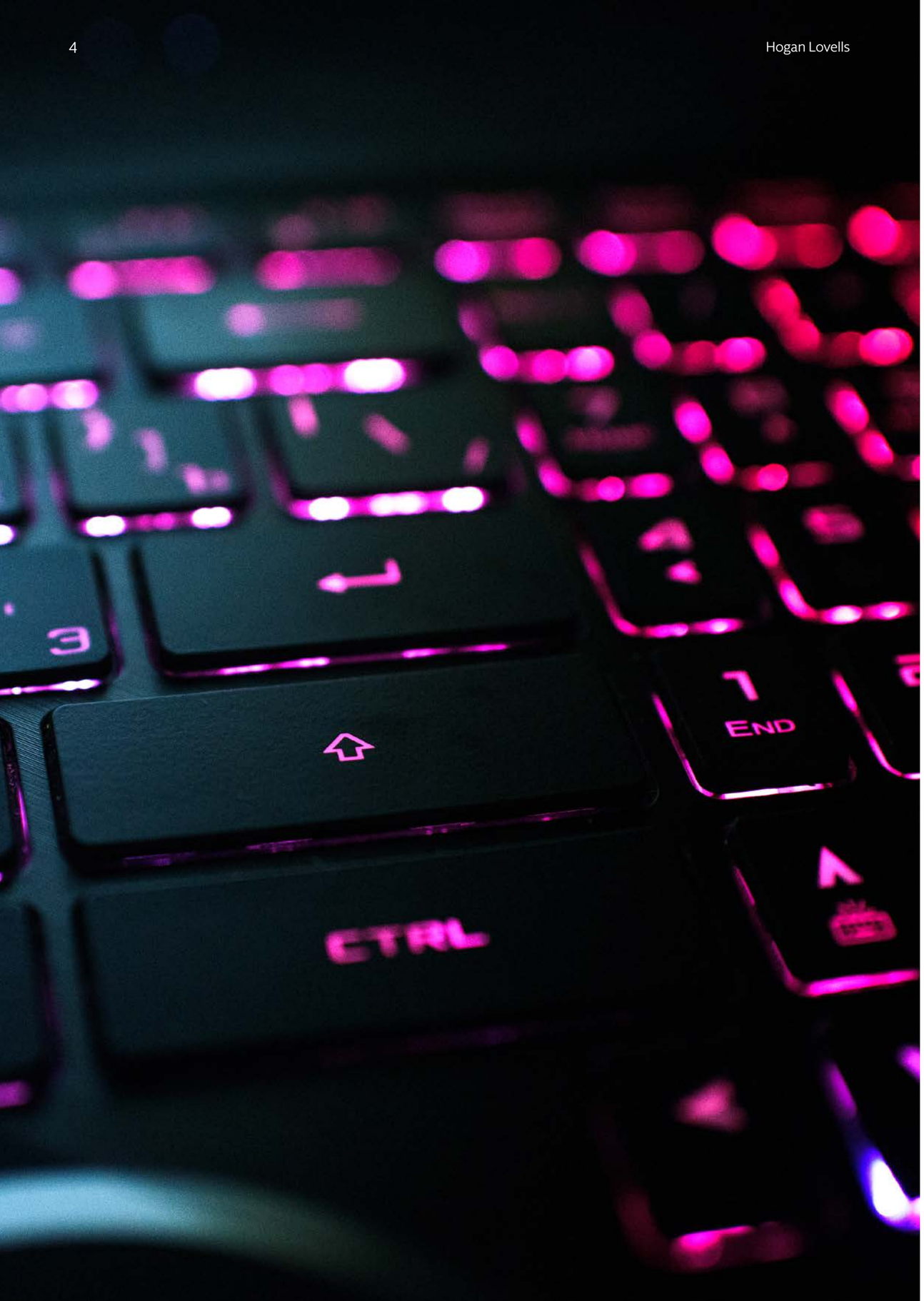
Hogan Lovells

Asia Pacific Data Protection and Cybersecurity Guide **2023**

Contents



Asia-Pacific data protection and cybersecurity regulation

2022 in review; looking ahead to 2023

Data protection and cyber security regulation in the Asia-Pacific ("**APAC**") region continued to develop at a rapid pace through 2022, with China's Personal Information Protection Law ("**PIPL**") in particular establishing a new reference standard for organizations to meet, with wider implications for the region. As discussed in more detail in this guide, a number of other jurisdictions also implemented key changes in regulation that have driven higher compliance standards to the region, but the scale of the Chinese economy, the comprehensive scope of PIPL compliance requirements and the law's extra-territorial effect mark out the moves in China as being particularly critical for businesses.

PIPL is, in a number of respects, modelled closely on the European Union's General Data Protection Regulation ("**GDPR**"), requiring organizations to take a holistic view of data protection compliance and implement a range of internal policies that, taken together, amount to a broad program of organizational data governance. The compliance effort under GDPR and PIPL is not just a matter of completing specific compliance tasks, such as preparing data protection notices, and adhering to broadly framed principles, such a applying appropriate security to data. Under the evolution of data protection law that GDPR and PIPL represent, organizations must undergo a cultural change that characterizes data protection compliance as a key management competency and places data protection at the heart of organizational risk management.

