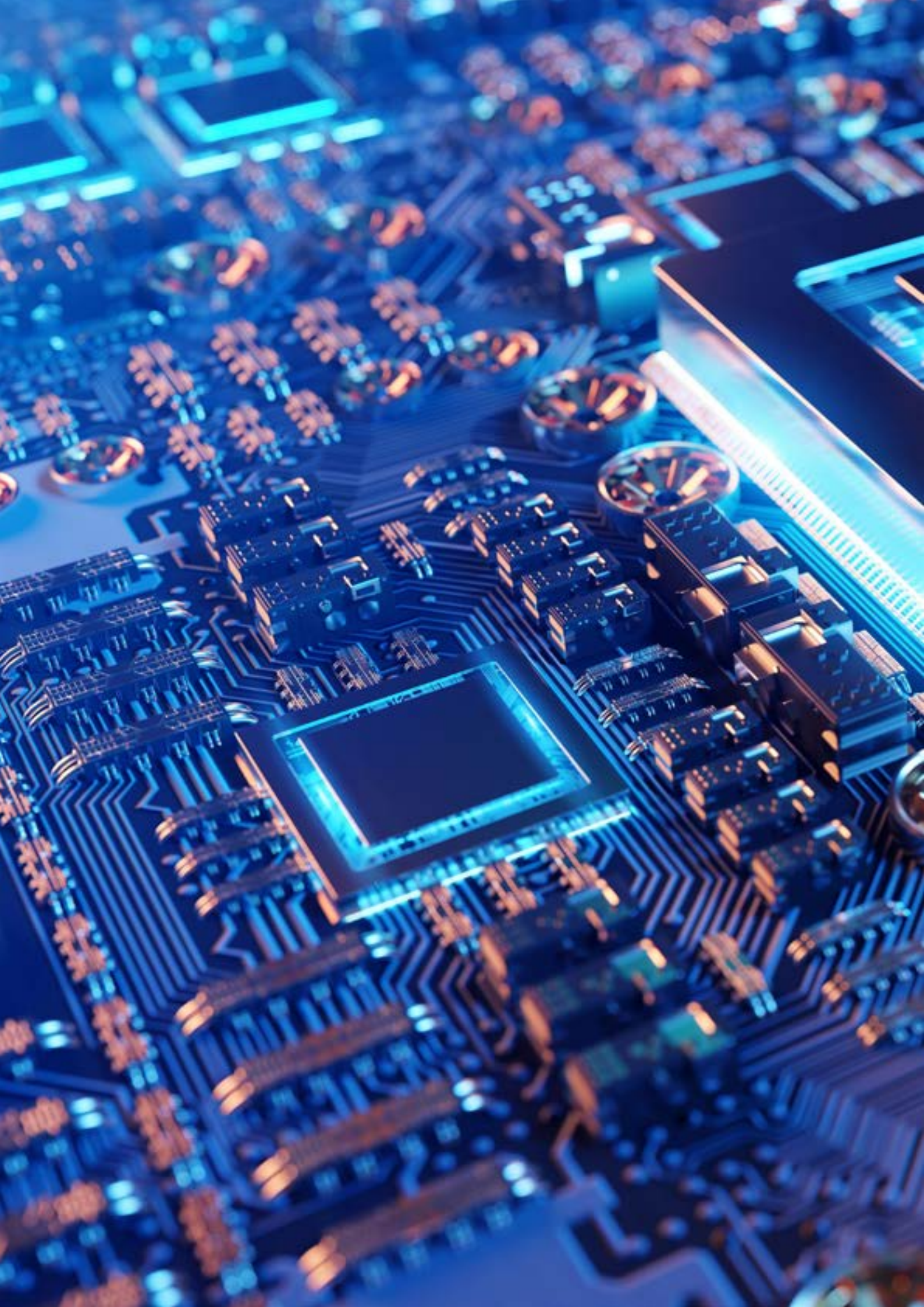


The image features the Hogan Lovells logo in the top left corner, consisting of the firm's name in a black serif font inside a solid lime green square. The background is composed of large, overlapping geometric shapes in shades of lime green and a light blue-purple gradient, creating a modern, abstract design.

Hogan  
Lovells

# **Asia-Pacific Data, Privacy and Cybersecurity Guide 2025**







# Contents

Key Contacts	5
2024 in Review: A Look Ahead at 2025	6
Heat Map	10
Individual Country Spotlights	12
Mainland China	12
Hong Kong SAR	31
India	36
Singapore	40
Australia	48
South Korea	51
Japan	52
Indonesia	59
Vietnam	67
A Guide to Making (and Keeping) Your Business Compliant	84
Hogan Lovells’ Asia-Pacific Data, Privacy and Cybersecurity Practice	95



## Key Contacts

**Tommy Liu**

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

**Sherry Gong**

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

**Charmian Aw**

Partner, Singapore  
T +65 6302 7142  
charmian.aw@hoganlovells.com

**Gastón Fernández**

Partner, Hanoi, Ho Chi Minh City  
T +84 28 3829 2100  
gaston.fernandez@hoganlovells.com

**Hiroto Imai**

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

**Mochamad Kasmali**

Partner, Jakarta  
T +852 2840 5072  
mochamad.kasmali@hoganlovells.com

**Kenneth Cheung**

Associate, Hong Kong  
T +852 2840 5613  
kenneth.cheung@hoganlovells.com

**Flora Feng**

Associate, Beijing  
T +86 10 6582 9546  
flora.feng@hoganlovells.com

## Global Co-heads of Hogan Lovells' Data, Privacy and Cybersecurity Practice

**Eduardo Ustaran**

Partner, London  
T +44 (20) 7296 5249  
eduardo.ustaran@hoganlovells.com

**Scott Loughlin**

Partner, Washington, D.C.  
T +1 (202) 637 5565  
scott.loughlin@hoganlovells.com

# 2024 in Review: A Look Ahead at 2025

2024 was another year of rapid change to the data, privacy and cybersecurity regulatory landscape in the Asia-Pacific (APAC) region. The brisk pace of development has clearly become the norm. Since GDPR became the benchmark for data protection regulation internationally in 2018, the significant uplift to European standards is gradually making its way across the region. APAC jurisdictions with longer histories of data protection regulation have been upgrading their laws by cherry-picking from GDPR, with innovations such as data breach notification obligations and revenue-based fines becoming typical across the region. At the same time, jurisdictions with no history of data protection regulation at all have been taking GDPR as their template, confirming that it has become the inevitable reference point for laws in the area. The difference now is that many regional data protection authorities have gained experience with GDPR-inspired concepts and have made them their own, raising compliance expectations along the way. However, we see a pause (or perhaps even a reversal) of the trend to adopt ever-more stringent privacy compliance requirements inspired by GDPR, now that both the data protection regimes in APAC and the authorities tasked with on-the-ground implementation begin to mature. With time, we see regulators taking a more pragmatic approach and even dialling back some of the requirements, in the face of the economic downturn and the challenges local businesses face in practice to achieve compliance.

Case in point are the challenges faced by organisations dealing with China's cross-border data transfer restrictions. The Cyberspace Administration of China (CAC) launched its security assessment procedure late in 2022, followed by the introduction of standard

contractual clauses and personal information privacy assessment guidelines in 2023. Organisations have generally found the process to be extremely challenging, with a lengthy security assessment questionnaire requiring organisations to provide the authorities with detailed – and in some cases very sensitive – technical information about the data processing environment supporting the transfer, both in mainland China and abroad. Official data indicates that successful applications have been few in number, prompting the CAC to roll out measures by relaxing the restrictions and clarifying the thresholds triggering transfer requirements of different levels, would create a number of exemptions for various types of data transfer.

It is clear that data transfer regulatory policy in China is struggling to achieve a balance between, on the one hand, a vision of comprehensive “cyber sovereignty” considered necessary to Chinese national security and, on the other hand, a business environment that is supportive of foreign investment. China's approach to cross-border data transfer regulation is already having its influence, with Vietnam launching a similar review procedure in the summer of 2023, which was met with similar resistance.

The other key variable is that a growing number of APAC jurisdictions are coming to focus on cybersecurity and national security concerns, with the effect that the underlying policy applicable to data protection regulation may differ from the GDPR.

For example, we see China introducing a raft of new laws and regulations to prescribe further requirements on network and data security, categorising and defining data of



varying importance, such as “important data” and “core data”, with different obligations attached to such data categories.


We expect to see these tensions continue through 2025, with data policy becoming increasingly intertwined with geopolitics and trade policy.

## Data protection 2.0: the 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 in a way that 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 now clear, however, that organisations’ data protection compliance programmes should take their strategic direction from the “accountability-driven” model championed under the GDPR. The points of compliance organisations are required to manage under the disparate laws, including data subject consents and notifications, the exercise of data subject rights and the satisfaction of mandatory breach notification obligations, are now so numerous that a piecemeal approach to compliance is becoming increasingly risky. The overlay of data governance through various measures, such as the documentation of data protection policies, the conducting of privacy impact assessments and the implementation of privacy by design, means that a holistic, organisation-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 organisation-wide considerations of branding and corporate ethics. At present, the appointment of a data protection officer (DPO) is only required under



An aerial photograph of a city skyline, likely Chicago, with the Willis Tower prominently visible. In the foreground, there is a large body of water, possibly a lake or a series of connected ponds, surrounded by green grass and some trees. The sky is a pale, hazy blue, suggesting a clear day.

a few data protection laws in APAC, but the benefits of doing so are clear. Managing data protection compliance risk through a project management structure with designated points of accountability and appropriate management oversight significantly improves the organisation's ability to avoid increasingly costly adverse publicity, investigations, and fines.

