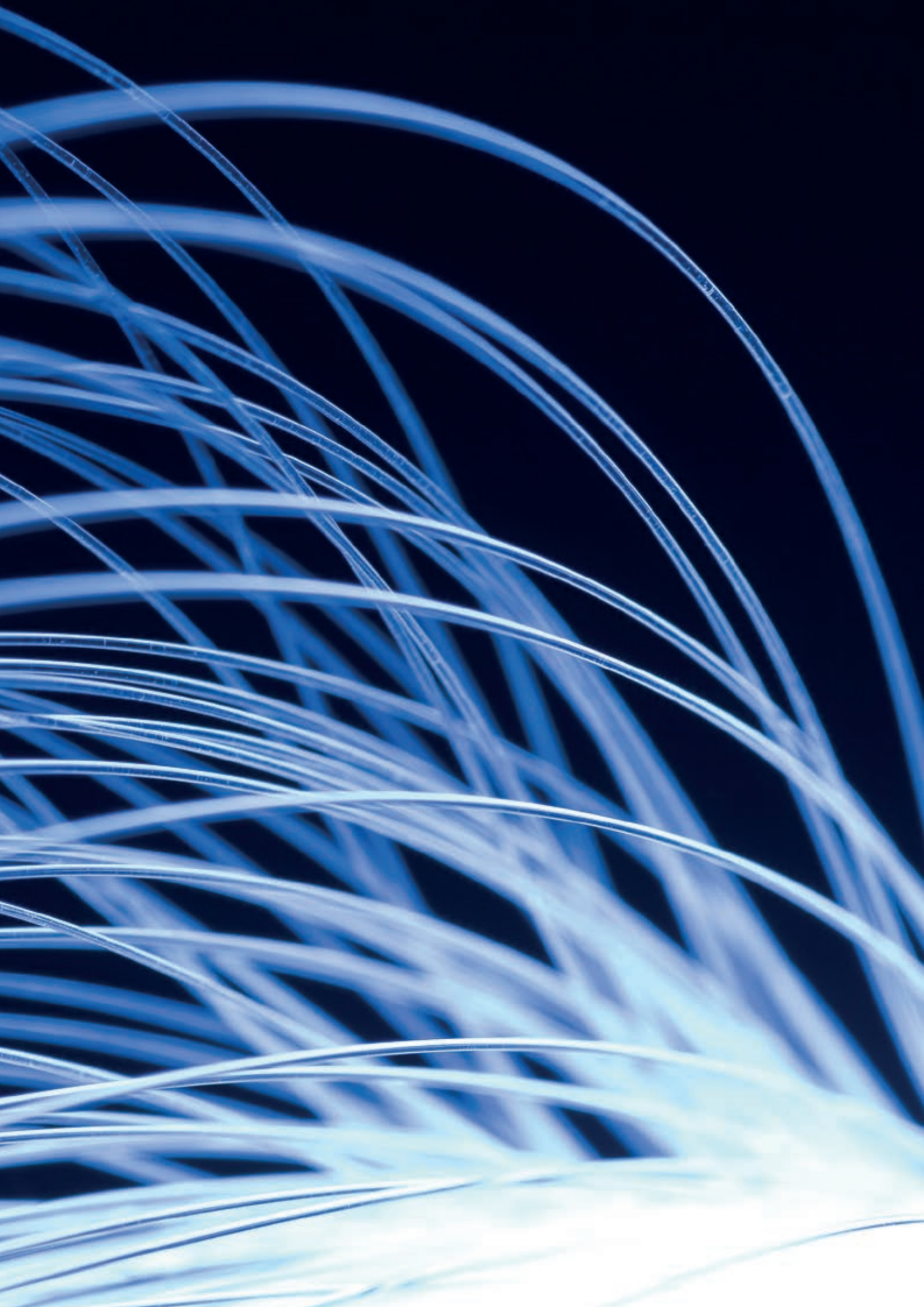
A legislative committee tabled the first draft of the law to the Ministry of Electronics and Information Technology (“**MEITY**”) in the summer of 2018. At the time, the scope and complexity of the draft law surprised many observers, charting a course for India that would involve its first data protection 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.

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 or, and to 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 behavioural 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.

We understand that a 20-person parliamentary panel has been struck to take feedback on the draft law from citizens, industry, law enforcement agencies and other groups. According to press accounts, the Indian technology sector has been particularly vocal about the changes. The offshore serviced industry lobby, the National Association of Software and Services Companies ("**Nasscom**") and the Internet and Mobile Association of India have both published concerns about the law in terms of its impact on data management costs in general, and the data localization measure in particular.

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**"). The authority has also been very active investigating complaints, most significantly with respect to the Singapore health system breach in 2018, which reportedly compromised the personal data of 1.5 million Singaporeans.