As clear as it is that PIPL has its roots in GDPR, the recent changes in Chinese law must also be considered in the context of China's focus on "cyber sovereignty" and the equally comprehensive nature of its cyber security regulation. Many jurisdictions moving to implement cyber security regulation limit the law's scope of application to "critical infrastructure" such as telecommunications networks, securities trading platforms and other systemically important infrastructure, requiring operators to adopt and certify against specific cyber security standards, share information about cyber incidents with regulators and develop specific cyber security competencies within their ranks. Under China's 2017 Cyber Security Law ("**CSL**") (supported by the 2019 revamp of its Multi-Level Protection Scheme ("**MLPS**")), a wide range of organizations operating in mainland China must comply with specific technology risk management standards, make reports to regulators and assist law enforcement in the investigation of crime. At present, the most important intersection of PIPL with cyber security laws is seen in the regulation of cross-border data transfers, specifically the security assessment program implemented by the Cyberspace Administration of China ("**CAC**") in September 2022, which requires organizations meeting certain data volume thresholds to obtain approval of their transfers, an administrative process requiring the submission of significant volumes of information and materials describing the transfer and the data protection and cyber security environment in which the transfer will take place.

It is fair to say that PIPL implementation has not proceeded at the pace that some expected. While lawyers interpreting GDPR have the benefit of volumes upon volumes of interpretative guidance and years of legal and administrative precedent, the situation under PIPL is very different. Apart from the CAC security assessment measures referred to above, PIPL continues to be an under-specified law whose requirements are vague and poorly understood even a year after its introduction. PIPL compliance has been supported in practice in areas where the law borrows quite literally from GDPR. For example, the CAC has not yet issued detailed guidance with respect to PIPL's privacy impact assessment framework or a data subjects rights program. However, these are two areas where the text of PIPL appears to closely track GDPR requirements, creating an opportunity to leverage international learning and approaches to documentation. Where PIPL departs significantly from GDPR, such as its numerous requirements for "separate consents", we see organizations focusing on understanding the approach taken by industry peers and in many cases taking more of a "wait and see" approach pending clearer direction from regulators.

China's economic headwinds in the months following PIPL implementation appear to have blunted some of the sharp edges of PIPL implementation.

China's Covid-19 measures and geopolitical tensions seem to have restored some focus on China's needs for foreign investment and job creation. We do not expect that most foreign multi-national businesses will experience a sharp tightening of compliance requirements under PIPL any time soon. However, the overall direction under PIPL, CSL and MLPS are clear enough, and we do recommend that appropriate compliance measures be taken and organizations be ready for what may come. We also see that developments in China have created fresh impetus for organizations across the APAC region to step up their data protection compliance programs.

China was not the only jurisdiction to challenge organizations with data protection and cyber security reforms in 2022. As discussed in more detail in the sections that follow:

- In April 2022, new data protection measures took effect in Japan, including the introduction of extra-territorial application, a mandatory data breach notification obligation and an expanded range of data subject rights.
- In June 2022, Thailand's Personal Data Protection Act took full effect, bringing comprehensive, GDPR-inspired regulation to the country for the first time.
- In October 2022, Indonesia enacted its Personal Data Protection Law, a GDPR-inspired replacement for a number of separate instruments regulating personal data.
- In October 2022, the Singapore government increased maximum fines under the Personal Data Protection Act to the greater of S$ 1 million and 10% of annual turnover in Singapore for organizations with annual local turnover exceeding S$10 million.
- In December 2022, Australian lawmakers amended the Privacy Act to increase maximum penalties for serious or repeated privacy breaches from the current AUS$2.22 million penalty to the greater of:
  - AUS$50 million (US$ 33 million);
  - three times the value of any benefit obtained through the misuse of information; or
  - 30 per cent of an organization's adjusted turnover in the relevant period.

A number of jurisdictions are developing new data protection laws or proposing significant amendments to existing data protection laws, including:

- Vietnam's Ministry of Public Security has announced a draft decree on data protection, with plans to introduce a new law on data protection in 2024.
- Australian government completed a full review of the Privacy Law, proposing a number of sweeping reforms.
- Hong Kong's government announced plans to follow through with a number of reforms to its Personal Data (Privacy) Ordinance first proposed in January 2020, including the introduction of a mandatory data breach notification obligation and the regulation of data processors.
- In October 2022, the Malaysian government proposed the introduction of a mandatory data breach notification obligation to its Personal Data Protection Act.
- India's long road towards data protection reform took an abrupt turn in 2022, with the August shelving of a 2019 reform bill and its replacement in November with a much-abbreviated bill focused on digital personal data protection.

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

The recent developments in APAC data protection laws noted above suggest there is significant cross-region movement towards GDPR standards, but this 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.

It is clear, however, that organizations' data protection compliance programs should take direction from the "accountability-driven" model championed under 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, meaning 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 establishing such a role 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.

The rising tide of enforcement

The importance of data protection compliance in APAC is underscored by the increasing volume of data protection enforcement activity in the region.

Perhaps the most eye-catching development in APAC data protection enforcement in 2022 was the July announcement by China's CAC that a leading Chinese ride-hailing service had been fined RMB 8 billion (USD 1.2 billion) for breaches of the CSL, DSL and PIPL across a range of issues, including unlawful collection of smartphone images and excessive collection of location tracking data. The decision to fine the service reportedly followed a yearlong investigation, during which time the company's apps were suspended from Chinese apps stores.