### **Data protection compliance strategies for APAC**

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

GDPR compliance programmes have provided a blueprint for organisations seeking a systemic approach to compliance. The introduction of the Personal Information Protection Law (the *PIPL*) in China has brought the GDPR reference point closer to home. Extending a GDPR-compliance programme 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 programme for APAC that reflects the rising “high water mark” and so avoids “re-inventing the wheel” for each jurisdiction.

Organisations take different approaches to compliance for different reasons, but there is now a proven process for taking a GDPR compliance programme 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 in most (if not all) jurisdictions, recognising that there may be a need for “topping up” in APAC jurisdictions that have exceptional requirements in particular areas.

To provide 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” registers 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 2025

We expect data protection and cybersecurity regulatory development to continue at a rapid pace during 2025.

### *Key points to watch for:*

- China’s economic challenges seem to have led to a relaxation of cross-border transfer regulation, but as the security agenda continues to move forward in the world’s second largest economy, watch for further clarification in the regulation of “important data” and in the handling of “work secrets”.
- As artificial intelligence continues to dominate discussions of digital transformation globally, data protection authorities have been pushed to the fore as presumptive leaders in formulating official policy. As the considerations for AI regulation touch on many issues beyond data protection, watch for movements by industry

regulators and the start of an important regulatory dialogue in this space.

- The implementation of India’s Digital Personal Data Protection Act will bring the world’s most populous nation into the fold of comprehensive data protection regulation, an important new contributor to the policy debate in APAC.

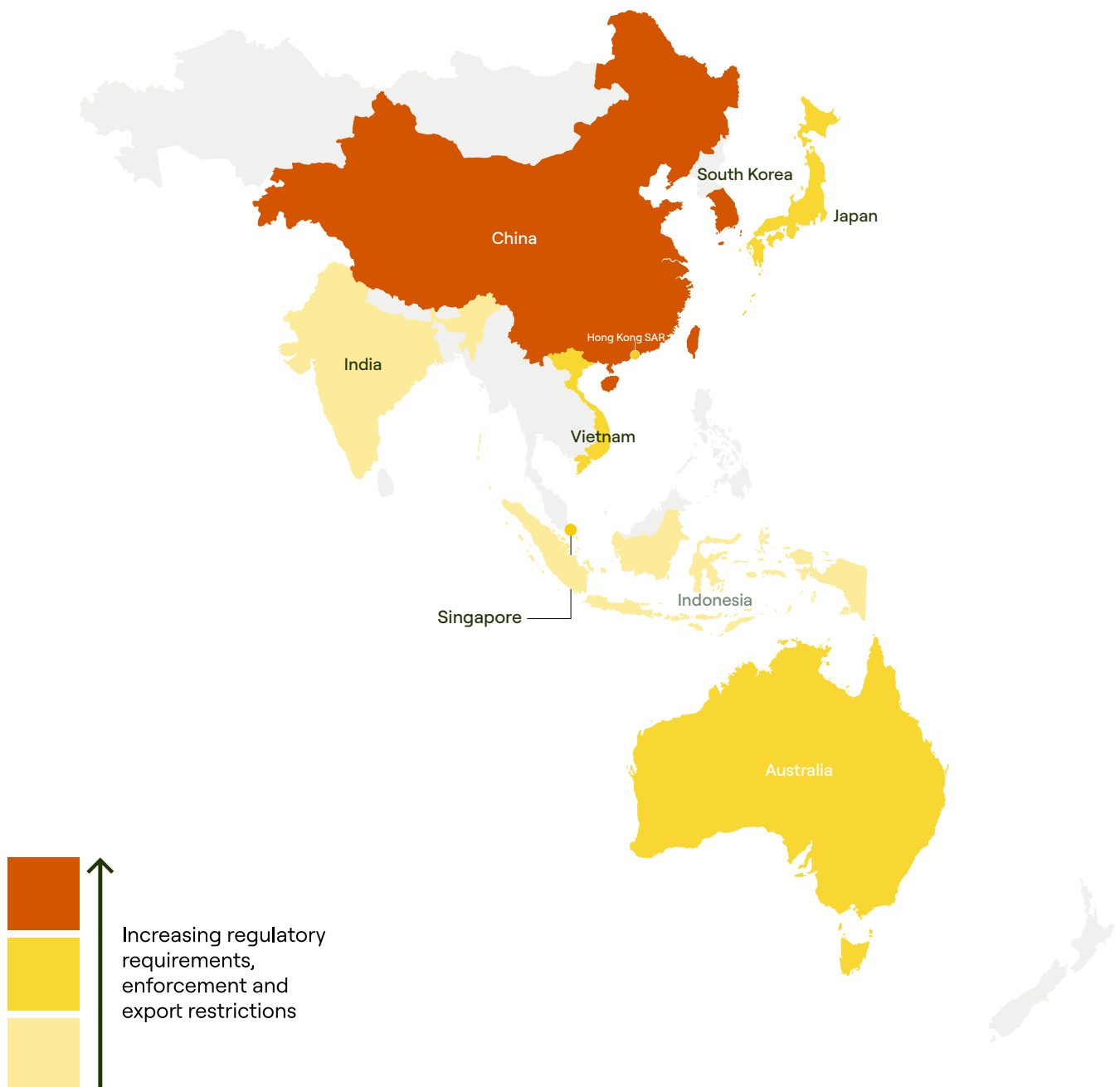
# Heat Map

Our Asia-Pacific data, privacy and cybersecurity 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

## Mainland China

China's unique approach to data and cybersecurity 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 entire region's business environment, even as the country currently faces significant economic challenges.

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

### The Cybersecurity Law

The *CSL* came into effect on June 1, 2017, making it the cornerstone of China's current data protection and cybersecurity 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.

### Localisation

When the *CSL* was introduced in 2017, there were widespread concerns that data localization, long threatened, would at last be formalized under Chinese law. Companies across a range of sectors fear that the policy direction under *CSL* could force them to establish separate operating platforms in China by making use of local technology if foreign technology is considered to raise national security concerns.

Comprehensive data localisation did not come to pass with the introduction of the *CSL*.

Organisations considered to be operators of "critical information infrastructure" (*CIIO(s)*) did face this prospect for important data and personal data generated and collected during *CIIOs'* operation in China (which will be subject to a security assessment with the competent authority), but most foreign businesses found themselves to be classified as "network operators", a lower risk grading unlikely to be subject to data localisation required under the *CSL*. While not imposing localisation, the *CSL* does require network operators to meet a number of obligations, including storing internet logs for at least six months, blocking the dissemination of illegal content, and providing "technical support and assistance" to the authorities in national security and criminal investigations.

### Multi-Level Protection Scheme

The most significant lasting impact of the introduction of the *CSL* for multinational businesses has been the reboot of China's cybersecurity grading system, the Multi-Level Protection Scheme (*MLPS*), which was revamped in 2019.

*MLPS 1.0* (2007-2019) requires organizations to self-assess their cyber risk against a five-tier grading system. Organisations having a risk rating of three are required to report their status and self-assessment to the authorities, procure information security products and engage *MLPS* assessment institutions meeting special conditions, implement cybersecurity monitoring and detection, be subject to annual inspections by the Ministry of Public Security (*MPS*), among other requirements. More broadly, *MLPS 1.0* includes a series of graded technical standards, addressing a wide range of issues, from cybersecurity governance through to specific technical requirements for ICT



infrastructure and data management. MLPS 1.0 introduced annual inspections by government officials and MPS, in a move that has raised significant concern for multinationals operating in China.

Based on the CSL, MLPS 2.0 (2019-) optimises the MLPS 1.0 from the following aspects:

- Introducing extended security requirements for emerging technologies like cloud computing, IoT, mobile internet, industrial control, and big data.
- Transitioning from passive defense to a dynamic protection system that includes pre-emptive defense, real-time response, and post-event auditing;
- Updating the grading process requires expert review and approval by competent authorities for Level 2 and above systems;
- Adjusting the grading levels, with systems causing significant harm to legal rights now classified as Level 2 instead of Level 2; and;
- Empowering MPS to perform remote access inspections (upon prior notice) and on-site inspections.

### **Proposed amendment to the CSL**

On September 12, 2022, the Cyberspace Administration of China (CAC) issued a draft to amend the CSL, mainly aimed to improve the legal responsibilities regarding the security protection of critical information infrastructure (*CII(s)*) and other network information security and operational security. Overall, the draft proposed to increase penalties, and impose penalties equivalent to those implemented in the PIPL (i.e., fines of up to RMB 50,000,000 or 5% of the preceding year's turnover). According to the Work Report of the Standing Committee of the National









People's Congress, released on March 14, 2025, stated that an amendment of CSL is one of the legislative priorities for the Chinese government in 2025. To date, there hasn't been a new draft for public consultation regarding the amendments to the CSL. It remains uncertain whether future updates will be included in addition to the increased legal responsibilities.

