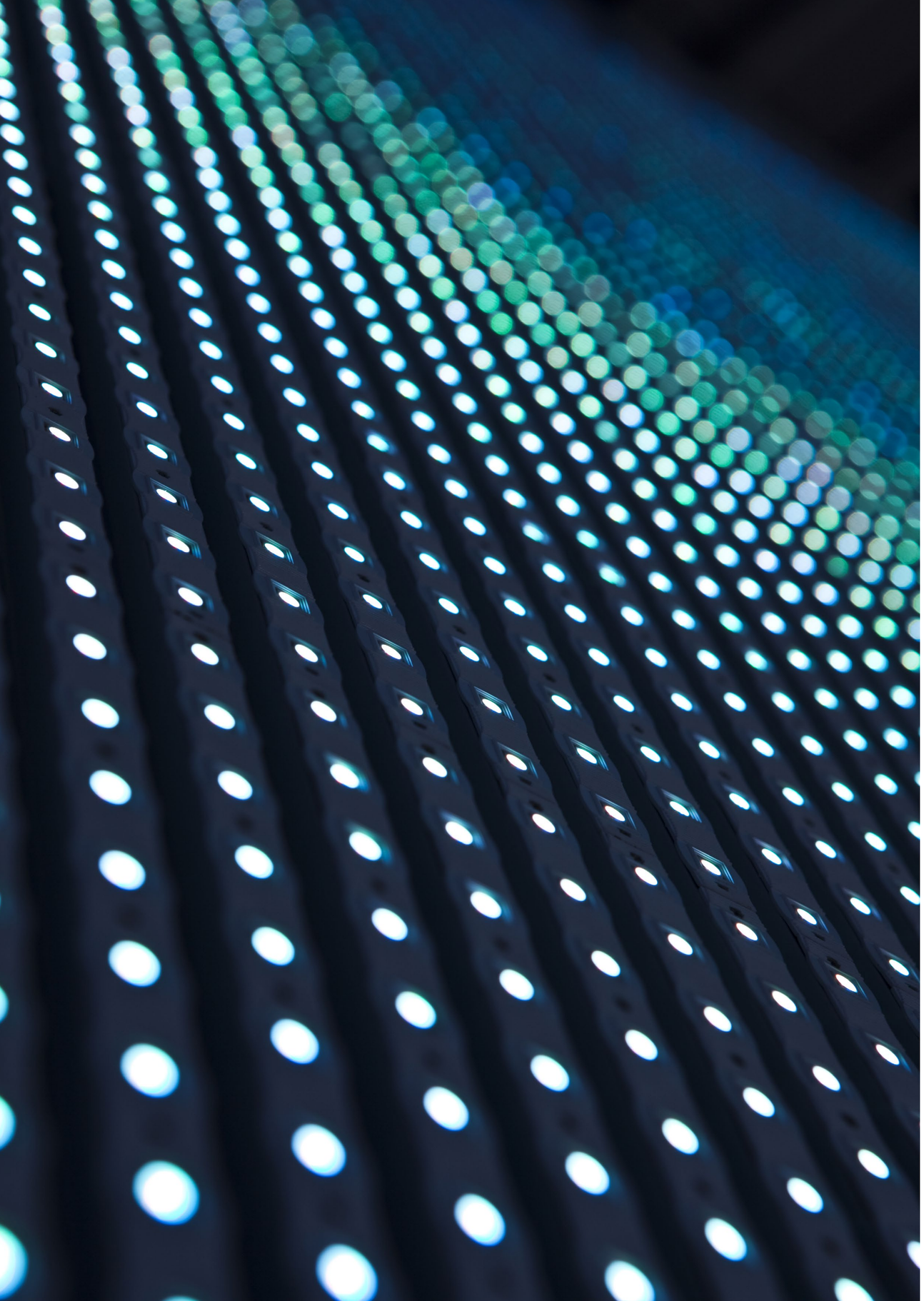
Asia Pacific Data Protection and Cybersecurity Guide **2022**

Hogan Lovells

Contents



Asia-Pacific data protection and cybersecurity regulation

2021 in review and looking ahead to 2022

The Asia-Pacific ("APAC") data protection regulatory landscape continued to develop rapidly through 2021, with much still to watch for in 2022.

The trendline in APAC is clearly towards stricter and more complex regulation, with China's introduction of two primary pieces of data regulation, the Personal Information Protection Law ("**PIPL**") and the Data Security Law ("**DSL**"), promising a new high water mark for data regulation in the region. India's move towards data protection regulation has been a case of two steps forward, one step back since the tabling of its Personal Data Protection Bill in 2019. There are, however, indications that 2022 will see the restyled bill, now addressing non-personal data as well as personal data, bring India closer to joining a growing club of major APAC economies with comprehensive, "European-style" data protection regulation.

Law-makers in China and India were not alone in pressing for more stringent data protection. In August, 2021, Japan issued guidelines concerning its most recent set of amendments to its Act on the Protection of Personal Information, taking effect April, 2022. In October, 2021, the Australian government published a far-reaching white-paper on privacy policy that suggest a significant update to the law is forthcoming. Thailand's Personal Data Protection Act, implementation of which was postponed due to the Covid-19 pandemic, is scheduled to take full effect 1 June, 2022. Hong Kong, Indonesia, South Korea, Sri Lanka and Vietnam all have legislative agendas featuring debate of papers proposing new laws or a stepping up of existing data protection laws in those jurisdictions.

The apparent convergence towards the European Union's General Data Protection Regulation ("**GDPR**") still leaves room for important local variations in data protection policy, reflecting individual jurisdictions' specific policy goals across a wide range of areas, including consumer protection, human rights, national security and economic development.

However, we are now at a stage where it is clear that organizations' data protection compliance programs should take direction from the "accountability-driven" model championed under the GDPR. There are so many points of compliance to manage, including data subject consents and notifications, the exercise of data subject rights and the satisfaction of mandatory breach notification obligations, that a piecemeal approach to compliance is becoming increasingly risky for organizations. The overlay of data governance through various measures, such as obligations to document data protection policies, carry out privacy impact assessments and implement privacy by design, mean that a holistic, organization-wide approach to compliance is needed. The compliance response demanded under these laws is increasingly sophisticated and complex, linked to a range of corporate functions and to organization-wide considerations of branding and corporate ethics. At present, the appointment of a data protection officer ("**DPO**") is only required under a few data protection laws in APAC, but the benefits of doing so are clear. Managing data protection compliance risk through a project management structure with designated points of accountability and appropriate management oversight significantly improves the organization's ability to avoid increasingly costly adverse publicity, investigations and fines.