In September 2022, South Korea's Personal Information Protection Commission issued its largest ever fines, imposing penalties on two leading US technology companies equivalent to US$ 50 million and US$ 22 million, respectively, in connection with default privacy settings that assumed users were willing to share their personal data with third party sites.

The scale of fines in these three cases go far beyond what has been typical to date in the APAC region. It is noteworthy that the relevant authorities in China and South Korea have the discretion to base their fines on percentages of business turn-over, an innovation introduced by the EU in GDPR. Recent moves by Singapore, Australia and the Philippines follow the same approach, as to proposed reforms to Hong Kong's Personal Data (Privacy) Ordinance.

We can expect a "new normal" of large-scale, revenue-based fines in APAC, making the potential 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. The introduction of PIPL in China has brought the GDPR reference point closer to home. Extending a GDPR-based 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 to compliance 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 2023

We expect data protection and cybersecurity regulatory development to continue at a rapid pace during 2023.

Key initiatives to watch for:

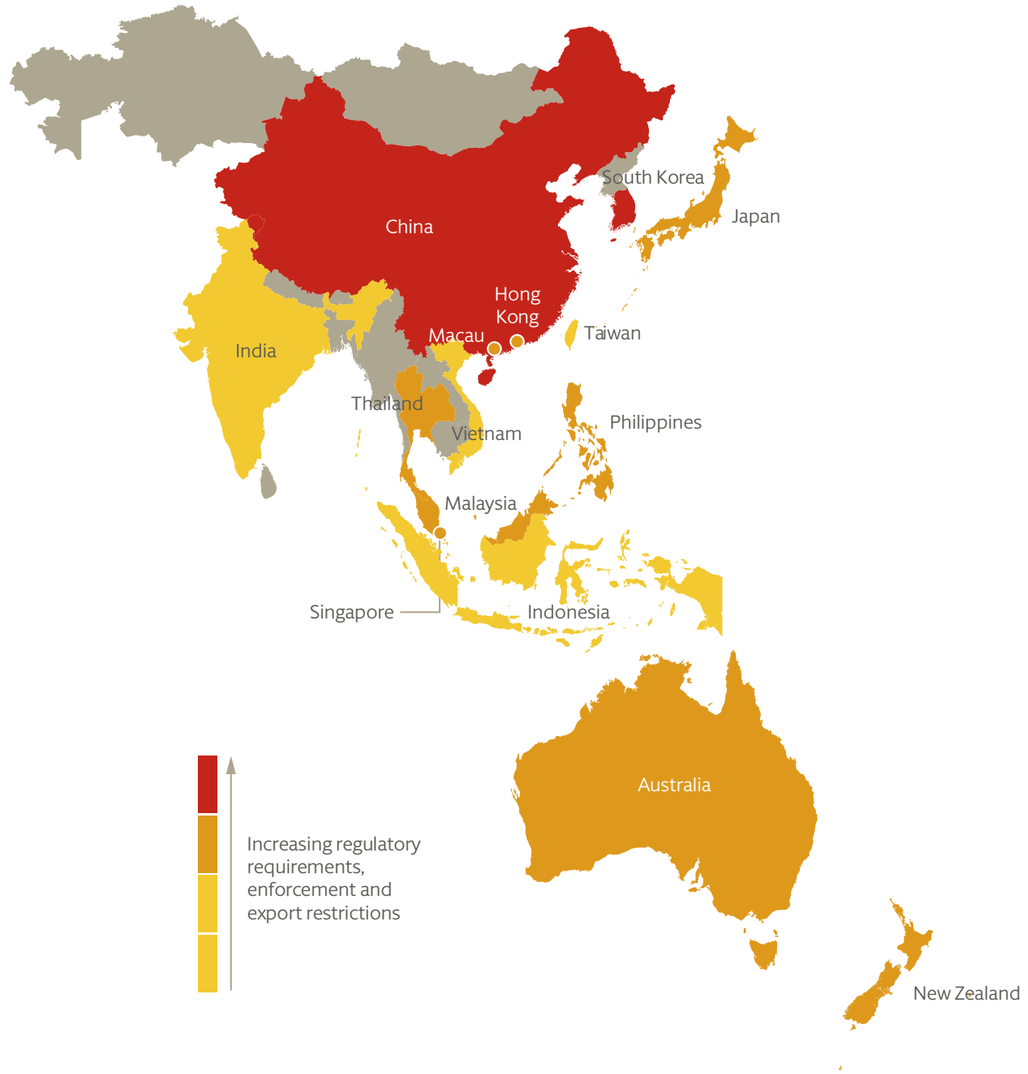
- Although we are now over a year into the implementation of China's PIPL, there is a continued lack of clarity in a number of key areas, including challenging requirements in respect of "separate consents" and the low uptake of CAC security assessments of cross-border data transfers. PIPL's extra-territorial effect is another critical area in which foreign multi-nationals are seeking greater certainty.
- India will continue to be a jurisdiction to watch in 2023, with the first round of comments on the new Digital Data Protection Bill having closed in December 2022. Given the slow pace of legislative development under the predecessor bill, many observers are reluctant to speculate on the likelihood that the bill will move forward in 2023. However, given the growing importance of India, whose economy is expected to overtake Japan's and become the region's second largest as early as 2030, many organizations will be focused on the approach taken here.
- Long awaited amendments to Hong Kong's PDPO have become more likely in the course of 2023. We anticipate the amendments to cover the areas of reform that were first proposed in 2020, including mandatory data breaches, regulation on data processors and increased fines and sanctions.
- The introduction of data breach notification obligations and revenue-based fines to data protection laws in Australia, Singapore and the Philippines may mean that 2023 is the year in which data protection fines in the tens of millions of US dollars become the new normal.