### **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 September 1, 2021, provide guidance on whether or not an organisation is CIIO and requires CIIO to only deploy safe and reliable network products and services. For network products and services that may affect national security, CIIO shall complete a national security review.

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

- The degree of importance of 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; and,
- Any other related impact on other industries or sectors.
- Some of the key obligations in relation to *CIIs* include the obligation to:
- Design, implement, and utilise 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, CIIOs that store or handle information that involves state secret information are subject to certain State secret laws and regulations and CIIOs that utilise commercial encryption products are subject to relevant encryption regulations.

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

### **The Data Security Law**

Next in line of the three primary data and cybersecurity laws, the DSL, which came into effect September 1, 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 organisations and individuals carrying out data-related activities; (c) measures to support the promotion and development of data security; and (d) the establishment of mechanisms to guarantee the security of government data, and promote the openness of government data.

It is important to understand that, whereas the 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.

### Extra-territorial application

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 organisations in China.

### Core 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, the lifelines of the national economy, important people’s livelihoods and vital public interests. The DSL provides that more stringent requirements would be developed in respect of core data.

### Important Data

A key feature of DSL is a 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.

Further to the introduction of the concept of important data in the DSL, CAC defines “important data” for the first time in the Measures for Security Assessment for Cross-Border Data Transfers (effective from September 1, 2022) as data which, if distorted,

damaged, leaked, or illegally obtained or used, may endanger national security, economic operation, social stability, public health, and security, etc. Subsequently, the definition of important data has been further developed in the Regulation on Network Data Security Management (*Network Data Regulation*, effective on January 1, 2025), as data associated with specific field, specific group, or specific region or with a certain degree of accuracy and scale, which, once tampered with, destroyed, divulged, illegally obtained or illegally used, may directly endanger national security, economic operations, social stability, public health, and security.

In a relaxation that may prove to be significant, the Provisions to Promote and Regulate Cross-Border Data Transfers (*CBDT Provisions*) (effective March 22, 2024) and the Network Data Regulation state that, unless industry or local regulators have published or notified industry participants of a particular type of data as being important data, such data exportation will not be subject to a CAC security assessment that applies to cross-border transfer of important data.

The topic of “important data” continues to cloud China’s data regulation landscape. There has been some movement to define “important data”, with a number of industry regulators consulting on data catalogues and classification rules.

On March 21, 2024, TC260 released the non-binding national standard, GB/T 43697-2024 Data security technology — Rules for data classification and grading (*2024 Data Classification GB*), effective on October 1, 2024. According to Article 6.5 (b) of the 2024 Data Classification GB, data that meets any of the following conditions is identified as important data. The 2024 Data Classification GB also provides that data that only affects individual organisations or citizens is not classified as important data E.g., data related to

the internal management of an enterprise is not considered important data.

- Data that, if leaked, tampered with, damaged, or illegally obtained, used, or shared, would directly cause moderate harm to national security;
- Data that, if leaked, tampered with, damaged, or illegally obtained, used, or shared, would directly cause severe harm to economic operations;
- Data that, if leaked, tampered with, damaged, or illegally obtained, used, or shared, would directly cause severe harm to social order (e.g., affecting social stability);
- Data that, if leaked, tampered with, damaged, or illegally obtained, used, or shared, would directly cause severe harm to public interests (e.g., endangering public health and safety);
- Data directly related to national security, economic operations, social stability, public health, and safety in specific fields, groups or regions;
- Data of a certain accuracy, scale, depth, or importance that directly affects national security, economic operations, social stability, public health, and safety;
- Important data as determined by the competent (regulatory) authorities in the industry sector.

In particular, Annex G of the 2024 Data Classification GB states that the identification of new important data should be based on compliance with 6.5 (b) and data with one of the following factors can be identified as important data:

- Data directly affecting territorial security and national unity, or reflecting the basic condition of China's natural resources,







such as data of undisclosed territorial land, territorial waters, and airspace;

- Data which could be used by other countries or organisations to launch a military strike against China, or reflect China's strategic reserves, emergency mobilisation, combat capabilities, etc., such as geographical data which meets certain accuracy indicators or data related to the capabilities and reserves of strategic goods;
- Data directly affecting the order of market economy, such as data which supports the core business operations of industries and fields with critical information infrastructure or the production of important economic sectors;
- Data reflecting the characteristics of China's language and writing system, history, customs and habits, national values, etc., such as data which records historical and cultural heritage;
- Data reflecting the physical security protection of key targets and important places or the location of undisclosed geographical targets, which could be used by terrorists and criminals to cause damage, such as construction drawings, internal structures, and security data describing key security units, important production enterprises, and important national assets (such as railways and oil pipelines);
- Data related to China's scientific strength, affecting China's international competitiveness, or related to export control items, such as data reflecting major national scientific and technological innovation achievements, or describing the design principles, process flows, and production methods of export-restricted or export-prohibited items, as well as data involving source codes, integrated circuit layouts, technical solutions, important parameters, experimental data, and test reports;
- Data reflecting the overall operation, development and security protection of critical information infrastructure and its core software and hardware asset information and supply chain management, which could be used to carry out cyberattacks on critical information infrastructure, such as data related to system configuration information, system topology, emergency plans, assessments, operation and maintenance, and audit logs of critical information infrastructure;
- Data involving undisclosed attack methods, attack tools production methods, or attack support information, which could be used to launch supply chain attacks, social engineering attacks, and other cyberattacks on key targets, such as sensitive customer lists of governments, military units, etc., as well as undisclosed data on the procurement of products and services and undisclosed data on major vulnerabilities;
- Data which reflect the basic conditions of the natural environment, the production and living environment, or which could be used to cause environmental safety incidents, such as undisclosed data related to soil, meteorological observations, and environmental monitoring;
- Data reflecting the reserves and development and supply of resources, including water resources, energy resources, land resources and mineral resources, such as unpublished data describing hydrological observation results, changes in cultivated land area or quality;
- Data which reflect the situation of nuclear materials, nuclear facilities, and nuclear activities, or which could be used to cause nuclear damage or other nuclear safety incidents, such as data related to the design drawings of nuclear power plants and the operation of nuclear power plants;

- Data related to the security of overseas energy resources, the security of strategic sea lanes, and the safety of overseas citizens and legal persons, or which could be used to implement damage to China's participation in international economic and trade, cultural exchanges, or to impose discriminatory prohibitions, restrictions or other similar measures on China, such as data describing the production and transactions of special items for international trade and the equipping, use and maintenance of special equipment;
  - Data related to China's actual or potential interests in strategic new areas, including outer space, the deep sea, and the polar regions, such as undisclosed data related to scientific research, development and utilisation of outer space, the deep sea and the polar regions, as well as data affecting the safe passage of personnel in the aforementioned areas.
  - Data reflecting the research, development and application of biotechnology, reflecting ethnic group characteristics and genetic information, related to major infectious diseases, animal and plant epidemics, biological laboratory safety, or which could be used to create biological weapons or carry out biological terrorist attacks, or related to invasive alien species and biodiversity, such as important biological resource data and basic research data on microbial resistance;
  - Data reflecting the overall situation or key areas of economic operation and financial activity, related to industrial competitiveness, which may cause public safety incidents or affect the safety of citizens' lives, and may trigger mass activities or affect group emotions and perceptions, such as undisclosed statistical data and the trade secrets of key enterprises;
  - Data reflecting the physical condition of the national or regional population's health, related to the spread and prevention of disease, and related to food and drug safety, such as data involving healthcare resources, diagnosis and treatment mass population and health management, disease control and prevention, health rescue and protection, specific drug experiments, and food safety traceability;
  - Other data which may affect the security of the homeland, military, economy, culture, society, technology, electromagnetic space, network, ecology, resources, nuclear, overseas interests, space, polar regions, deep sea, biology, artificial intelligence, etc.;
  - Other data which may cause serious harm to economic operations, social order, or the public interest.
- Other than the above, there are also certain industry regulations and "negative data lists" (which outline the scope of important data applicable to organisations located in free trade zones) that could shed some light on determining if certain types of data involved in the organisations' business will be identified as important data.
- The vagueness of the provisions relating to important data and core data has been troubling for multinational businesses seeking to comply with the requirements of the DSL. We expect to see further movement in 2025 as more industry regulators move to develop catalogues of importance. The Ministry of Industry and Information Technology (*MIIT*) has implemented its Measures for Data Security Management in the Field of Industry and Information Technology (Trial Implementation), with effect from January 1, 2023. These measures call for data classification, including the identification of important data in the telecommunications and industrial sector. The Measures for Data Security Management of Banking and Insurance Institutions, issued on December 27, 2024, by the National Financial Regulatory



Administration (*NFRA*), stipulate that the NFRA will develop a catalogue of important data for the banking and insurance sectors based on national data classification and grading requirements. The NFRA will also propose a core data catalog and supervise and guide banking and insurance institutions in data classification, grading management, and data protection. The Measures for Data Security Management in the Field of Natural Resources, issued on March 22, 2024, further defines important data in the natural resources sectors and proposes systematic compliance requirements for important data.