While the diversity of developments across the region makes it increasingly difficult to distil themes across APAC, we see the following as key to understanding the current direction of travel:

China's move towards comprehensive data regulation

China's approach to data and cyber security regulation is the most striking feature of APAC region developments in recent years. China's vast population and the scale of its markets mean that its policies impact the region as a whole, particularly as organisations seek global or regional compliance programs as an efficient approach to compliance.

Data and cybersecurity compliance in China is now grounded in three laws: the Cyber Security Law, which took effect in June 2017 ("**CSL**"), the Data Security Law ("**DSL**"), which took effect in September 2021 and the Personal Information Protection Law ("**PIPL**"), which took effect in November 2021.

The promulgation of two important new data laws in 2021, namely, the DSL and the PIPL, represent a significant move towards comprehensive data regulation, not only in respect of personal data, but also in terms of non-personal data identified as having particular importance from the perspective of Chinese national security, economic strategy or other policy considerations.

The introduction of the DSL and PIPL signal a seismic shift in China's regulatory landscape, but specific requirements still remain unclear. While the Chinese authorities have published various implementing measures in the closing months of 2021, most of these arrived in draft form, leaving much to look out for in the course of 2022. The DSL, in particular, currently functions as a framework for future development of rules and requirements, tasking industry regulators with classifying data as "important" or "core" and promulgating specific restrictions on collection, use and transfer. Few industries have these classifications in place, leaving much uncertainty for businesses trying to asses impact on their China operations.

The PIPL has arrived with more detail as to its requirements, but has still left organisations with a watching brief.

Whilst at a high level, the PIPL closely tracks many of the principles found in European data protection model, China's policies towards "cyber sovereignty" are a differentiating feature that casts GDPR innovations such as extra-territorial effect in a different light, meaning that reference to corresponding requirements under GDPR may not be sufficient. Furthermore, some of the obligations imposed on organisations under the PIPL actually go above and beyond what is required under GDPR, such as the requirement to obtain a "separate consent" from data subjects before proceeding with international transfers of personal data. With no specifications as yet for standard contractual clauses or official review of international data transfers, organisations are left with no choice but to take a wait-and-see approach, carefully managing compliance requirements where they have been sufficiently specified.

Please see our Individual County Spotlight discussion on China for more details on these developments.

"Data protection 2.0": The new reference point for APAC

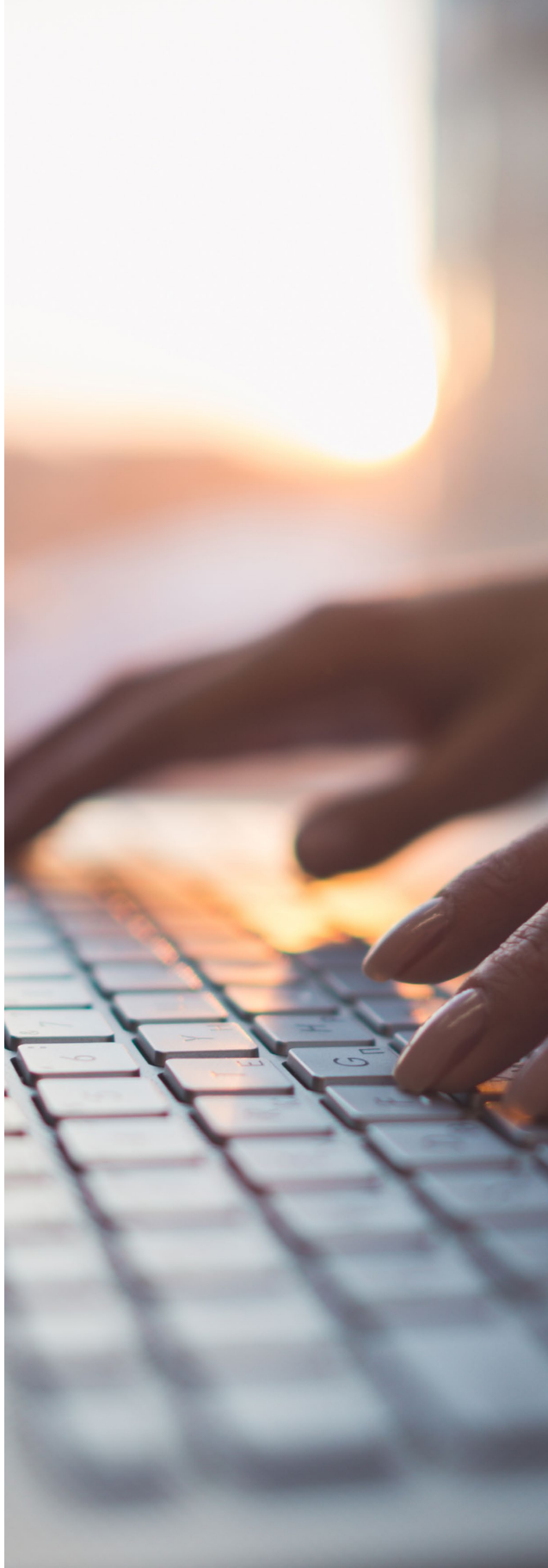
The GDPR, implemented in the EU in May 2018, continues to influence data protection policy development internationally, creating important reference points for APAC-based data protection compliance programs.

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 continue to see concerted effort by APAC businesses to better understanding the extent to which 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.

Depending on their particular circumstances, APAC businesses may be uncomfortable with a need to "firewall" the EU-facing aspects of their business, imposing GDPR standards only in respect of operations touching on the EU. With data protection compliance requirements in APAC on the rise and moving closer to GDPR standards, however, there is greater logic in moving to a global GDPR-based standard, perhaps creating exceptions where GDPR requirements represent a significant and unnecessary overreach when measured against the applicable APAC requirements.

APAC lawmakers' moves to reform their regimes to reflect this "version 2.0" upgrade of comprehensive data protection regulation is driving a significant change in thinking, with increasing numbers of organizations in APAC engaging data protection professionals as DPOs charged with developing and implementing comprehensive data protection compliance programs that achieve a sensible alignment of APAC requirements against GDPR standards.



The rising tide of enforcement

It is clear that the volume of data protection enforcement activity is on the rise in the APAC region.

In China, the introduction of the PIPL has further bolstered highly-publicized investigation campaigns, with a particular focus on online data collection by mobile apps. In particular, China's telecommunications regulator, the Ministry of Industry and Information Technology ("**MIIT**"), has launched several rounds of inspections against unlawful data collection and use of personal information by mobile apps. Since the start of 2021, the MIIT has stepped up enforcement and rectification efforts against the malpractices of Apps infringing on the rights of mobile app users. Structurally, the MIIT has organized 3 "look-backs" – i.e. phases of enforcement on key issues, with different focuses each time. In its most recent enforcement phase, the emphasis was placed on the excessive collection of personal information. A total of 55 mobile apps were ordered to rectify the non-compliance issues by the MIIT and the provincial Communications Administrations. A further 106 smartphone apps were ordered to be removed from China's app stores for data violations.