Asia-Pacific data protection regulatory heat map

Our Asia-Pacific Data Protection Regulatory Heat Map is a graphic representation of the relative stringency of the various data protection regulatory regimes across the region

The map below compares the various regimes in Asia-Pacific by grading jurisdictions against four criteria:

1. data management requirements;
2. data export controls;
3. direct marketing regulation; and
4. the aggressiveness of the enforcement environment. More challenging jurisdictions are represented as red, with less challenging ones appearing as green.



Individual country spotlights

China

China's unique 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 organizations 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 CSL, which took effect in June 2017, the Data Security Law ("**DSL**"), which took effect in September 2021 and the PIPL, which took effect in November 2021.

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. Companies across a range of sectors fear that the policy direction under CSL could force them to establish separate operating platforms in China making use of local technology if foreign technology is considered to raise national security concerns.

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 (discussed in more detail below) has 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**").

There is no exhaustive definition of OCII, with the authorities ultimately having the discretion to designate organizations as such. 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 is 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.

In practical terms, CSL compliance is heavily guided by requirements under China's Multi-Level Protection Scheme (**MLPS**), which was revamped in 2019, as discussed in the section below "MLPS 2.0".

MLPS 2.0

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.

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 OCII 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 OCII 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, OCII 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.

OCII 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

PIPL is China's first comprehensive data protection law, taking effect 1 November 2021. Drawing on the principles of GDPR, PIPL sets a high bar for Chinese data protection compliance. Some of the key features under 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, PIPL does not follow GDPR by providing a legitimate interests basis for processing without consent where obtaining consent is not practical. It is also important to note that 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**: 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 organizations 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 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:** 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. Organizations subject to 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. Please see the discussion of the security assessment measures below for further information.
- **Accountability:** Organizations meeting as yet unspecified thresholds are required to appoint a DPO. In addition, Article 51 of PIPL prescribes a set of potentially broad obligations requiring organizations 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 PIPL.
- **Revenue-based fines:** Under 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 CSL is primarily concerned with the regulation of ICT infrastructure and networks in China and PIPL is focused entirely on the regulation of personal data, the DSL is concerned with "important data" and "core data", which may include personal data, but are more likely to be non-personal data identified as such by reference to their importance to state interests rather than privacy.

A key feature of DSL is the national data security working coordination mechanism, a procedure for the development of catalogues 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.

Pending clarification through the classification of "important data" envisaged by the DSL, organizations find it difficult in practice to understand whether or not they are processing important data.

In January 2022, the National Information Security Standardisation Technical Committee (also known as TC260) published a draft non-binding guideline on the identification of important data (the "**TC260 Guideline on Important Data**"). The TC260 Guideline on Important Data follows previous draft guidance in stating that, as a general concept, important data is data that, if leaked, could directly affect national security or other public interests. However, this new guideline states that important data is electronic data and will not generally include business, production and operational information, internal management information or personal information. The TC260 Guideline on Important Data sets out a number of categories of information that could be important data based on the state and public interests engaged:

- Defense interests, including information relating to:
  - National strategic reserves and emergency mobilisation capabilities, for example., strategic material production capacity and reserves;
  - Information that may be used to launch military attacks against China;
  - Confidential information of defense contractors and other government vendors;
- National security interests, including information relating to:
  - The physical security of key infrastructure and assets, for example., design information, information on internal structures, the security of important enterprises or national assets (such as railways and oil pipelines);
  - The operation of critical infrastructure or industrial production in key fields.
  - Security measures which protect critical information infrastructure, for example, network security plans, system configuration data, core software and hardware designs, system topology and emergency plans.
  - Supply chains for critical equipment and system components that could be used to mount a cyber-attack, for example, important customer lists and undisclosed vulnerabilities.
  - Export-controlled items, for example, design principles, technological processes and production methods for such items.
  - The production and use of equipment that may become subject to sanctions by foreign governments, for example, financial transaction data of key enterprises, production and manufacturing information of important equipment or equipment used in the construction of major national projects and other activities.
  - The operations of government and government agencies, including intelligence agencies, law enforcement and the courts, including unpublished statistics.
  - Intellectual property rights related to national security (or national defense interests) and other scientific and technological information affecting China's international competitiveness.
- Strategic economic interests, i.e. information relating to:
  - The health and physiological status of certain population groups and genetic information, for example, population census data, human genetic resource information and gene sequencing data.
  - Natural resources and environmental data, for example, unpublished hydrological observation data, meteorological observation data and environmental monitoring data.

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, at this stage 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.

Cross-Border Data Transfer Regulation

On 31 August 2022, the CAC finalized the security assessment application guidelines and template application form (the "**Security Assessment Application Guideline**") under the Measures for Security Assessment of Outbound Data Transfers (the "**Security Assessment Measures**").

Under the Security Assessment Measures, from 1 September 2022 organizations are required to apply to the CAC before transferring personal data or "important data" 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 organizations that handle the personal data of at least 1,000,000 persons
- 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) since 1 January of the preceding year
- As otherwise prescribed by the applicable authorities

Organizations are required to carry out a self-assessment 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. Remediation was expected to be completed by 1 March 2023.