### Localisation

Further to the CSL, DSL's localisation requirements mandate that certain types of data, particularly important and critical data, must be stored and processed within China.

This includes:

- *CIIO (already included in the CSL)*: CIIO must store personal data and important data collected and generated within China domestically. If there is a need to transfer such data abroad, it must undergo a security assessment.
- *Important Data*: The cross-border transfer of important data collected and generated within China by organisations other than CIIO shall comply with relevant requirements (which were specified in 2022 and relaxed afterwards in 2024 in the CBDT Provisions), with an aim to enhance data security and protect national interests by preventing unauthorised access to China's important data and potential risks associated with cross-border transfers of such data.

### Personal Information Protection Law

The PIPL is China's first comprehensive data protection law, taking effect November 1, 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 the GDPR by providing a legitimate interests basis for processing without consent where obtaining consent is not practical. It is also important to note that 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. Personal data handlers (who independently determine the handling purpose and method in the handling of personal data) 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 for the collection and use of 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 data, right to withdraw consent), but also includes a right to request an explanation of the organization’s data processing practices.

*Extraterritorial effect:*

PIPL applies not only to personal data handlers based in China, but also foreign personal data handlers 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) analysing or evaluating the behaviour of individuals in China; or (iii) other circumstances provided under Chinese law. Personal data handlers subject to PIPL which do not have operations in mainland China are required to appoint a local representative.

*International data transfers:*

Personal data handlers that transfer personal data outside of China are required to satisfy one of the following regulatory formalities, subject to certain thresholds (i.e., data category and volume involved) and exemptions, including: (a) conducting a security assessment by CAC (*CAC Security Assessment*); (b) undergoing appropriate certification (*Third Party Certification*); (c) entering into standard contractual clauses (SCCs), collectively, referred to as “Data Transfer Review”. In addition, personal data handlers must obtain a separate consent from relevant data subjects for such cross-border transfers, conduct a prior privacy impact assessment and implement necessary measures to ensure the processing activities of the offshore recipients will meet the PIPL standards. Please see the discussion of the security assessment measures below for further information.

*Accountability:*

Personal data handlers 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 personal data handlers 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 personal data handlers, 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 organisation's annual revenue in the preceding year, with fines of RMB 100,000 to 1,000,000 imposed on responsible individuals.

## **Cross-border data transfer regulation**

On March 22, 2024, CAC finalised the CBDT Provisions, which refreshed the threshold of Data Transfer Review and introduced a number of exemptions to China's restrictions on cross-border personal data flows.

With CBDT Provisions taking effect, CAC Security Assessments (the most rigorous form of Data Transfer Review) will only apply to data transfers undertaken:

- By CIIOs transferring any personal data or important data collected and generated within China; and
- By organisations other than CIIOs that, from January 1 of the current year, have cumulatively made international transfers of personal data (excluding sensitive personal data) of more than one million individuals or sensitive personal data of more than 10,000 individuals.

Organisations that have cumulatively transferred non-sensitive personal data of more than 100,000 but less than 1 million individuals or transferred sensitive personal data of less than 10,000 individuals are required to complete one of the other two forms of Data Transfer Review: i.e., either obtaining a Third Party Certification or entering into and filing SCCs.

With respect to important data, as mentioned above, unless industry regulators or other officials have published or notified industry participants of a particular type of data as being important data, the CAC Security Assessment procedure will not apply.

In addition to making adjustments to the thresholds for Data Transfer Review, the CBDT Provisions also introduced some exemption scenarios for Data Transfer Review:

*No personal data or important data:*

Export of data generated during activities such as international trade, academic cooperation, cross-border transportation, cross-border manufacturing and marketing, which do not contain personal data or important data, would be exempted.

*Offshore data:*

Personal data collected and generated overseas and subsequently transferred to China for processing would be exempted, provided that no domestic personal data or important data is introduced during the processing (an exemption that is most likely meant to address situations in which China-based shared services operations and outsourcing arrangements process data originating from outside mainland China).

*Exemption for "contractual necessity":* Where it is necessary to provide personal data overseas for the conclusion or performance of a contract to which the data subject is an interested party, including cross-border shopping, cross-border

payment, cross-border account opening, and examination services.

*Exemption for emergency:*

Where it is really necessary to provide personal data abroad in an emergency to protect the life, health and property safety of a natural person.

*Exemptions for employment relationship:*

Where it is really necessary to provide employees' personal data abroad for the purpose of conducting cross-border human resources management in accordance with the employment rules and regulations formulated in accordance with the law and collective contracts concluded in accordance with the law.

*Exemptions for limited transfer:*

Personal data handler other than CIIIO who have cumulatively provided personal data (excluding sensitive personal data) of less than 100,000 people to foreign countries since January 1 of the current year.

Pursuant to CDBT Provisions, Free Trade Zones (FTZs) are enabled to formulate their own "negative data lists" stipulating the types of data which are subject to Data Transfer Review. As of March 2025, some FTZs such as Beijing, Tianjin, Shanghai, Fujian, and Hainan have issued their negative and positive data lists. In practice, we've also seen some multinational companies benefit from FTZ rules in the context of cross-border data transfer.

The CDBT Provisions formalise some long-anticipated exemptions to Data Transfer Review that will no doubt be welcomed by organisations in a position to benefit. However, it is important to understand that even where exemptions to Data Transfer Review apply, personal data handlers are still required to comply with their obligations under the PIPL. For example, an organisation exempt from the requirement to file their SCCs, a privacy assessment report is still required to complete. More broadly, the CDBT Provisions do not create general exemptions to PIPL.









requirements and related implementation rules. Personal data handlers are still obliged to perform the broad range of statutory compliance obligations, including notifying data subjects and obtaining their separate consent to the international transfer, as well as executing data transfer agreement and taking necessary security measures, leaving much work still to be done.

## Network Data Regulation

China's newly enacted Network Data Regulation (effective January 1, 2025) introduces critical updates to strengthen governance over network data while balancing cross-border data flows and compliance flexibility. As a supplement to the CSL, DSL, and PIPL, the regulation clarifies operational requirements for foreign and domestic entities whose data processing subject to the said laws (including those that subject to the extra-territorial application thereof). For instance;

### *Incident Report:*

Data incidents affecting national security or public interest must be reported to relevant supervising authorities within 24 hours.

### *Portability of Personal Data:*

Data subjects may request data transfers if: (i) identity of the requester is verified; (ii) data requested to be transferred was collected via consent/contract; and (iii) the requested transfer is technically feasible and not harmful to others' legitimate interests and rights. The network data handler is entitled to charge for excessive requests.

### *Obligations for Massive Data Processing:*

Network data handler processing personal data of more than 10 million individuals shall: (i) appoint network data security officer and establish the dedicated network data security body; (ii) implement technical and organisational measures to ensure network data security and promptly report to

provincial-level or higher regulators the data disposal plan and identity, and contact details of data recipients in case of merger, division, dissolution, or bankruptcy (or other events jeopardising data security, collectively *Key Transactions*).

### **Obligations for large network platforms:**

Large network platforms (with more than 50 million registered users or 10 million monthly active users, who have complex business types (undefined) and whose data processing may have significant impact on national security, economic operations, and public welfare) shall release annual social responsibility reports on personal data protection and be mindful of the activities using network data, algorithms, and platform rules (e.g., no fraud, no coercion, no unreasonable restrictions and no unreasonable differential treatment).

### *Obligations for Network Platform Service Providers:*

1. Network platform service providers shall legally bind third-party entities on its platform to adhere to data security obligations through enforceable contractual terms or platform policies (same for manufacturers of equipment such as smart terminals pre-installed with applications). Relatedly, they will bear shared liability for violations committed by third-party service providers operating within their ecosystems.
2. Providers of application distribution services must conduct pre-launch security evaluations of hosted applications and mandate corrective actions for non-compliant offerings.
3. Platforms utilising automated decision-making systems for personalized content delivery must implement user-controlled opt-out mechanisms, ensuring individuals can freely disengage from algorithmic recommendations.



*Privacy Policy Checklist:*

Privacy policies informing individuals of the purpose, method, and type of personal data to be collected and provided to other network data handlers (in which case the information of the network data recipient should also be notified) should be displayed in a checklist or similar form.

*Obligations for Processing Important Data:*

Network data handler processing important data shall: (i) establish and appoint a dedicated officer and an organisational body responsible for network data security; (ii) conduct risk assessment prior to providing important data to others (as entrusted processor or data handler) or jointly handling important data with others; (iii) implement technical and organisational measures to ensure network data security and promptly report to competent regulators the data disposal plan and identity, and contact details of data recipients in case of Key Transactions; (iv) conduct annual risk assessments and submit such assessments to the CAC and provincial-level authorities.