Emerging patterns across the region point to an uptick in enforcement, particularly as data breach incidents become increasingly publicized in the press and as mandatory breach notification obligations become the norm.

Historically, fines in the APAC region for data protection violations have been minimal. This appears to be changing. Amongst the largest reported fines in 2021 were those awarded by the Korea Personal Information Protection Commission, which fined a social media platform ₩6.46 billion (USD 5.4 million) for its creation and storage of facial recognition templates of users without consent.

Proposed amendments to Australia's Privacy Act would increase penalties to AU$10 million, three times the value of the benefit obtained through the misconduct, or 10% of annual turnover. This legislative development appears to track enforcement sentiment, noting that a telecommunications carrier was fined AUD 2.53 million (USD 1.8 million) by the Australian Communications and Media Authority in 2021, this fine, which related to data breaches, was the largest fine yet awarded in that country.

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.

The "new normal" of large-scale, revenue-based fines in APAC will make the costs of non-compliance increasingly significant.

Data protection compliance strategies for APAC

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

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

Smart data protection compliance in APAC, therefore, requires a local view. It also requires a regional view, given there is significant efficiency to be gained from developing a compliance program for APAC that reflects the rising "high water mark" 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.

What to watch for in 2022

We expect data protection and cybersecurity regulatory development to continue at a rapid pace during 2022.

Key initiatives to watch for:

- As the region's largest economy, China's fast-developing data protection landscape continues to be a key point of focus for business. A firm landing on international transfer regulation has been at the top of the wish list for three and a half years. The inclusion of extra-territorial measures in the new data protection laws raises another critical variable for multi-nationals. Continuing geopolitical tensions are very likely to influence China's program of regulatory reform, particularly now with the specific inclusion of counter-measures in the newly-introduced laws in response to discrimination against Chinese interests.
- Amendments to Hong Kong's data protection law – the Personal Data (Privacy) Ordinance (the "**PDPO**") – have become more likely in the course of 2022. We anticipate the amendments to cover the areas of reform that were previously proposed in 2020, including mandatory data breaches, regulation on data processors and increased fines and sanctions. Separately, 2021 saw an amendment to the PDPO that criminalizes doxxing acts (i.e. disclosing personal data for the purpose of shaming or intimidation) and empowering the semi-autonomous region's data protection authority, the Privacy Commissioner for Personal Data (the"**PCPD**") to perform criminal investigations and institute prosecutions for doxxing offences.
- The much-anticipated report on India's draft Data Protection Bill was published in December 2021. This new data protection law would set the stage for this increasingly significant economy asserting its influence on regional policy developments for the first time. However, the draft bill has generated significant disagreement over what the right balance is for India between data protection, data sovereignty and the freedom for technological innovation that cross-border data transfers can support. Given this controversy, coupled with the impact of the pandemic, it is difficult to say if or when the bill will be enacted.
- We expect events, data breaches locally and multi-million Euro fines in the EU, in particular, to continue to heavily influence the development of "Data Protection 2.0" reforms. 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.

Individual country spotlights

China

2021 saw a significant steps made in China's data protection framework, with the introduction and update of several substantive privacy and data-related laws and regulations.

The PRC Civil Code

First, we saw the enactment of the PRC Civil Code on 1 January 2021, which made explicit reference to the right of privacy and the lawful protection of personal information that must be afforded by the law. The term "privacy" was also specifically referenced and has been given an official definition (i.e. the "undisturbed private life of a natural person and his private space, private activities and private information that he does not want to be known to others").

The Cyber Security Law

The CSL came into effect on 1 June 2017, making it the cornerstone of China's current data protection and cyber security regulatory regime.

The focus under the CSL is not specifically on data protection, although the data protection measures found in the law remain important, even as the CSL has been largely supplanted by the PIPL in this regard.

Policy development under the CSL has led to concerns of over-regulation of technology in China. 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.

The implementation of MLPS 2.0 and the Draft Security Measures (discussed in more detail below) have added to the significant regulatory overheads in the technology sphere in China.

The CSL 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 CSL outlines the industries (including telecommunications, energy, transport and financial services) and state activities (public services and e-government) that form the law's focus. The classification and identification of OCII would be carried out in accordance with the CII Rules as discussed below.

NO have a far more open-ended definition, essentially encompassing any organization that operates a computer network in China, whether externally facing or not.

Since the introduction of the CSL, the threat of data localization has been a key concern for multi-national organizations. Article 37 of the CSL 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. 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. Draft measures published in 2017 suggested that the CSL would impose international transfer restrictions on NO as well as OCII, but these measures were never finalized. CSL, however, considers to be critical for multi-national organizations across a range of areas of cyber security compliance, such as steps needed to secure ICT functions in China. In this regard, there are important links between CSL compliance and China's Multi-Level Protection Scheme (MLPS), which was revamped in 2019, as discussed in the section below "MLPS 2.0".

The Rules on the Protection of the Security for Critical Information Infrastructure

The Rules on the Protection of the Security for Critical Information Infrastructure (the "**CII Rules**"), effective from 1 September 2021, provide guidance on whether or not an organization is OCII and requires OCII to only deploy network products and services that have completed a national security review.

When setting the standards for the identification of CIIs in different industries, industry regulators are required to consider the following:

- The degree of importance of the network facilities or information systems to the core business of the corresponding industry or sector
- The degree of harm that might be caused by the network facility's or information system's destruction, loss of function or data leakage
- Any other related impact on other industries or sectors.
- Some of the key obligations in relation to CIIs include the obligation to:
- design, implement and utilize security protection measures;
- establish a comprehensive security protection and accountability system;
- establish a specified security management body, which will be responsible for security protection works;
- carry out network security testing and risk assessment at least once a year; and
- report significant cybersecurity incidents to the relevant public security organs, etc.

Further, CIIs that store or handle information that involve State secret information are subject to certain State secret laws and regulations and CIIOs that utilize commercial encryption products are subject to relevant encryption regulations.

CIIOs found to breached the CII Rules are liable to provisional warnings, correctional orders, a fine of up to RMB 1,000,000 and a confiscation of revenue illegally obtained.