The Security Assessment Application Guideline requires applicants to submit a significant volume of information in support of the self-assessment report and present conclusions that risks have been identified and appropriately mitigated. Many organizations responding to the application process have reported that the information being requested by the CAC includes sensitive details of the security environment in the destination jurisdiction, raising significant difficulties.

Organizations that do not meet the security assessment thresholds referred to above are still required to undergo self-assessments regarding risks of the proposed transfer and must either:

- enter into the CAC's Standard Contractual Clauses for the Cross-border Transfer of Personal Information ("SCCs"), which were finalized 24 February 2023; or
- obtain a certification by a third party professional institution.

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 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.

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.

In a briefing to Hong Kong's Legislative Council (Hong Kong's legislative body) on 20 February 2023, the PCPD announced that the long-awaited amendments to the PDPO will be introduced in the first half of 2023.

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.

India

Comprehensive data protection regulation has been a long time coming in India. India's Ministry of Electronics and Information Technology ("**MeitY**") had brought forward the Personal Data Protection Bill 2019 for legislative consideration. The 2019 bill was very much a comprehensive data protection law which borrowed liberally from GDPR. After a challenging legislative debate which saw the bill revised in 2021, the bill was finally withdrawn in August 2022. December 2022 saw the introduction of a Digital Data Protection Bill 2022 ("**2022 Bill**") which is notably slimmer than its predecessors, representing a significant narrowing of scope and ambition when compared to the original proposals.

As its title indicates, the 2022 Bill only concerns itself with digital data regulation, whether that data is collected online or collected offline but subsequently digitized. Key elements of the 2022 Bill include:

- **A dedicated authority:** The 2022 Bill would establish the Data Protection Board of India ("DPBI"), which would be responsible for enforcement. As proposed in the 2022 Bill, details of the qualifications and composition of the board will be determined by executive order.
- **Extra-territoriality:** Drawing inspiration from GDPR, the 2022 Bill would regulate all digital personal data collected or processed within the territory of India, processed by any Indian organization and to the processing of digital personal data outside India, provided such processing is undertaken for the purpose of:
  - 'profiling' or processing personal data specifically to 'analyze or predicts aspects concerning the behavior, attributes or interests' of an individual in India;
  - offering of goods or services to individuals in India.
- **"Data fiduciaries" and "Significant data fiduciaries"**: The 2022 Bill would regulate "data fiduciaries", which are defined in similar terms as "data controllers" under GDPR. The 2022 Bill would require that data fiduciaries assessed to be "significant" (based on the volume and sensitivity of data processed) to 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.
- **Basis for processing:** Like its predecessor bills, the 2022 Bill requires informed data subject consent to the processing of personal data, subject to prescribed exceptions. However, the 2022 Bill appears to provide for relaxation from previous drafts, with scope for deemed consent, including deemed consent where data subjects voluntarily provide their personal data to the data fiduciary and it is reasonably expected that they would provide such personal data, as well as legitimate interests processing without consent.
- **Data subject rights:** In addition to rights to access and correct personal data, the 2022 Bill would provide data subjects with a right of erasure and a right to register a grievance with Data Fiduciaries.
- **Mandatory data breach notification:** The 2022 Bill would require organizations to notify the DPBI and impacted data subjects of any breach. Notably, the breach notification obligation found in the 2022 Bill does not reference the 72 hour time limit found in the 2021 Bill.

- **Data localization:** The 2022 Bill will rekindle concerns that India is seeking to introduce data localization. Article 17 provides that India's central government may "white list" jurisdictions which may receive transfers of digital personal data, subject to terms and conditions being met. Article 18(1)(d) provides an exemption which appears to target re-exports of foreign personal data by offshore service providers in India, but otherwise, the 2022 Bill provides for very little scope to transfer personal data from India.

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 other jurisdictions "cherry picking" GDPR concepts for their own laws. 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, has introduced 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 the final set of amendments having taken effect in October 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 to 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 is 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.

The 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' license numbers, credit/debit card numbers, health insurance information and medical history information.

Extended Deemed Consent Provisions

Singapore has marked itself out as one of the more business-friendly data protection regimes in the APAC region, including by providing for a substantial number of exemptions from the requirement to obtain consent to the processing of personal data. Amendments under the Bill have expanded 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 to the processing 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.

In January 2023, the PDPC issued its first decision concerning the application of the PDPA's legitimate interests exception, finding in favor of an online grocer collecting photo identification card details from suppliers making deliveries to its warehouses. The PDPC made its decision on the basis that this collection of data was for the purpose of public food hygiene and safety, which was in the legitimate interests of both the grocer and also of its business partners and ultimately, Singapore consumers.

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

Increased Deterrence

The Bill strengthened 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.

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 has been 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

After a year of significant changes prompted by major data breaches affecting millions of Australian individuals, privacy and cybersecurity law in Australia looks set for further upheaval in 2023. Among the major upcoming developments is the long-awaited overhaul of the Privacy Act (the "**Privacy Act**"), which may potentially introduce new requirements to align the Privacy Act closer to international privacy frameworks, such as GDPR.

Key developments in 2022

In 2022, urgent reforms to the Privacy Act were passed in response to major data breaches affecting the personal information (including health/sensitive information) of millions of Australian individuals. Notably, these reforms dramatically increased the penalties for non-compliance with the Privacy Act.