A number of key areas of reform are in train for 2020:

Mandatory data breach notification

obligation: Singapore currently has a voluntary data breach notification regime, but on 1 March 2019, the PCPD announced an intention to implement a mandatory breach reporting regime with respect to breaches which are either of a significant scale or are likely to result in significant harm or impact to the individuals to whom the information relates. Under the proposed mandatory regime (now reflected in the current voluntary regime), organizations would be required to notify individuals as soon as practicable and notify the PDPC as soon as practicable but no later than 72 hours of having knowledge of the breach, with a 30 day assessment period for suspected breaches (the 30 days running from when the organization or its data processor becomes aware of the incident). The notification obligation is subject to certain exemptions, including cases in which the data is encrypted and cannot be decrypted and cases in which remedial action was taken and the breach is unlikely to result in significant harm or impact.

Data portability: In January 2020, the PCPD published its response to feedback on a consultation in respect of proposed amendments to the PDPA concerning a right to data portability. The right would require organizations, at an individual's request, to transmit their personal data to another organization in a commonly used machine-readable format. The PCPD intends to proceed to implement such a right, but to limit the right to "white-listed datasets": i.e., specific categories of personal data specified by the PCPD in consultation with industry,

in order to bring clarity to the right and reduce the costs of compliance. The PCPD intends to publish guidance on the fees that organisations may charge in order to exercise their portability rights. The PCPD also indicated that it would likely implement the right to data portability on a phased basis with the publication of binding Codes of Practice in respect of specific industries.

Data innovation: The PDPC's January, 2020 consultation feedback also indicates an intention to proceed with a proposal to allow organizations to use (but not collect or disclose) personal data without consent for "business improvement" purposes. The exception is intended to enable organizations to use data to "improve business efficiency, product and service development to better meet consumers' needs". The PCPD intends to further clarify the scope of the exception and its interaction with the proposal in respect of legitimate interests processing and the consent exemption for research under the PDPA. In February 2018, the PCPD issued a Guide on Data Sharing, which invites organizations to apply to the PCPD for an exemption from data, subject consent requirements where data sharing is unlikely to have any adverse impact on the individuals and the benefits to the public (or a section thereof) of the sharing outweigh any adverse impact to the individuals.

Australia

Australia continues to review its Privacy Act, with fresh impetus in 2019 off the back of the Digital Platforms Inquiry led by the Australian Competition and Consumer Commission (the "ACCC"). The Office of the Australian Information Commissioner will be taking forward a recommendation to implement a new binding Privacy Code for digital platforms and increased penalties for privacy breaches, amongst other potential reforms, although there are reports that legislative reform of the Privacy Act will not be complete until 2021.

Australia has made significant moves to upgrade its Privacy Act in recent years, and the focus now appears to be to make the law fit for purpose for a rapidly advancing digital economy.

The ACCS's separate Consumer Data Right initiative promises a vision for consumer data sovereignty to improve competition across a range of industry sectors, including financial services and telecommunications. The API-powered vision of data portability is a striking move, but will of course raise the stakes from a data privacy point of view. With this in mind, the potential fines for breaches of the Privacy Act would increase from a maximum of A\$2.1 million (USD 1.4 million) for serious or repeated breaches, to the greatest of: (i) A\$10 million (USD 6.9 million); (ii) three times the value of any benefit obtained through the misuse of information; and (iii) 10% of annual domestic turnover.

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.

January 2020 saw amendments to PIPA, the IT Network Act and the Credit Information Use and Protection Act. Key amendments seek to help support South Korea's drive to continue to be an innovation economy. A key amendment will narrow 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 include the elevation of the Personal Information Protection Commission (the "**PIPC**") to the status of a central administrative agency reporting directly to the prime minister. The PIPC will have 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.

Vietnam

Vietnam's new Law on Cybersecurity ("**Cybersecurity Law**"), effective January 2019, has garnered much attention due to its sweeping attempt to regulate online content available to internet users in Vietnam. Among provisions most concerning to multi-national businesses, is the requirement that both foreign and domestic online service providers store personal data of Vietnamese end-users in Vietnam, surrender such data to Vietnamese government authorities upon request, and supervise user posts and remove "prohibited" content (defined to include content viewed as disparaging of the Vietnamese government and/or government officials or state agencies). The law also requires offshore service providers to open branches or representative offices in Vietnam, and meet certain data localization requirements, presumably to facilitate enforcement of the Cybersecurity Law against them.

Finalization of key implementing measures for the Cybersecurity Law, including the law's





data localization measures, has been delayed. Published drafts of the implementing measures suggest some narrowing of potential scope of localization, limiting localization of foreign service providers' data to cases in which the following three criteria are met: (i) localization is necessary for the purposes of national security, social order, social ethics or the health of the community; (ii) the organization in question carries out regulated services and processes specific categories of personal data identified by regulation; and (iii) the organization has failed to comply with official warnings to take measures to ensure that processing does not breach Vietnamese laws.