Personal Information Protection Law

The PIPL is China's first comprehensive data protection law, taking effect 1 November 2021. Drawing on the principles of the GDPR, the PIPL sets a high bar for Chinese data protection compliance. Some of the key features under the PIPL are as follows:

- **Bases for Processing:** Consent is the main legal basis for processing personal data (with specific exemptions for conclusion or performance of contracts with data subjects, HR management, compliance with applicable laws, public health and public interest processing). Notably, the PIPL does not follow the GDPR by providing a legitimate interests basis for processing without consent where obtaining consent is not practical. It is also important to note that the PIPL mandates a "separate consent" in respect of "controller-controller" transfers, with a plain reading of these words suggesting that an unbundled revocable consent (i.e., a separate tick box consent) is required. Organizations are also required to notify data subjects of the specific identity of transferees.
- **Sensitive personal data:** The PIPL introduces specific requirements in respect of the collection and handling of sensitive personal data, which unlike under GDPR, is not defined exhaustively but instead is defined as information which, if misused, could readily cause harm to the dignity or interests of impacted individuals. Personal data of children under the age of 14 is also considered sensitive. A "separate consent" is required before organisations may collect and use sensitive personal data, as well as completion of a form of privacy impact assessment.
- **Data subject rights:** Data subjects entitled to a range of data protection rights, which broadly mirror those under the GDPR (e.g. a right to request correction of data, the right to obtain a copy of their personal information, right to withdraw consent), but also includes a right to request an explanation of the organization's data processing practices. Pending clarification from the authorities, this may amount to something more than providing a data protection notification.
- **Extraterritorial effect:** The PIPL applies not only to organizations based in China, but also foreign organizations that process personal data of Chinese data subjects where the processing is for the purpose of: (i) providing services or products to individuals in China; (ii) analyzing or evaluating the behavior of individuals in China; or (iii) other circumstances provided under Chinese law. Organisations subject to the PIPL which do not have operations in mainland China are required to appoint a local representative.
- **International data transfers:** Organizations that transfer personal information outside of China are required to satisfy certain requirements, including: (a) conducting an authorized security assessment; (b) undergoing appropriate certification; (c) entering into standard contractual clauses; or (d) satisfying some other basis for the transfer under Chinese laws. In addition, organizations must obtain a separate consent from relevant data subjects and must also conduct a privacy impact assessment for such cross-border transfers. The frameworks for certifications and security assessments have not been established, nor has there been publication of the standard contractual clauses.
- **Accountability:** Organisations meeting as yet unspecified thresholds are required to appoint a DPO. In addition, Article 51 of the PIPL prescribes a set of potentially broad obligations requiring organisations to formulate internal management structures and operating procedures concerning personal data, undertake data classification, adopt security measures, formulate data security incident response plans and conduct security training for employees. There is no specific obligation to prepare and maintain a record of processing under PIPL, but we are finding that in practice a data inventory is essential to effective compliance.
- **Data breach notification:** When a data breach occurs, remedial measures must be immediately adopted. The corresponding government departments and the affected individuals must be notified in the manner prescribed under the PIPL.

- **Revenue-based fines:** Under the PIPL, fines of up to RMB 1,000,000 could be imposed on organizations, with fines of RMB 10,000 to 100,000 imposed on responsible individuals. In more serious cases, the fine could be increased to RMB 50,000,000 or 5% of the organization's annual revenue in the preceding year, with fines of RMB 100,000 to 1,000,000 imposed on responsible individuals.

The Data Security Law

The DSL, which came into effect 1 September 2021, provides a set of high-level national data security principles and policies, and the main elements of which are: (a) the establishment of basic mechanisms for data security management, such as data classification and management, data security risk assessment, monitoring, warning and emergency response; (b) the data security protection obligations of organizations and individuals carrying out data-related activities; (c) measures to support the promotion and development of data security; and (d) the establishment of mechanisms to guarantee the security of government data, and promote the openness of government data.

It is important to understand that, whereas the PIPL is concerned with the collection and processing of personal data, the DSL is concerned with "important data" and "core data", which may include personal data, but which are defined more directly by their importance to state interests rather than privacy.

The national data security working coordination mechanism, a procedure to be established by the national security agency under Article 5 of the DSL, will develop a catalogue of important data at the central level while local authorities and industry supervising authorities will in turn identify important data within their regulatory remits, as well as specify enhanced protections applicable to each category.

As matters stand, pending official guidance, it is difficult to understand in precise terms what "important data" is and how it will be regulated. We would note, however, the draft Data Security Administration Measures issued by the Cyberspace Administration of China in May 2019 (see the more detailed write up below) defines "important data" as data that, if leaked, could directly affect national security, economic security, social stability or public health and safety, such as unpublished government information, large scale population data, generic health data, geographic data or data relating to mineral resources. The definition of "important data" here is stated to not generally include business, production and operational information, internal management information or personal information. The Guidelines for Cross-border Data Transfer Security Assessment, which is also in draft status, provides guidelines on "important data" identification, defining the scope of important data based on different industries and regions.

The concept of "core data" was introduced to the DSL as a last minute inclusion, making its terms of reference even more scant than "important data". The DSL broadly defines "core data" as data related to China's national security, lifelines of the national economy, important people's livelihoods and vital public interests. The DSL provides that more stringent requirements will be developed in respect of core data.

The vagueness of the provisions relating to important data and core data has been troubling for multi-national businesses seeking to comply with the requirements of the DSL. However, it is important to understand that, in this regard, the DSL is more a framework for further regulatory development rather than a specific set of actionable requirements.

Notably, the DSL extends the geographic scope of Chinese data laws, applying to organizations or individuals outside China if they carry out data activities in such a way that may undermine national security, other public interests of China or the legitimate rights of any citizens or organizations in China. The DSL introduces extraterritorial regulation of data processing activities, a dimension not yet seen under the CSL, which has been understood to apply only to systems and technology physically located in mainland China.

Draft Security Assessment Measures

On 29 October 2021, the CAC published the draft Measures of Security Assessment of Cross-border Data Transfer (the "**Draft Security Assessment Measures**") for public consultation. The Draft Security Assessment Measures are subsidiary to all three of China's primary data and cyber security laws: the CSL, DSL and PIPL. If and when finalized, these measures will provide clarification on the practical requirements for cross-border data transfers from China.

Under the Draft Security Assessment Measures, organisations are required to apply to the CAC before transferring personal data or "important information" in the following circumstances:

- Any transfer of personal data or important data by OCIIs
- Any transfer of important data
- Any transfers of personal data by organisations that handle the personal data of at least 1,000,000 persons
- Cumulative transfers of personal data involving the personal data of more than 100,000 persons (or 10,000 persons in the case of sensitive personal data)
- As otherwise prescribed by the applicable authorities

Organizations are required to carry out self-assessments regarding data export risk and apply to the CAC via their provincial cybersecurity regulators. Applications may be rejected if the transfers are considered to be potentially harmful to national security or public interest or it lack effective safeguards.

If the proposed data export involves "important data", the provincial authorities may, under the Draft Security Measures, solicit the opinions of other relevant regulatory authorities. Approvals last for two years, except in cases where there are changes to the scope, volume or duration of the transfer.