The key changes to the Privacy Act included (amongst others):

- increased maximum penalties for 'serious' or 'repeated' interferences with an individual's privacy. The increased penalties for a body corporate are now an amount not more than the greater of:
  - AU$50 million;
  - if the court can determine the value of the benefit that the body corporate, and any related body corporate, have obtained directly or indirectly and that is reasonably attributable to the conduct constituting the contraction – 3 times the value of that benefit; or
  - if the court cannot determine the value of that benefit – 30% of the adjusted turnover of the body corporate during the breach turnover period for the contravention.
- Amendments to section 5B of the Privacy Act to expand its extra-territorial application to capture foreign businesses that carry on business in Australia. The requirement that a foreign organization must collect and hold personal information in Australia has now been removed. In effect, this means that foreign organizations can be captured by the Privacy Act provided they carry on business in Australia, even if they do not directly collect and hold data in Australia; and
- new enforcement and information sharing powers for the Australian Information Commissioner, which include powers to (amongst other things):
  - request an entity to provide information and documents in relation to an eligible data breach under the Notifiable Data Breach Scheme ("NDB Scheme");
  - assess whether an entity is compliant with its obligations under the NDB Scheme;
  - issue infringement notices for entities that fail to provide requested information;
  - share information obtained under the Privacy Act with other enforcement bodies (such as the Australian Communications and Media Authority), an alternative complaint body, and a State, Territory or foreign privacy authority; and
  - disclose information to the public where it is in the public interest to do so.

Potential reform this year

The Australian government has indicated that it intends to undertake a major overhaul of the existing privacy legislation. Further reforms to the Privacy Act to address the issues raised in the Commonwealth Attorney-General's Privacy Act review are anticipated in 2023 ("**Privacy Act Review**").

On 16 February 2023, the Attorney-General's Department released the final report to the Privacy Act Review ("**Privacy Act Review Report**"). Key changes proposed in the Privacy Act Review Report include (amongst others):

- broadening the definition of 'personal information' under the Privacy Act to encompass information that 'relates' to an individual and includes technical and inferred information;
- extending some of the protections of the Privacy Act in relation to personal information to de-identified information, such as the requirement for entities to protect de-identified information from misuse, interference and loss, and from unauthorized re-identification, access, modification or disclosure, and requirements to take reasonable steps to ensure that overseas recipients of de-identified information do not breach the Privacy Act in relation to that information;
- require consent for the collection, use and disclosure of geolocation tracking data;
- the eventual removal of the small business exemption (though this will only occur after an impact analysis and consultation with businesses has taken place);
- modifying the employee records exemption to introduce enhanced privacy protections to private sector employees (the implementation of which will be subject to further consultation);
- requiring collection notices to be 'clear, current, and understandable' and introducing standardized collection notices;
- requiring the collection, use and disclosure of information to be 'fair and reasonable in the circumstances,' irrespective of whether consent has been obtained;
- establishing a direct right of action for breach of privacy;
- introducing new individual rights, such as the right to erasure, right to de-indexation, and right to object to the processing of their information (similar to GDPR);
- imposing additional requirements on entities engaging in 'high privacy risk activities' (which include, but are not limited to, the collection of sensitive information on a large scale, the collection of information about children and vulnerable people, direct marketing, and the use of information in automated decision-making) to complete a privacy impact assessment prior to undertaking the activity;
- creating additional protections in relation to children and vulnerable people;
- introducing additional requirements in relation to direct marketing, targeting, and trading of personal information;
- introducing the concepts of 'controllers' and 'processors' into the Privacy Act;
- introducing prescribed countries and standard contractual clauses in relation to the cross-border disclosures of personal information; and
- amend the NDB Scheme to require entities to notify the Information Commissioner of an eligible data breach within 72 hours.

Japan

Amendments to the APPI

On 1 April 2022 a number of substantial amendments to the Japanese Act on the Protection of Personal Information ("**APPI**") took effect. The amendments

aim 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.

Japan's Personal Information Protection Commission ("**PPC**") published various guidelines in support of the amendments. Key provisions in the amendments and the PPC's guidelines include:

- **Expanding the 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 on a "controller-controller" basis 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.

Amendments to the TBA

Promulgated on 17 June 2022, amendments to Japan's Telecommunications Business Act ("**TBA**") will take effect from 16 June 2023. One of the aims of the update is to obtain a secure and reliable communications service network. According to the Ministry of Internal Affairs and Communications ("**MIC**"), relevant guidelines are expected to be issued by the effective date. Key takeaways include:

Introduction of the new concept of "Specific User Information" ("SUI") and related obligations: SUI is user information that is obtained in connection with telecommunications services that: (1) falls under the category of communications secrets; or (2) is information that can identify users and specified in the applicable Order of MIC.

The MIC may designate particular telecommunications carriers having "a large impact" on users' benefits in consideration of the contents, the scope of users, and the usage conditions, as carriers that must properly handle SUI ("**Designated carriers**").

Within 3 months from designation, Designated carriers are required to (1) establish "information handling regulations" and notify the MIC, (2) establish an "information handling policy" and make this public and (3) appoint a "Chief administrator of specified user information". Designated carriers must also conduct a self-assessment regarding the handling status of SUI every fiscal year and, if necessary based on the results, update such "information handling regulations" or "information handling policy".