## **China's Personal Information Protection Compliance Audits Measures**

China's Personal Information Protection Compliance Audit Measures (*Audit Measures*), finalized by the CAC on February 14, 2025, refine existing obligations under the PIPL and Network Data Regulation. Effective May 1, 2025, the rules establish a dual-track audit framework: *mandatory periodic audits* for high-volume data handlers and *authority-triggered audits* for data handlers facing significant risks or breaches.

The Audit Measures provide further guidance on the conduct of personal information protection compliance audits (*Data Audit*), the selection of professional institutions to conduct Data Audits, the frequency of audits, and the obligations of personal information handlers, and professional institutions during Data Audits.

*Key Requirements include:**Regular Data Audit:*

- Personal data handler processing personal data of over *10 million China-based individuals* must conduct Data Audits every two years.
- Accordingly, personal data handlers processing personal data of less than 10 million China-based individuals are given some flexibility and are not obliged to conduct the Data Audit every two years. They should reasonably determine the frequency of Data Audit based on their own conditions, pursuant to the Q&A Session regarding the Audit Measures.
- Other sector-specific rules (e.g., annual audits for minors' data under the Regulations on the Protection of Minors in Cyberspace) may impose stricter obligations.

*Authority-Instigated Audit:*

The Audit Measures clarify three specific scenarios where the competent authorities may order the personal information handler to engage a professional institution to conduct Data Audits:

- Where there are significant risks in personal information processing activities, e.g., serious impact on personal rights and interests or severely inadequate security measures;
- Where there are personal information processing activities that may infringe on the rights of numerous individuals; and,
- Where there are personal information incidents leading to the leakage, tampering, loss, or destruction of personal information for over 1 million individuals or of sensitive personal information for over 100,000 individuals.

### *Audit Scope:*

- Audits cover 26 critical areas, including the legality basis of personal information processing activities, the processing rules, joint processing, entrusted processing, the transfer to other personal information handlers, cross-border transfer, automated decision-making processing, the processing of sensitive personal information, etc.

Under the Audit Measures, personal data handlers processing the personal information of over one million individuals must designate a personal information protection officer responsible for compliance audits. It is still unclear whether this is aimed to clarify the threshold for the requirement to appoint a personal information protection officer (i.e., the DPO) under the PIPL.

Additionally, the Audit Measures echo the PIPL by proposing an independent oversight mechanism for personal information handlers providing significant internet platform services with large user bases and complex business types. These handlers must establish an independent body, mainly consisting of external members, to oversee personal information protection compliance audits, regardless of whether the audit is conducted internally or by a professional institution.

The Audit Measures mark China's shift toward a *preventive governance* model, balancing regulatory rigor with operational efficiency. By integrating independent oversight and granular accountability, the framework aims to bolster public trust while supporting sustainable growth in the digital economy.









# Hong Kong SAR

Hong Kong's Personal Data (Privacy) Ordinance (the *PDPO*) is one of the APAC region's oldest data protection laws, coming into effect in 1995, with only two amendments since.

With China's significant upgrade of data protection standards under PIPL, Hong Kong's PDPO appears to be long overdue for an update. This is particularly so, in light of policy objectives to draw Hong Kong into closer economic collaboration with Guangdong province as part of China's Greater Bay Area (*GBA*) initiative, which seeks to link Hong Kong's position as a leading financial hub to Shenzhen's technological might and Guangdong province's manufacturing prowess.

A short list of reforms has been foreshadowed as far back as January 2020, when Hong Kong's Privacy Commissioner for Personal data (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.

However, little headway has been made with the proposed legislative reform so far. In a briefing to Hong Kong's Legislative Council (Hong Kong's legislative body) (*LegCo*) on February 20, 2023, the PCPD announced that the long-awaited amendments to the PDPO will be introduced in the first half of 2023, but this did not come to pass. More recently, the PCPD reported in a meeting of the LegCo Panel on Constitutional Affairs on February 17, 2025, that the comprehensive review of the PDPO was still ongoing, however they have yet to work out a concrete plan and timetable to introduce proposals for legislative amendments.

## Proposed legislative changes to the PDPO

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 unauthorised or accidental access of personal data. However, unlike an increasing number of laws internationally, the PDPO does not include an obligation to notify the PCPD or impacted data subjects if this provision has been breached. This lack of a breach notification requirement was heavily publicised following the PCPD's investigation of a substantial data breach by Cathay Pacific Airways in 2018. 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 current definition of an “identified” natural person. This would cover more categories of data, for example, tracking and behavioural data generated by big-data tools.

As privacy regimes in the mainland and other APAC jurisdictions continue to evolve, the PDPO appears to be increasingly out of step with international standards. It remains to be seen whether there would be more concrete developments for the proposed PDPO reform in 2025.

Despite the stagnant reforms for Hong Kong’s primary privacy legislation, progress has been made on other fronts, as seen in: (i) the launch of the GBA standard contract initiative; (ii) the release of data protection

guidelines for organisations adopting AI; and (iii) the enactment of the Protection of Critical Infrastructure (Computer System) Bill.

Hong Kong received a potential boost from a data protection perspective with the publication in December 2023 by the CAC and Hong Kong’s Innovation, Technology and Industry Bureau of implementation guidelines for standard contracts for cross-boundary flows of personal data within the GBA. The requirements for the GBA standard contracts are noticeably relaxed when compared to the general review of international data transfers from China. However, the GBA arrangements apply only to transfers of personal data controlled in Guangdong province, and do not permit onward transfer of personal data from Hong Kong.

In addition, the PCPD provided guidance on how organisations could harness the benefits of AI while safeguarding personal data privacy. The PCPD published a model framework for personal data protection on June 11, 2024, targeting organisations that procure AI solutions and process personal data in their operation of AI system. It covers a set of best practices in the following four areas:

- Establishing AI strategy and governance;
- Conducting risk assessment and human oversight;
- Customisation of AI models and the implementation and management of AI systems; and
- Communication and engagement with stakeholders.

Meanwhile, as the use of generative AI becomes more prevalent, the PCPD also issued guidelines for the use of such tools by employees in the workplace in March 2025 to assist organisations in the development of internal policies while complying with the PDPO.

## The Protection of Critical Infrastructure (Computer System) Ordinance

In late June 2024, the Security Bureau of the Hong Kong SAR Government proposed the first specific cybersecurity legislation in Hong Kong, entitled the Protection of Critical Infrastructure (Computer System) Bill (the *Bill*), to strengthen the security of the computer systems of critical infrastructure and minimize the chance of essential services being disrupted or compromised due to cyberattacks.

After a proposal for the Bill was released for public consultation in July 2024, the draft Bill was introduced to the LegCo for the legislative process in late 2024. After rounds of deliberation and further amendments, the Bill was enacted on March 19, 2025, and the Protection of Critical Infrastructures (Computer Systems) Ordinance was gazetted on March 28, 2025 (the *PCICSO*).

The PCICSO marks the first standalone cybersecurity law in Hong Kong, an important step to narrow the gap between Hong Kong's cybersecurity regulatory requirements and international standards. A regulatory framework is established to empower authorities to:

- Identify critical infrastructures ("CI"), which deliver essential services in eight core sectors (i.e. energy; information technology; banking and financial services; air transport; land transport; maritime transport; healthcare services; and telecommunications and broadcasting services), and those that maintains important societal and economic activities; and
- Designate operators of such CI ("CI Operators"), and their computer system as critical computer systems ("CCSs").

The PCICSO imposes statutory obligations on CIOs to establish and maintain cybersecurity measures and internal policies in relation to







their CCSs. Non-compliance could result in fines ranging from HK\$500,000 to HK\$5 million.

*Key obligations of the CI Operators include:*

- *Organisational:* maintaining an office in Hong Kong, reporting operator change promptly, and maintaining a computer system security management unit;
- *Preventative:* notifying the authorities of significant changes to CCS, submitting security management plans, performing regular risk assessments and audits; and
- *Incident reporting and response:* participating in security drills, submit emergency response plans, and notify authorities of security incidents in relation to CCSs, etc.

We expect the authorities to publish codes of practice or guidance notes in the future, to spell out the technical requirements and clarify how the PCISCO is to be implemented in practice, in the run up to and even after the PCISCO's effective date of January 1, 2026.





# India

Comprehensive data protection regulation has been a long time coming in India. Following the passage in August 2023 of the Digital Personal Data Protection Act (*DPDP Act*), which has yet to come into force, in January 2025, the Ministry of Electronics and Information Technology (*MEIT*) released a draft of the Digital Personal Data Protection Rules (*Draft Rules*) that seeks to implement the DPDP Act. The Draft Rules invited comments from the public which ended March 2025. We expect these feedback to be taken into consideration by the government. It is anticipated that the DPDP Act will be implemented by the end of this calendar year following finalization of the Draft Rules.

## *Key elements of the DPDP Act include:*

### *A dedicated authority:*

The DPDP Act would establish the Data Protection Board of India (“DPBI”), which would be responsible for enforcement. The move to a dedicated data protection authority is an important one, as it has been an important indicator of how strict enforcement will be under a new data protection law. That said, the DPBI has only adjudicatory powers, and the rule making powers under the law have been entrusted with the government.