Organizations that do not meet the thresholds referred to above are still required to undergo self-assessments regarding risks of the proposed transfer.

The Cybersecurity Review Measures

The Cybersecurity Review Measures ("CRM") were introduced on 28 December 2021 and officially took effect on 15 February 2022. The CRM provides the basis for cybersecurity reviews to be conducted. The CRM provides further details to the requirements under DSL, CSL and the National Security Law, reinforcing the interplay between network operations, data processing and national security priorities.

Under the CRM framework: (a) procurement by CIIOs of network products and services (e.g. important telecommunications products) that have a potential impact on national security; (b) data processing activities conducted by NOs that may impact national security; and (c) proposed listings outside China conducted by NOs that control over 1,000,000 users' personal information, are subject to the regulatory regime and are required to conduct cybersecurity reviews in accordance with the CRM.

For the purpose of the cybersecurity reviews, the Office for Cybersecurity Review will take into account, amongst other factors, the risk of CIIOs being illegal controlled and manipulated, the risk posed to network information security, the threat to supply channels due to political, diplomatic or trade factors, etc.

Personal Information Security Specification

The non-binding data protection standard entitled "The Information Security Technology - Personal Information Security Specification" issued by the Standardization Administration of China ("**GB/T 35273-2020" or the "Personal Information Security Standard**") continues to be useful as an interpretive tool for the data protection requirements under the PIPL and CSL. The Personal Information Security Standard came into effect on 1 May 2018, with subsequent amendments coming into effect 1 October 2020.

The Personal Information Security Standard provides a series of best practices for the collection, processing, retention, use, sharing and transfer of personal information and for the handling of information security incidents.

The standard has been read by regulators and law enforcement officials as important elaboration of a number of the general principles concerning data protection stated in the CSL, in particular, adding some important glosses on expected best practice:

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

The App Rules

On 12 March 2021, the Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications (the "**App Rules**") was jointly issued by the CAC, the MIIT, the SAMR and the MPS. The introduction of the App Rules came amidst the wave of other sweeping changes made throughout the year, highlighting another effort by the Chinese authorities to rein in what it considers to be excessive collection of personal data in the mobile and consumer internet space.

The App Rules identified 39 types of common mobile internet applications and set out the scope of necessary personal data that these apps may collect. The types of apps include, among others, maps and navigation, instant messaging, online payment and shopping, marriage and dating, housing rentals, etc.. In the 39 categories listed, the App Rules specified that 13 of them did not require personal data for the performance of basic functions. For the other categories, the scope of necessary personal data varies depending on the app's basic functions. The App Rules also prohibit network operators from refusing application access as well as basic functions and services to users if users do not agree to provide non-essential personal data.

MLPS 2.0

In addition to the CSL, China maintains a tiered cyber security grading regime referred to as the Multi-Level Protection Scheme ("**MLPS**") administered by the Ministry of Public Security ("**MPS**"). Revamped in 2019 following the introduction of the CSL, "MLPS 2.0" requires organizations to self-assess their cyber risk against a five tier grading system. Organizations having a risk rating of 3 are required to report their status and self-assessment to the authorities, implement cybersecurity monitoring, detection and incident response programs, and make incident notifications to relevant bodies, amongst other requirements.

More broadly, however, MLPS 2.0 includes a series of technical standards which all organizations of whatever grading are expected to comply with, addressing a wide range of issues, from cyber security governance through to specific technical requirements for ICT infrastructure and data management.

MLPS 2.0 introduce 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.

Hong Kong

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

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

It is expected that these reforms are to be discussed and finalized as part of the Legislative Council's 2022's legislative session.

Proposed Legislative Changes

The PDPO Review Paper focuses on the following areas:

- **Mandatory Breach Notification Obligation:** At present, the PDPO requires data users to take all practicable steps to prevent unauthorized or accidental access of personal data. However, unlike an increasing number of laws internationally, the PDPO does not include an obligation to notify the PCPD or impacted data subjects if this provision has been breached. This lack of lack of a breach notification requirement was heavily publicized following the PCPD's investigation of a substantial data breach by Cathay Pacific Airways. The PDPO Review Paper proposes a mandatory breach notification, which would require further formulation on: (i) how a "personal data breach" is defined; (ii) the threshold for notification; (iii) the timeframe for notification (which was proposed to be done as soon as practicable and in not more than 5 business days); and (iv) the method of notification (the PCPD seemed to consider a formal written notification to be a more appropriate mode of notification). A key challenge for the proposed notification obligation is to strike a balance between alerting the PCPD of data breaches whilst avoiding "notification fatigue".
- **Data Retention:** The PDPO's data protection principles require data users to ensure personal data is not kept longer than necessary for the fulfilment of the purposes of collection, but does not specify when the personal data is "no longer necessary". The PDPO Review Paper recommends amending the PDPO to require data users to develop clear personal data retention policies, covering the maximum retention period for different types of personal data, the legal requirements that may affect those retention periods and how those retention periods are calculated.
- **Fines and Sanctions:** At present, the PCPD may issue an enforcement notice requiring a data user to remediate its breach of the data protection principles. A breach of an enforcement notice may result in a Level 5 fine (HK$50,000) (approx. USD 6500) and imprisonment for two years on first conviction. To increase the deterrent effect of these fines, the PDPO Review Paper proposes to increase these fines and to allow the PCPD to issue administrative fines.
- **Regulation of Data Processors:** Currently, the PDPO only regulates data users and not data processors, but the PDPO does require data users to ensure that data processors adopt measures to protect personal data. The PDPO Review Paper goes further and proposes regulatory oversight directly over data processors.
- **Definition of Personal Data:** The PDPO Review Paper proposes to expand the definition of "personal data" to include data that relates to an "identifiable" natural person as opposed to the currently definition of an "identified" natural person. This would cover more categories of data, for example, tracking and behavioral data generated by big-data tools.

Anti-doxxing provisions now in effect

The Personal Data (Privacy) (Amendment) Ordinance 2021 came into effect in October 2021, effectively criminalizing "doxxing" acts - i.e., the practice of disclosing personal data for the purpose of shaming or intimidation - a phenomenon which intensified during the political unrest in Hong Kong over the past few years.

Under these new provisions, malicious disclosure of personal information without the data subject's consent constitutes an offence can attract up to a fine of HK$1,000,000 and to imprisonment for 5 years. The severity of consequences vary, depending on whether "specified harm" is caused to the data subject – i.e. bodily or psychological harm as defined under the Amendment Ordinance.

In addition, statutory powers are conferred on the PCPD to require the removal of doxxing-related content and to conduct criminal investigations and prosecutions powers. The amendments have extra-territorial effect, whereby non-Hong Kong based service providers could now be asked to comply with the PCPD's rectification orders.