The categories of regulated services continue to be broad, but with a focus on telecommunications and messaging services, e-commerce, social media and online gaming.

Thailand

Thailand's long journey towards comprehensive data protection law will come to fruition on 28 May 2020, the date scheduled for the introduction of the Personal Data Protection Act (the "**Thailand PDPA**").

Key features of the new law include:

- **A dedicated authority:** The Thailand PDPA will establish a Personal Data Protection Commission, which will be under the supervision of the Ministry of Digital Economy and Society, which may signal a move to align the new authority with the industry regulator, much in the way Singapore has done with its PCPD.
- **Basis for processing:** The Thailand PDPA takes consent as the general basis for processing personal data, with consent being revocable and a requirement that data controllers not make consent conditional on the provision of goods or services. Relatively uniquely in the Asia-Pacific region, however, the Thailand PDPA permits legitimate interests processing as an alternative to consent. There are further exemptions to the consent requirement, including a public interest exemption and exemptions for necessity of contractual performance, law enforcement purposes and educational, research and statistical collection purposes.

- **Sensitive personal data and personal data of children:** The processing of “sensitive personal data” would require explicit consent. “Sensitive personal data” is defined to include data relating to ethnicity, race, political opinions, religious or philosophical beliefs, sexual behavior, criminal record, health data, genetic and biometric data and other data designated as sensitive by the regulator. The Thailand PDPA requires parental consent for processing of personal data of minors under 10 years of age.
- **Data protection officers:** The Thailand PDPA requires that foreign data controllers and data processors appoint a local representative in Thailand, unless they are not engaged in the processing of sensitive personal data or large amounts of personal data in general.
- **Data subject rights:** The Thailand PDPA incorporates an impressive array of data subject rights, including rights to access and correct personal data, a right to data portability, a right to object to processing or disclosure and a right to erasure/anonymization.
- **International transfer restrictions:** The Thailand PDPA would introduce an international transfer restriction which, bucking the trend for recently introduced laws, does not involve outright data localization. Organizations seeking to transfer personal data from Thailand would need to transfer the data to a "white list" jurisdiction or satisfy an exception, the list of exceptions, including data subjects' express consent, transfer under a data transfer agreement and transfer as necessary for the performance of a contract with the data subject.
- **Mandatory data breach notification obligation:** Thailand will follow others in introducing a mandatory data breach notification obligation, requiring organizations to notify the data protection authority without undue delay and in any event within 72 hours of becoming aware of the breach.

Japan

In April 2019, the Personal Information Protection Commission of Japan (the "PPC") published an interim report on its review of the Act on the Protection of Personal Information (the "APPI"). The interim report proposed that the APPI, which was last amended in 2017, be amended to introduce a mandatory data breach notification obligation, a right of data portability, strengthened regulation of cross-border transfers, stiffer penalties for contravention (including administrative fines) and the introduction of "big data" reforms concerning anonymization and the processing of pseudonymized personal data similar to reforms introduced in South Korea.

The interim report was followed by a final report in November 2019, which omitted proposals in relation to data portability and the potential for administrative fines. Clarity on the focus and substance of reforms is expected in the course of 2020.

Indonesia

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

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

Indonesia is now following the regional trend towards the introduction of comprehensive data protection legislation, with the introduction in January 2020 of a new bill concerning online data protection.



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 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.





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 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 cyber security 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 cyber security regimes proliferate and develop, however, there are more and more local distinctions that will need to be taken into account.

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 practised 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 clients structure and allocate risk in relation to cross-border data transfers, including as part of outsourcing, shared services and cloud arrangements;
- Advising on the acquisition of personal data as an increasingly important part of merger and acquisition and joint venture activity;
- Advising on data protection issues arising from online data capture, whether as part of electronic and mobile commerce, 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

Hong Kong



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



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

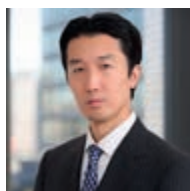


Tommy Liu
Senior Associate
T: +852 2840 5072
tommy.liu@hoganlovells.com



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

Japan



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

Shanghai



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

Beijing



Roy Zou
Office Managing Partner
T: +86 10 6582 9596
roy.zou@hoganlovells.com



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

Singapore



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



Matthew Bousfield
Counsel
T: +65 6302 2565
matthew.bousfield@hoganlovells.com

Vietnam



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



Our global privacy 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 our blog,

Chronicle of Data Protection
<http://www.hldataprotection.com>.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
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

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2020. All rights reserved. 1169698_0320