### *Extra-territoriality:*

Drawing inspiration from GDPR, the DPDP Act would regulate all digital personal data collected or processed within the territory of India, processed by any Indian organisation and to the processing of digital personal data outside India, provided such processing is undertaken in connection with any activity related to the offering of goods or services to individuals in India. An earlier draft of the DPDP Act had made reference to extra-territorial monitoring of the behaviour of individuals in India, but this aspect of GDPR was dropped in the final draft. It is also relevant to note that the applicability of almost all

substantive provisions of the DPDP Act have been exempted where personal data of data subjects outside India is processed in India pursuant to a cross-border contract. This effectively exempts the processing of foreign personal data by the offshore/outsourcing industry from the new law.

### *“Data fiduciaries” and “Significant data fiduciaries”:*

The DPDP Act would regulate “data fiduciaries”, which are defined in similar terms as “data controllers” under GDPR. The DPDP Act would require that data fiduciaries assessed to be “significant” (based on various factors such as the volume and sensitivity of data processed) to appoint an India-based 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:*

The DPDP Act requires the free, specific informed, unconditional, unambiguous, and affirmatively indicated data subject consent to the processing of personal data, subject to prescribed exceptions, including “certain legitimate uses” such as where data subjects have voluntarily provided their personal data to the data fiduciary in circumstances in which they have not indicated to the data fiduciary that they do not consent to the use of their personal data. As the exemptions are fairly limited and there is no “legitimate use” type of ground under the law, consent would be the main ground for processing personal data. Further, given the manner in which consent is defined and requirements of privacy policies/notices, the standard for consent would be more or less the same as under GDPR.

### *Data subject rights:*

In addition to rights to correct and have personal data erased, the DPDP Act would

provide data subjects with a right to receive a summary of personal data which is being processed by the data fiduciary and the processing activities undertaken by that data fiduciary, as well as the identities of all other data fiduciaries and data processors with whom their personal data has been shared. The DPDP Act also includes certain other data subject rights such as a right to grievance redressal, and right to nominate another individual who can exercise rights of such data subject under the law in case of his/her death or incapacity.

*Mandatory data breach notification:*

The DPDP Act would require organisations to notify the IDPB and impacted data subjects of any breach in such form and in such manner as may be prescribed by regulations. Notably, there are no impact/harm thresholds prescribed under the law for reporting breaches and all breaches would need to be reported. The Draft Rules, in fact, prescribe a two-stage reporting to the DPBI, one immediately and another within 72 hours. Along with existing cybersecurity breach reporting, a data breach would trigger four data breach notifications.

*Data localisation/international transfer regulation:*

The DPDP Act significantly relaxes restrictions on international transfers of personal data proposed in earlier drafts of the law. As passed, the DPDP Act allows for cross-border transfers to all countries unless specifically restricted by the Indian government. The law however does not restrict the applicability of data localisation restrictions under other sector specific laws in India. The Draft Rules do however suggest the government may impose conditions on the transfer of personal data outside India.

*Wide data access powers of the government:*

The DPDP Act empowers the government to call for information from any data fiduciary or intermediary or the DPBI for purposes related to the law. The government is also empowered to exempt, in the interest of national security, the applicability of the DPDP Act to processing









of personal data by any of its agencies. Further, almost all substantive provisions of the law do not apply to processing of personal data by any court or government agency involved in performance of any judicial, quasi-judicial, regulatory, or supervisory function.

*Penalties:*

The DPDP Act includes a list of offences and prescribes monetary penalties of up to INR 2.5 billion (up to USD 30 million).





# Singapore

## Data protection

Singapore's push to be a leading innovation economy in APAC continues to be reflected in its regulatory approach to personal data under the Personal Data Protection Act (the *PDPA*), and in the commercially-sensitive thought leadership provided by the Personal Data Protection Commission (the *PDPC*). In particular, as we noted in our previous guide, Singapore's emerging data protection policy provides a wider latitude, compared to other Asian jurisdictions, to businesses that seek to create economic or social value through the processing of personal data.

### AI Guidelines

That policy approach was amply illustrated first in 2023, with the PDPC's circulation of a set of proposed advisory guidelines on the use of personal data in artificial intelligence (*AI*) recommendation and decision systems (*AI Guidelines*) and the issuance of the same on March 1, 2024. The *AI Guidelines* explain how the *PDPA* applies to the use of personal data by organisations that seek to develop, deploy, and procure AI systems – systems that embed machine learning models to make decisions autonomously, or to assist a human decision-maker through recommendations and predictions. In particular, the *AI Guidelines* address how and when exceptions to consent afforded in the *PDPA*, such as the business improvement exception and research exception, apply to exempt organisations developing AI systems, as well as identify the scope of data protection obligations that developers assume when training, testing, and monitoring AI systems.

### Exceptions to consent in AI system development

The *AI Guidelines* examine two statutory exceptions by which an organisation may

use personal data without consent from the individuals involved in order to develop AI systems.

The first is the “Business Improvement Exception”, which applies when an organisation uses personal data to improve existing goods or services, or to develop new ones; to improve the operational efficiency of delivering such goods or services; or to personalise or customise such goods or services. Examples of possible applications, relevant in the development of AI systems, include recommendation engines on social media platforms that offer personalised content; job assignment systems that assign jobs to platform workers; or AI systems that provide new product features to improve the competitiveness or appeal of those products.

The second exception is the “Research Exception”. This exception allows organisations to use personal data without consent, in order to conduct research or development that may not have any immediate application for their products, services, operations, or markets. To qualify for this exception, there must be a clear public benefit to an organisation's use of personal data for its research. The results of such research must neither identify any relevant individual, nor be used to make any decision that affects him.

### Data protection considerations

The *AI Guidelines* set out a concise list of factors, which organisations seeking to rely on each exception must consider. But whichever of these exceptions is employed, the *AI Guidelines* also remind organisations that they must implement technical, process, and legal controls in the process of designing, training, and monitoring AI systems using personal data. In particular, organisations are encouraged to

de-identify or minimise the use of personal data wherever possible, and to develop adequate policies regarding the use of personal data in the development of their AI systems. At the same time, the AI Guidelines recognise that the use of anonymised data may compromise model accuracy or the reproducibility of research results. Accordingly, organisations are permitted to “carefully weigh” the advantages and disadvantages of using anonymised versus personal data. If personal data is used, that decision must involve stakeholder consultation and senior management consideration. The organisation must also clearly document its reasons for using personal data.

In allowing this margin of discretion, the AI Guidelines illustrate the PDPC’s overarching support for a pro-responsible business, pro-innovation approach in its regulation of personal data and governance of trustworthy AI. That position is consistent with – and indeed, builds upon – the introduction of the Business Improvement Exception and other amendments in 2020 through the Personal Data Protection (Amendment) Bill.

### **Consent and notification obligations in AI deployment**

The AI Guidelines reinforce the importance of the PDPA’s consent and notification obligations in the deployment of AI systems that form recommendations or decisions based on personal data.

The AI Guidelines state that organisations must enable individuals to provide meaningful consent for the collection, use, or disclosure of his personal data in such AI systems. In practical terms, this means that an organisation must notify them of the function of the product or service that requires the collection of their personal data; the types of personal data collected; and the specific features of personal data that are likely to influence the product feature.







At the same time, the AI Guidelines also allow organisations a margin of discretion. They state that where an organization evaluates that it is necessary to omit any of the above information due to commercial sensitivity or intellectual property protection, the organisation may limit critical details, or provide a general explanation of the information cited above. However, the organization must justify and document internally the reasons for its decision. Thus, in the deployment of AI systems, as in their development, the AI Guidelines demonstrate the PDPC's innovation-friendly approach in the regulation of personal data for AI use.

### **Accountability obligation in AI deployment**

The AI Guidelines also emphasise the importance of the PDPA's accountability obligation – an organisation's duty to take and demonstrate responsibility for the personal data in its possession or control. In the deployment of AI systems involving personal data, this obligation entails the development of written policies to ensure the appropriate use of such data: a use consistent with purposes that individuals have consented to, or with another legitimate purpose.

The AI Guidelines also recommend that an organisation's policies should contain measures to ensure the proper use of personal data. Examples include measures to ensure that AI systems provide fair and reasonable recommendations, such as recommendations free from bias; technical safeguards to protect personal data, such as pseudonymisation or data minimisation; and – for higher-impact cases – information on how adequate accountability mechanisms and human oversight have been implemented.

### **Procurement of AI systems**

The AI Guidelines state that where service providers process personal data on their customers' behalf in order to help develop or deploy AI systems, such service providers may

occupy the role of data intermediaries. In that capacity, they must comply with the PDPA obligations that apply to data intermediaries: firstly, to implement strict measures to protect personal data from unauthorised access or use; secondly, to retain personal data only insofar as necessary to fulfil a legal or business need or the purpose for which it was collected; and thirdly, to report data breaches to the organisation they are processing personal data on behalf of.

The AI Guidelines also recommend that such service providers must support their customers, to help such customers comply with their own notification, consent, and accountability obligations. In particular, service providers should understand the information that their customers are likely to need, in order to comply with these obligations. Service providers should also design systems that can extract such information.