Before these amendments, the PCPD had previously referred doxxing cases to the Hong Kong police or the Department of Justice. With its new investigatory and prosecution powers, the PCPD made its first ever doxxing-related arrest on 13 December 2021.

Enforcement

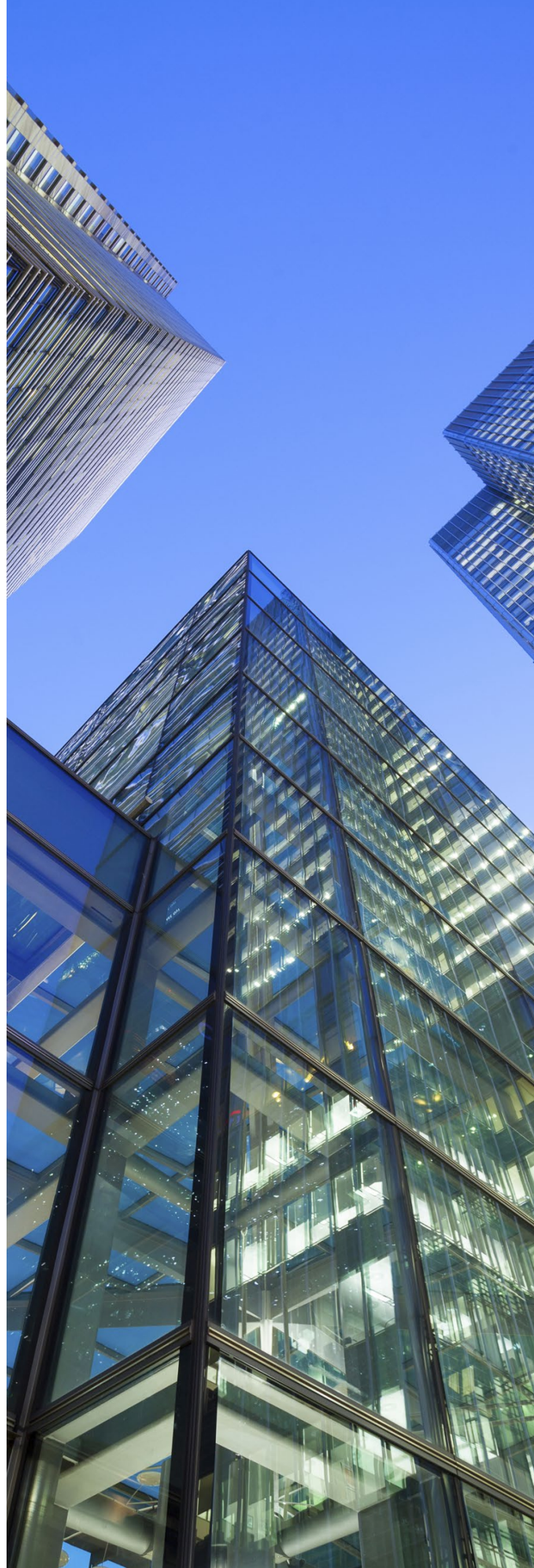
Over the past year, the PCPD received 3,157 complaints, with doxxing-related cases accounting for approximately 30% of all complaints lodged with the PCPD. The numbers reflected a 71% drop from the year before.

India

After nearly two years of deliberation, India's parliamentary committee released the long-awaited report on the Personal Data Protection Bill 2019 (the "**Bill Report**"), together with an updated draft of the proposed law on 16 December 2021, with the new version of the law styled as the Data Protection Bill 2021 ("**2021 Bill**"). The 2021 Bill builds upon many of the core elements found in its predecessor, whilst also expanding beyond what was originally envisaged.

The 2021 Bill is expected to be enacted in the course of 2022. However, there continues to be significant debate surrounding various provisions of the law, in particular its application to government authorities and exemptions relating thereto. Reportedly, eight members of the Joint Parliamentary Committee that authored the Bill Report have dissented to the report itself.

As India's population is expected to be the largest in APAC in a few years and the country is likely to emerge as a significant economic force regionally, its data protection framework will be a critical bell weather for regional policy-making.



Key elements of the 2021 Bill include:

- **A dedicated authority:** The 2021 Bill would establish the Data Protection Authority of India (the "Indian DPA"), which would serve as a dedicated data protection regulator, which is a key indicator for measuring the likely seriousness of intent for a new data protection regime.
- **Extra-territoriality:** Drawing inspiration from GDPR, the 2021 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. Several of the provisions contained in the 2021 Bill apply to non-personal data as well, as discussed below.
- **Regulation of non-personal data:** The scope of the 2021 Bill will be expanded to include "non-personal data" (i.e. data that is not identifiable with individuals). This likely includes databases and anonymized personal data. This proposed revision is certainly unprecedented in the world of data protection laws, as no other country has such a blanket regulation over non-personal data. Accordingly, organizations that leverage non-personal data would likely be significantly impacted if and when the provision comes into effect.
- **Wider powers for the Government:** The 2021 Bill provides the Indian authorities with a broader range of powers and exemptions, including the power to exempt governmental agencies from the application of the 2021 Bill on the basis of, amongst other grounds, national security, state sovereignty and public order. This exemption can only be exercised in compliance with a "just, fair, reasonable and proportionate procedure".
- **"Significant data fiduciaries" and data protection officers:** The 2021 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 2021 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 2021 Bill requires informed data subject consent to the processing of personal data, subject to prescribed exceptions. Consent is revocable under the 2021 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. Amendments to the 2021 Bill provide some scope for legitimate interests processing in specific circumstances, specifically where non-sensitive personal data is processed for necessary employment purposes and where processing is necessary for reasonable purposes as may be specified by regulations.

- **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 2021 Bill separately includes measures directed at processing personal data of children (defined as those under the age of 18), requiring the consent of a parent or guardian and prohibiting profiling, tracking and behavioral monitoring of children. Under the 2021 Bill, data fiduciaries that process the personal data of minors or provide services to minors would automatically be characterized as "significant data fiduciaries" and be subject to stricter requirements. Moreover, all processing must be done to protect the rights of children, which differs to the approach in an earlier draft of the bill that focused on "acting in the best interests of the child".
- **"Reasonable purposes" processing:** The 2021 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 2021 Bill would provide data subjects with rights of erasure and portability. Data subjects also have the right to nominate legal representatives or heirs to exercise certain rights in the event of his or her death.
- **Privacy by design policy:** The 2021 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 2021 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 2021 Bill would require organizations to notify the Indian DPA as soon as possible and not later 72 hours of becoming aware of the data breach. It is noteworthy that amendments to the 2021 Bill would mean that the notification obligation applies to non-personal data as well as personal data.