Establishment of regulation regarding external transmission of user-related information: MIC may issue orders designating providers of telecommunications services specified as having "an impact that is not minimal" on users' benefits in consideration of the contents, the scope of users, and the usage conditions, as well as telecommunications carriers that are subject to certainnotification or registration requirements under the TBA.

When designated carriers attempt external transmission of user-related information, such as cookies, they will generally need to either notify or establish arrangements that allow users to easily be informed of (1) the content of the user-related information to be transmitted, (2) telecommunications facilities to which such information will be transmitted and (3) other matters specified in the Order of MIC in advance.

Indonesia

On 17 October 2022 the Indonesian president gave assent to Law No. 27 of 2022 on Personal Data Protection (the "**PDP Law**"), Indonesia's first comprehensive data protection law.

Regulatory Framework

The PDP Law resembles GDPR in a number of respects, most importantly through its creation of a dedicated data protection authority, the regulation of both data controllers and data processors, an element of extra-territorial effect, a mandatory data breach notification obligation and the special treatment of "specific personal data", which is similar to special categories or sensitive personal data.

It is important to note, however, that the PDP Law will supplement (but not replace) a number of existing laws, including Law No. 11 of 2008 as amended by Law No. 19 of 2016 on the Electronic Information and Transactions (the "**EIT Law**"), Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions ("**GR 71/2019**") and the Minister of Communications and Informatics ("**MOCI**") Regulation No. 20 of 2016 on the Personal Data Protection in Electronic System ("**MOCI Regulation 20/2016**"). The continued effect of MOCI Regulation 20/2016, in particular, has consequences for the treatment of cross-border transfers of personal data.

Transitional Period

The PDP Law has been passed with a transitional period of two years, generally taking effect from 17 October 2024, save for with respect to criminal sanctions.

Extra-territorial effect

PDP Law adopts extraterritorial approach whereby it applies not only to domestic processing but also where processing personal data has legal consequences:

1. within the jurisdiction of the Republic of Indonesia; and/or
2. to Indonesian citizens, as personal data owners, residing outside the jurisdiction of Indonesia.

This "effects-based" approach to extra-territoriality is noticeably broader than the formulation under GDPR, which involves an element of targeting or intention to process the personal data of individuals in Europe.

Lawful Basis for Processing

The PDP Law provides the following legal bases for collecting and processing personal data:

- with the data subject's express consent;
- in accordance with contractual obligations under a contract to which the data subject is a party;
- in accordance with legal obligations of the data subject under applicable law;
- to protect the data subject's vital interests;
- in the public interest or in the exercise of lawful authority under applicable law; and
- in fulfilment of legitimate interests, taking account the purpose and necessity of processing and balancing the interests of the data controller against the data subjects' privacy interests.

The PDP Law provides that consent may be obtained through written or other recorded means, either electronically or non-electronically and using the Indonesian language.

In addition, the consent form shall be understandable, in an accessible format, and using simple and clear language — if not, the consent will be deemed null and void.

International Data Transfers

The PDP Law does not introduce any specific controls on international transfers of personal data. However, the PDP Law will not replace MOCI Regulation 20/2016, which requires that international transfers of personal data be notified to the MOCI using the form designated for this purpose either before or after the transfer.

It is expected that an implementing regulation to be issued by the Indonesian government to further regulate offshore data transfers.

Accountability and Data Subject Rights

The PDP Law draws heavily from GDPR in imposing an obligation on organizations to appoint a data protection officer where any of the following apply:

- processing personal data for public services,
- the core activities of the controller require regular and systematic monitoring of personal data on a large scale, or
- the core activities of the controller consist of large-scale processing for specific personal data or data related to criminal offenses.

Data controllers are required to conduct a data protection impact assessment where the processing of personal data has a high risk of harming the data subject, which includes:

- Automated decision-making that has legal consequences or a significant impact on data subjects;
- Processing of specific personal data (being sensitive personal data);
- Large-scale processing of personal data;
- Processing for systematic evaluation, scoring, or monitoring activities;
- Processing for matching activities or merging a group of data;
- The use of new technology; and
- Processing that restricts the exercise of data subject rights.

The PDP Law provides data subject with rights to access and correct their personal data, as well as rights to delay or restrict processing, revoke consent, object to automated decision-making and a right to data portability.

The "72 hours rule"

PDP Law now introduces a challenging 72 hour response time in the following circumstances:

1. notify affected data subject regarding instances of data breach no later than 72 hours after discovery of the breach;
2. update and/or correct errors and/or inaccuracies in personal data no later than 72 hours after receiving a request from the data subject to do so;
3. provide access to data subject no later than 72 hours after receiving a request from the data subject;
4. terminate personal data processing and erase personal data no later than 72 hours after the withdrawal of data subject's consent; and
5. suspend and limit processing activity no later than 72 hours after the request by the personal data subject to do so.