At the same time, the AI Guidelines emphasise that the primary responsibility for ensuring AI systems comply with these obligations rests with the organisation itself. In making this point, the AI Guidelines underscore the importance that the PDPC places in holding organisations accountable to their PDPA obligations. Organisations cannot avoid or reduce their obligations by engaging third parties to develop or deploy their AI systems.

### **Children's Data Guidelines**

Following a public consultation in 2023, the PDPC issued in March 2024 its Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment (*CD Guidelines*). The CD Guidelines apply to organizations whose online products or services are likely to be accessed by children. This is broader than products or services designed for and aimed specifically at children, but rather, are those that children access in reality. The CD Guidelines clarify that consent from parents or legal guardians are



required for children under 13 years old. For children between 13 and 17, their consent is only valid if the policies on data processing and how consent can be withdrawn are easily understandable by them.

The CD Guidelines recognise and support the use of age assurance methods, such as age verification or estimation to ascertain a user's age. Organisations must, however, ensure that data minimisation is adhered to, such that only personal data which is necessary to ascertain a user's age is collected.

While not explicitly prescribed in the PDPA, the CD Guidelines allude to children's personal data being of a greater sensitivity for which a higher standard of protection is warranted. To this end, it is advised that a data protection impact assessment be conducted before released products or services likely to be accessed by children, and the CD Guidelines include a list of sample questions to consider when conducting such assessment.

## Privacy-enhancing Technologies

A Proposed Guide on Synthetic Data Generation was launched in July 2024, to aid organisations in understanding potential use cases particularly for AI. This is a further step in PDPC's push towards promoting the deployment of privacy-enhancing technologies (*PETs*) starting with its regulatory sandbox for *PETs* launched in 2022. Practical guidance has also been issued in response to a social media provider's request, which references the use of multiparty computing and differential privacy for attributing digital advertising impressions and conversions.

## Notable enforcement cases

2024 saw an aggregate of S\$421,800 being imposed as financial penalties for breaches of the PDPA in 13 different cases. The vast majority of these involved infringements of the protection obligation in section 24 of the PDPA, which requires organisations to make

reasonable security arrangements to prevent any unauthorised processing of personal data in an organization possession or control. Notably, 2024 also saw an unprecedented increase in the take-up of voluntary undertakings by organisations, as a means to demonstrate remediation compliance in place of a full investigation and financial penalties by the PDPC for data breaches. While there were in total 15 enforcement decisions published by the PDPC last year, there were a whopping 44 accepted undertakings from organisations that potentially contravened the PDPA, but which promise implementation of specific remediation and rectification measures in exchange for the PDPC's dropping any further regulatory investigation or action. The above offers insights about the PDPC's implicit philosophy in enforcing breaches of the PDPA.

## Court decision on PDPA

On November 12, 2024, the District Court of Singapore issued its decision in *Martin Piper v Singapore Kindness Movement*, which arose from a claim by the plaintiff that the defendant had contravened the consent and purpose limitation obligations in the PDPA, and that he had suffered financial loss and emotional distress as a result.

The case facts were as follows. The plaintiff had sent an email from his personal address to the defendant, which is a registered charity in Singapore, asking that allegedly discriminatory messages about the plaintiff be removed. These messages were sent by the co-founder of the defendant's affiliate. After extensive email exchanges between the defendant and the plaintiff on the one hand, and the defendant and the co-founder on the other, the defendant eventually emailed the co-founder asking her to respond to the plaintiff directly. In this email to the co-founder, the defendant appended the various emails it had exchanged with the plaintiff. The plaintiff brought a claim alleging that by disclosing his name and email address

to the co-founder, the defendant had breached the consent and purpose limitation obligations in the PDPA, which led to his suffering loss and damage including emotional distress.

The Court held that there was no contravention of the PDPA by the defendant. In particular, the plaintiff was deemed to have given his deemed consent for his identity to be disclosed to the co-founder with a view to removing the allegedly discriminatory messages from the group chat. The conditions for deemed consent to operate under the PDPA were found to be met; namely, the plaintiff had voluntarily provided his identity to the defendant; and it was reasonable for him to have done so to facilitate the defendant's investigation into the matter. Additionally, the Court noted that the plaintiff did not at any time request for his complaint to be anonymised, despite it being open to him to have done so.

Finally, the Court considered that even if there had been a breach of the PDPA (which was not the case here), the plaintiff had failed to prove that he suffered loss or damage that was caused by the alleged contravention of the PDPA. Such causal link must be made out before damages can be awarded in a private action under the PDPA, and this echoes the position taken by the Singapore Court of Appeal in an earlier judgment, *Reed, Michael v Bellingham, Alex* in 2022.

## Thematic observations

Singapore continues to see a very high level of enforcement activity by the PDPC, which remains one of the most active data protection regulators in the region to-date. The publishing of the PDPC's enforcement decisions allow us to understand the considerations that are applied by the PDPC in any finding of a contravention as well as award of a financial penalty. In particular, section 48J of the PDPA requires the following salient aspects to be considered in the award of financial penalties for failures to protect personal data: the gravity









of a PDPA infringement, the volume, type and nature of personal data involved, and the extent to which the organisation has demonstrated its accountability for responsible data use.

At the same time, the PDPC decisions take care to cite mitigating factors, including prompt remedial action and the voluntary acknowledgement of failures made by each organisation. Moreover, the financial penalties above, while material, appear unlikely to undermine the financial viability of each of the organisations involved. In these respects, these decisions suggest the PDPC's overarching aim to ensure that companies are proportionately, not unduly, penalised for non-compliance with the PDPA. That objective in turn appears consistent with the PDPC's broader aim – of maintaining a regulatory environment that supports commercial innovation through the responsible use of personal data.

## **Amendment to Cybersecurity Act**

Singapore's forward-looking approach to tackling the rise of cybersecurity threats was reflected in an amendment to its Cybersecurity Act in May 2024.

The changes effected by this amendment:

- (a) Update the obligations on critical information infrastructure ("CII") owners to encompass new technological and business models, such as the use of cloud computing. CII owners will now be required to report to the CSA more types of cybersecurity incidents, including those that affect their supply chains. CII is prescribed as the following 11 sectors in Singapore: energy, water, banking and finance, healthcare, transport (land, maritime and aviation), info-communications, media, security and emergency services, and Government.
- (b) Expand Singapore's Cybersecurity Agency ("CSA")'s oversight to cover new classes of regulated entities, namely Systems of

Temporary Cybersecurity Concern (i.e. computer systems that are of higher risk due to temporary events or situations); Entities of Special Cybersecurity Interest (i.e. that hold sensitive information or perform a function of national interest); and Foundational Digital Infrastructure (i.e. cloud service providers and data centres).



# Australia

2024 marked the initial phase of Australia's long-anticipated privacy law reforms, following the government review of the Privacy Act 1988 (*Privacy Act*) in 2023.

In December 2024, the Privacy and Other Legislation Amendment Bill 2024 (Cth) (the *Privacy Amendment Bill*), as passed by the Senate in November 2024, received Royal Assent. The Privacy Amendment Bill introduced major amendments to the Privacy Act, some of which had already come into effect.

Notable amendments to the Privacy Act under the Privacy Amendment Bill include, amongst others:

- A brand-new statutory tort for serious invasions of privacy: this would allow individuals to commence legal proceedings against individuals or organisations for serious invasions of privacy where the alleged conduct under question was intentional or reckless.
- A new criminal offence for doxxing: it will be illegal to share personal information of any person with the intention to harm, punishable by up to 7 years' imprisonment.
- Sanctions for other privacy breaches: civil penalties will range from AUD 330,000 to AUD 50 million depending on the seriousness of the breach.
- Setting the scene for a Children's Online Privacy Code: the Office of the Australian Information Commissioner ("OAIC") is statutorily required to develop a code to address privacy concerns for children online.
- Transparency obligations for automated decision-making: organisations will be required to update their privacy policies to

disclose the making of decisions which used automated processes.

In late November 2024, the Cyber Security Act 2024 (Cth) (CSA) received Royal Assent as well, further implementing the 2023-2030 Australian Cyber Security Strategy.

*The key features of the CSA include:*

- Ransomware reporting: where a ransomware payment is paid, there are mandatory requirements to make reports to the Department of Home Affairs.
- Cyber Review Board: significant cybersecurity incidents will be reviewed by the Cyber Review Board on a no-fault basis.
- Limited use exception: to foster collaboration between the government and industry stakeholders during cyber incidents, the CSA includes provisions which restrict the use of information provided to certain governmental departments on a voluntary basis.
- Security standards for smart devices: the CSA imposes obligations on manufacturers and suppliers of smart devices to ensure such devices meet certain security standards where there is intention to make them available in Australia. Examples of these obligations include the production of a statement of compliance to confirm that the devices do meet certain requirements under the relevant standards.