  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. These breach notification requirements are also required for data breach incidents involving non-personal data.
- **Social media platforms:** The 2021 Bill incorporates specific regulations for social media platforms. A key area of international focus is the designation of platforms controlling content as "publishers" responsible for user content. These platform operators are required to verify accounts and set up an office in India if they have not already done so.

- **Data protection impact analysis:** The 2021 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 the data transfer restrictions in the 2021 Bill. The 2021 Bill restrictions apply 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 and obtaining the government's prior approval; or (iii) as otherwise permitted by the Indian DPA, which would be required to consult with the government before giving out such approvals. 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 2021 Bill has generated significant concerns.

Singapore

Singapore's push to be a leading innovation economy in APAC is reflected in its particular approach to the regulation of personal data under the Personal Data Protection Act (the "**PDPA**") as well as in the thought leadership of the Personal Data Protection Commission (the "**PDPC**"). In some ways, Singapore is an outlier against the trend towards stricter data protection across APAC seen in China's recent moves and the direct taken by Indian lawmakers. Singapore's emerging data protection policy, with broader exceptions to data subject consent than any other jurisdiction in APAC, is more supportive of businesses seeking to innovate through the collection and use of personal data.

The Personal Data Protection (Amendment) Bill (the "Bill"), passed by Parliament on 2 November 2020, proposed significant changes to the PDPA, focusing on four key themes: (1) strengthening accountability; (2) relaxing consent requirements; (3) increasing consumer autonomy; and (4) increasing deterrence and strengthening enforcement powers. Most of the amendments came into force on 1 February 2021, with different parts of the Bill being implemented in later phases in 2022.

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

Mandatory Data Breach Notification Regime

A mandatory data breach notification requirement was introduced in the Bill and the regime will cover data breaches which result in, or are likely to result in, significant harm to an affected individual, or which is of a significant scale (i.e. data breaches that affect 500 or more individuals). The organization concerned will be required to notify the PDPC and, if necessary, affected individuals following a data breach. There are various scenarios in which an organization need not notify the individual, including where sufficient remedial action has been taken, or the data is sufficiently encrypted.

Subsequent legislative amendments have made clear what "significant harm caused by data breaches" entail – significant harm includes "severe physical, psychological, economic, financial and other forms of harms that a reasonable person would identify as a possible outcome of a data breach". In practice, that may include those which compromise sensitive categories of personal data, such as social security numbers, drivers' licence numbers, credit/debit card numbers, health insurance information and medical history information.

Extended Deemed Consent Provisions

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

Under the first limb, consent will be deemed to have been given when the data subject voluntarily provides his or her personal data to the organization for a specific purpose and it is considered reasonable that the data subject would have done so. The onus here is wholly on the organization to prove and demonstrate that the data subject is indeed aware of the purpose for data processing.

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

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

Exceptions to the Consent Requirement

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

A "legitimate interests" exception was introduced to enable organizations to collect, use or disclose personal data where it is in the legitimate interest of the organization and where the benefit to the public outweighs any adverse effect to the individual.

This is very similar to the legitimate interest concept enshrined in the GDPR and will work to ensure IT and network security, as well as prevent illegal activities such as fraud and money laundering.

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

Data Portability Obligation

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

A number of exceptions to the data portability obligation will be introduced. One of the key exceptions will relate to data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organization. The right will also be limited to "white-listed datasets", being specific categories of personal data specified by the PDPC in consultation with industry. The data portability obligation has yet to take effect and is anticipated to come into force in the course of 2022.

Increased Deterrence

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

Whilst the PDPC will remain focused on holding organizations accountable for data protection, this move to directly criminalize the mishandling of personal by data by individuals is an important development in the safeguarding of personal data. Individuals found guilty of an offence will be liable upon conviction to a fine of up to SGD 5,000 and/or imprisonment for up to two years.

This would include employees who act in contravention of an employer's policies or act outside their scope of employment; as such, the role of the Data Protection Officer (mandatory for all entities in Singapore, regardless of size or operations), along with staff training and protocols, are likely to be given far more thought by Singapore organizations.

The maximum financial penalty under the PDPA will also be increased to the greater of 10% of an organization's annual turnover in Singapore where such turnover exceeds S$10 million, or in any other case, S$1 million.

Australia

2021 saw the Australian federal government continue to review and develop proposals to significantly reform its data protection laws in two parallel tracks: (i) the publication of in October 2021 of a Privacy Act Review - Discussion Paper" addressing potential amendments to the Privacy Act; and (ii) the publication the same month of an exposure draft exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (the "Online Privacy Bill").

Taken together, the measures chart a course towards a significant uplift in data protection requirements for Australia.

Much attention has been focused on proposals to increase the fines that may be awarded under the Privacy Act, which are currently capped at A$2.22 million in relation to corporations committing 'serious' or 'repeated' offences. Under the proposed reforms, fines would be increased to the greatest of:

(a) $10 million;

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

(c) 10% of a company's annual domestic turnover in the 12 months preceding the misconduct.

The scope of reforms currently in play in Australia is, however, much wider than just enhanced penalties, with proposals to remove the Privacy Act's exemptions for small businesses and processing of personal data in the employment context and proposals to expand the definition of personal data to include certain categories of technical data and online identifiers. The Online Privacy Bill would extend the Privacy Act to apply to overseas entities operating in Australia and mandate an online privacy code for social media platforms, data brokers and large online platforms.

The legislative developments track an increasingly assertive data protection authority in the Office of the Australian Information Commissioner ("OAIC"), which has commenced a number of high profile public sector and private sector investigations in recent years, including cases that are testing the extraterritorial scope of the Privacy Act in relation to foreign technology companies.

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.

South Korea's rigorous approach to data protection is reflected in the European Commission's adoption, in December 2021, of a finding that South Korea has broadly equivalent standards of data privacy protection, meaning that there are no additional requirements for transfers of personal data from the EU to South Korea (such as the use of standard contractual clauses or binding corporate rules).

The PIPA is well known for its requirement of separate, unbundled consents for a number of data collection and processing contexts, including international transfers of personal data, and the need to notify data subjects of the specific identity of data processors. Relatively uniquely for the APAC region, the PIPA does provide some scope for "legitimate interests" processing of personal data without data subject consent.

However, the practical scope of this exception is very limited, applying only in cases where the data controller's legitimate interests clearly override the rights of the data subject. Official guidelines provide that 'the preparation of supporting materials for the collection of service fees or the collection of debts, and the commencement or continuation of legal action are examples of what may constitute a 'legitimate interest.'

Japan

On June 12, 2020, the Japanese government announced substantial amendments to the Japanese Act on the Protection of Personal Information ("APPI"), requiring companies to take certain additional measures to protect personal data of data subjects. The amended version will come into effect on 1 April 2022, with the exception of the amendment to the updated penalties and the cross-border transfer opt-in requirement, which took partial effect since late 2020 and 2021 respectively. The amendment aims to broaden data subjects' powers to exercise control over their data and to establish a system to facilitate corporations' internal use of "big data". The update comes as part of the Japanese government's commitment to update Japan's privacy law every three years.