Sanctions

Breaches of the PDP Law will give rise to administrative sanctions as follows:

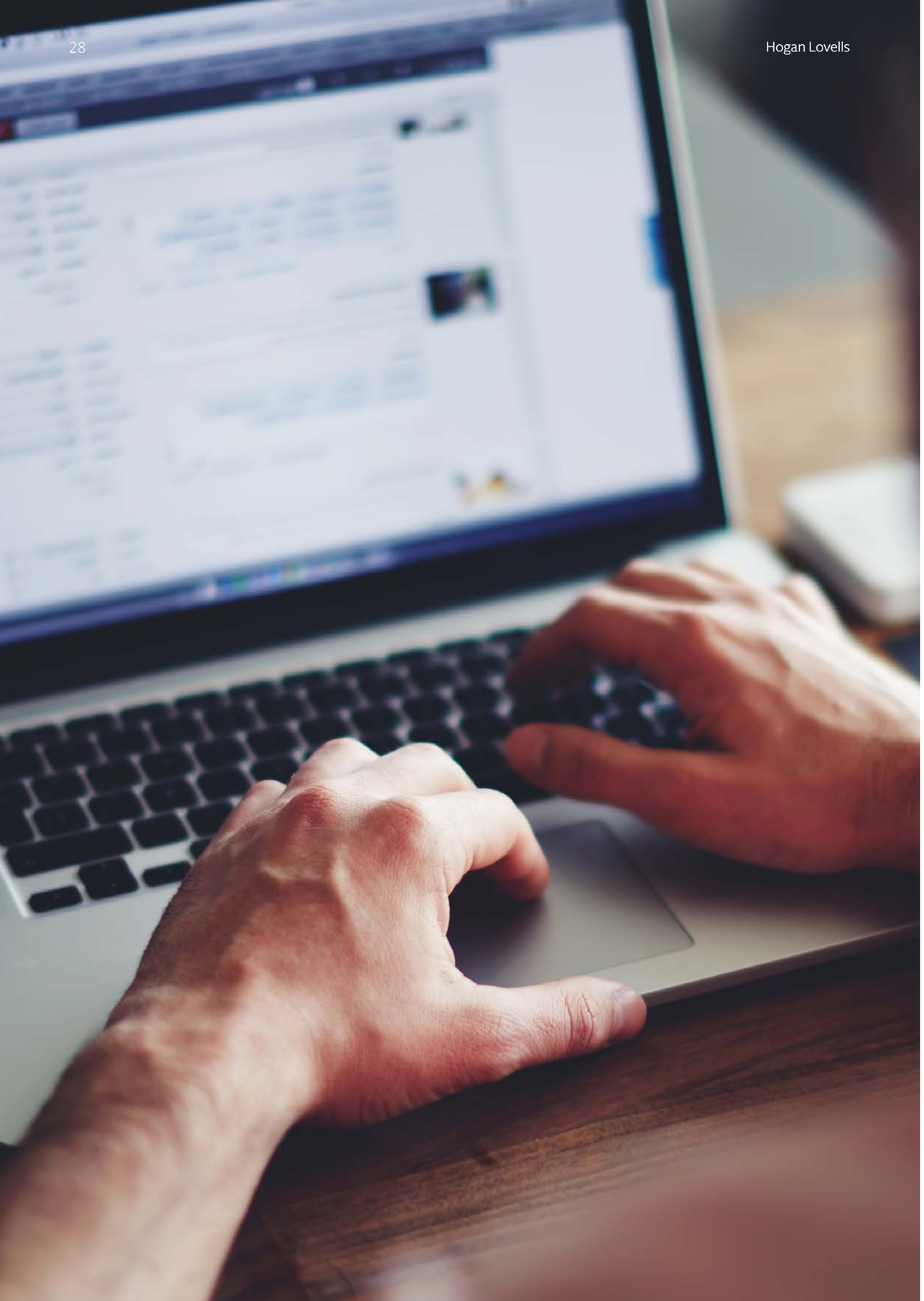
1. written reprimand;
2. an order to temporarily suspend the personal data processing activities;
3. an order to erase or destroy the personal data; and/or
4. fines of maximum 2% of the gross annual income.

We understand that the fines will be regulated further, pending the issuance of an implementing regulation.

Violations of the prohibited actions, which include unlawful collection, disclosure, and/or use and falsifying of personal data, will be subject to criminal sanctions ranging from four to six years imprisonment and/or criminal fines ranging from IDR 4 to 6 billion for individuals. For corporations, the criminal fines will be multiplied by a maximum of 10 times, amounting to a maximum of IDR 50 billion or approx. USD 3,182,878.

There are also additional sanctions for corporations in the form of, among others:

1. confiscation of profits and/or assets obtained or proceeds from the crimes;
2. suspension of the entire or part of the corporation's business;
3. permanent prohibition of certain actions;
4. shutdown of the entire or part of the corporation's place of business and/or activities;
5. fulfilment of neglected obligations;
6. payment of compensation;
7. license revocation; and/or
8. dissolution of any relevant corporate entity.



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

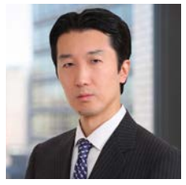
Bringing to bear the knowledge and experience of our extensive and market-leading data protection and cybersecurity management team across the world in finding solutions that work in Asia based on lessons learnt elsewhere.

Key contacts in APAC

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

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

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



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

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

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

Gaston Fernandez
Partner, Hanoi, Ho Chi Minh City
T +84 28 3827 1738
gaston.fernandez@hoganlovells.com

Chalid Heyder
Office Managing Partner, Jakarta
T +62 21 2788 7911
chalid.heyder@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 multinationals 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,

Click here to view more about ***Chronicle of Data Protection.***

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
Munich
New York
Northern Virginia
Paris
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

Associated offices*
Legal Services Center: Berlin

www.hoganlovells.com