In May 2021, the Japanese government announced further amendments to the APPI, which aims to integrate the standalone pieces of data protection legislation in relation to government bodies, national institutions and other administrative institutions and to harmonize them with the APPI.

In August 2021, Japan's Personal Information Protection Commission ("PPC") published guidelines to the 2020 amendments of the APPI, which provide clarity on the regulatory approach to be adopted in practice. Key provisions in the 2020 amendments and the PPC's guidelines include:

- **Expanding rights of data subjects:** The update aims to broaden the right of data subjects, making it easier for data subjects to request that a data handler cease use of or delete stored data. Further, the amendments broaden the scope of retained data which a data handler must disclose to a data subject upon request regardless of the retention period (at present, data retained for less than six months is subject to fewer restrictions).
- **Pseudonymization:** The amended APPI introduces the concept of "Pseudonymously Processed Information", as the conditions to anonymize personal information are very strict under the APPI so that it is hardly feasible to rely on anonymization. Data handlers can utilize pseudonymized data in limited circumstances, while obligations of dealing with data subjects' rights such as for disclosure and cease of utilization will be eased. Obligations of Pseudonymously Processed Information handlers are set out in greater detail under the PCC Guidelines.
- **Mandatory breach reporting:** The updated APPI makes it mandatory for data handlers to report a data breach to the PPC and the affected data subjects. The PPC guidelines clarify when mandatory reporting requirements are triggered under the new regime. The guidelines also specify the measures to be undertaken in the event of such data breach incident.
- **Revising and strengthening of penalties:** An entity may now be punished with a fine of up to 100,000,000 JPY (about USD 1 million) in case of violation of an order from the authority or illegitimate use of data.
- **Extraterritorial applicability:** The PPC will be granted authority to request foreign entities which supply goods or services in Japan and handle personal information of individuals in Japan to submit reports or to issue orders in case of violations of the APPI by foreign entities, which can be enforced with a penalty.
- **Cross-border transfer:** The amended APPI sets out the conditions for cross-border transfers. Data handlers that wish to transfer data outside of Japan must obtain the data subject's consent (the "opt-in requirement"), and the data exporter must conduct appropriate due diligence and describe the "personal information protection system" (i.e. data protection laws) of the receiving countries. The PCC guidelines provide further guidance on how data exporters can fulfill the requirements under the amended APPI.

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 amongst 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 be very 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 can be 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, but the overall gap between APAC requirements and GDPR is narrowing.

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 have seen China and India move quickly towards advanced data protection regimes and we expect, for example, new laws to emerge in Indonesia and Vietnam in the coming years. It is very likely 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 PIPL, DSL and CSL. 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 data security law, including the PIPL, the DSL and the CSL 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

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

Tommy Liu
Counsel, Hong Kong
T: +852 2840 5072
tommy.liu@hoganlovells.com

Anthony Liu
Foreign Registered Lawyer, Hong Kong
T: +852 2840 5613
anthony.liu@hoganlovells.com

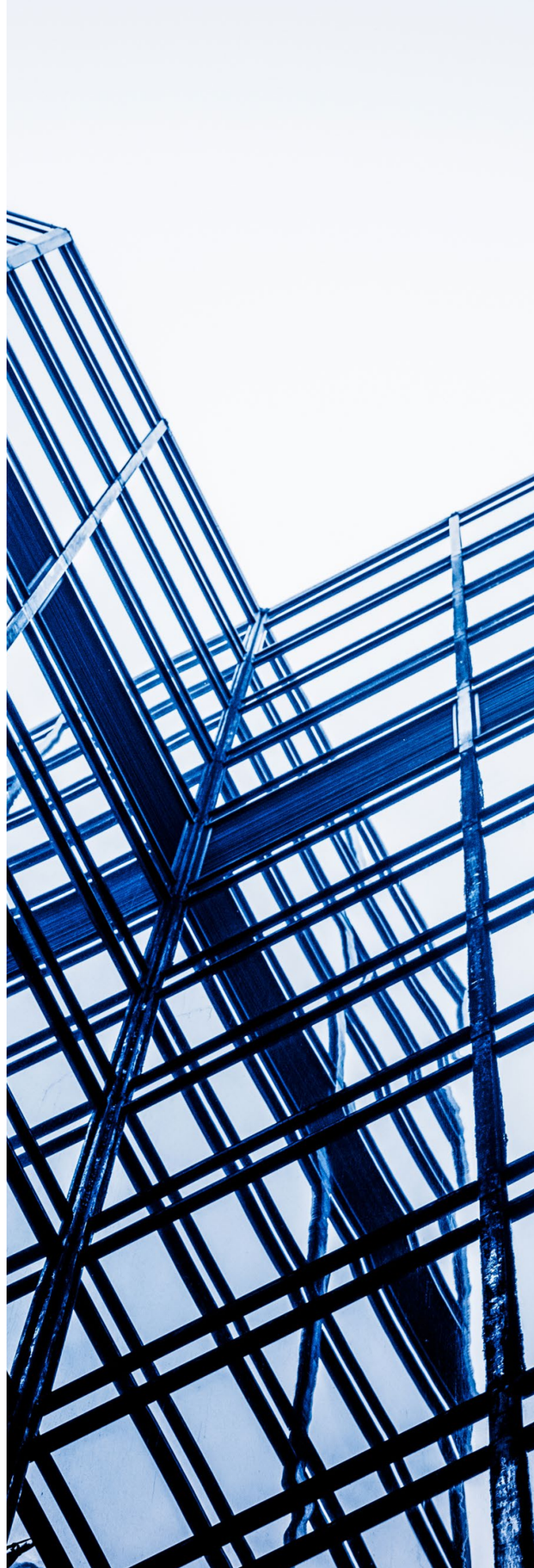
Sherry Gong
Partner, Beijing
T: +86 10 6582 9516
sherry.gong@hoganlovells.com

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

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

Gaston Fernandez
Office Managing Partner,
Hanoi, Ho Chi Minh City
T: +84 28 3829 5100
gaston.fernandez@hoganlovells.com

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



Our APAC data protection and cybersecurity practice

Realizing the true value of data

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

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

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

What we offer

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

Our focus and experience

The Hogan Lovells Privacy and Cybersecurity practice spans the globe and all aspects of privacy, data protection, cybersecurity, and information management.

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

How we can help

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

Chronicle of Data Protection

(http://www.hldataprotection.com)

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

*Our associated offices Legal Services Centre: Berlin
**Progressing with a wind down of operations in Moscow

www.hoganlovells.com