In 2024, there had been continued emphasis on AI as it interacts with privacy and data security. Notably, on October 21, 2024, the Office of the Australian Information Commissioner ("OAIC") published two guidelines:

- Guidance on privacy and developing and training generative AI models (*Developer AI*

*Guidance*): encourages developers seeking to use personal information to develop and train AI models to, amongst other things: (i) ensure accuracy through using quality data sets and proper testing; (ii) recognise privacy risks in web-scraping; (iii) obtain consent where sensitive information is scraped online or obtained from third-party datasets; and (iv) assess the purpose and legal basis for using existing personal data, ensuring individuals can withdraw consent if needed. Guidance on privacy and the use of commercially available AI products (*Business AI Guidance*): advises businesses to ensure privacy by, amongst other things: (i) conducting due diligence on AI products; (ii) transparently informing users about AI's personal information usage; and (iii) adhering to Australian Privacy Principles (APP) regarding data collection. It also emphasises the need for explicit consent for AI training and warns against entering sensitive data into public AI tools.

We expect Australian regulators will continue to work closely with its overseas counterparts. In 2023, the Australian Signals Directorate jointly released cybersecurity guidance on Secure-by-Design memory safe roadmaps, in partnership with the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NCSC-NZ) and Computer Emergency Response Team New Zealand (CERT NZ) and United Kingdom's National Cyber Security Centre (NCSC-UK). There is a strong emphasis on requiring technology providers and software manufacturers to prioritise design and implementation practices to minimise customer risk and vulnerabilities in their products.







## South Korea

South Korea has firmly established itself as one of the toughest jurisdictions for data protection and privacy compliance in APAC. Provisions of the over-arching Personal Information Protection Act (*PIPA*) and the IT Network Act are supplemented by sector-specific laws, creating a very difficult compliance environment.

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

The PIPA is well known for its requirement of separate, unbundled consents for a number of data collection and processing contexts, including international transfers of personal data (save in limited circumstances where international transfer is permissible without consent), and the need to notify data subjects of the specific identity of data processors. Relatively uniquely for the APAC region, the PIPA does provide some scope for "legitimate interests" processing of personal data without data subject consent (although, this is narrower than the "legitimate interests" under the GDPR).

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

In February 2023, the National Assembly passed the proposed amendments to the PIPA (the *Amendment Act*), which later took effect.

Notably, the key features of the Amendment Act are, amongst other things:

- New data portability right: a data subject will have the right to request that a data controller, which meets specific, transfer personal data to a government-designated specialised personal data management agency or another data controller that meets similar standards (to be defined).
- The Personal Information Protection Commission ("PIPC"): under the Amendment Act, the PIPC will be granted the additional power to order a data controller to suspend cross border transfers of personal data in the event that it determines such transfer breaches the PIPA or where there is a high risk of harm to data subjects.



# Japan

There was significant movement in 2024 with respect to Japan's treatment of data protection and cybersecurity regulation.

## Expansion of cases requiring security measures and data incident reporting

The Act on the Protection of Personal Information (*APPI*) distinguishes “personal information” and “personal data”. Under the APPI, “personal information” means information that can identify a specific individual and “personal data” means “personal information” compiled into a personal information database or the equivalent. Under the APPI and the Ordinance for the enforcement of the APPI, in the context of handling “personal information” that is not “personal data”, there is no explicit requirement to: (i) take appropriate measures necessary for security management; and (ii) report incidents when they occur.

As such, the current system does not provide adequate safeguards or measures against web skimming or similar attacks when “personal information” is targeted or stolen before it is compiled into a database or the equivalent and becomes “personal data”. Due to an increase in web skimming and similar attacks, effective since April 1, 2024, businesses handling “personal information” now need to: (i) take necessary and appropriate measures to manage not only “personal data” but also “personal information” that is expected to be handled as “personal data”; and (ii) report incidents involving “personal information” that is expected to be “personal data”.

In the current triennial review, the upcoming amendment of the APPI is under discussion. An interim report regarding the potential amendment was published to invite public opinions at the end of 2024 and details of the potential amendment are expected to be announced later in 2025.

## Cybersecurity measures requirements in the finance sector

On October 4, 2024, the Financial Service Agency (*FSA*) issued Guidelines on Cyber Security in the Financial Sector (*Guideline*), which stipulates specific rules in respect of cybersecurity requirements for most of the finance sector under the supervision of the FSA.

The FSA will continue to inspect and monitor on a risk-based approach based on the size and nature of each business, and evaluates the cybersecurity management system of each business to promote the enhancement of cybersecurity measures. The Guideline includes the following sections: (i) basic approach; (ii) establishing a cybersecurity management system; (iii) identifying cybersecurity risks; (iv) defending against cyber attacks; (v) detecting cyber attacks; (vi) responding to and recovering from cyber incidents; and (vii) managing third-party risks. This Guideline imposes more detailed obligations than before, and the financial businesses is required to implement “basic measure” (i.e. businesses generally need to implement, also known as, “cyber hygiene”). It also indicates “desirable measure” (i.e. businesses should implement in light of the nature of the business, including best practices) in addition to the basic measures.

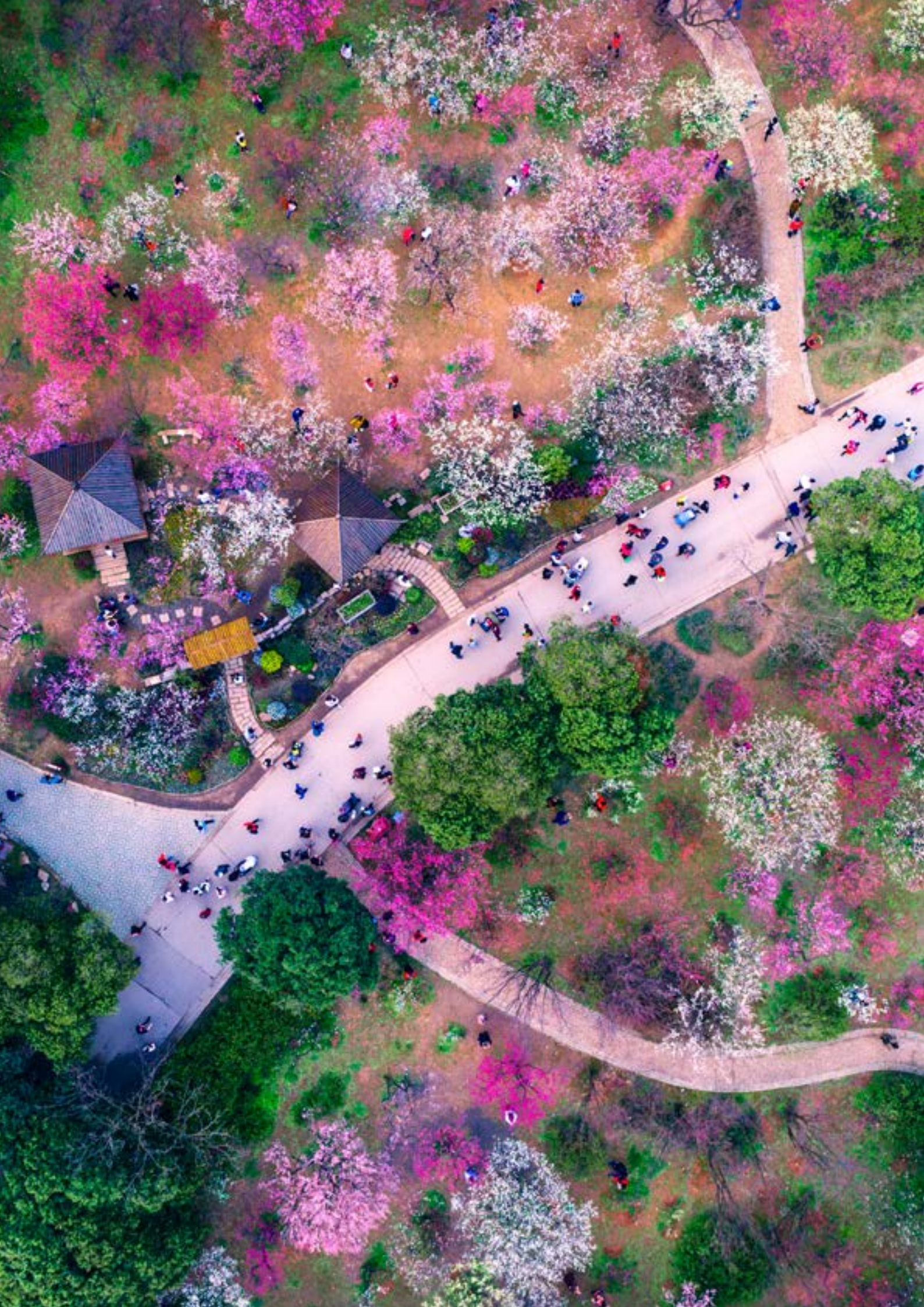
Please note that following items are not an exhaustive list.

- In respect of (i), this guideline is applicable to most businesses in the finance sector, including but not limited to major banks, insurance companies, financial institutions, money lenders, financial service intermediaries and crypto asset exchange businesses.

- In respect of (ii), businesses are required to establish basic policies, regulations, rules and processes, develop human resources, and have internal audits and risk management departments review and inspect.
- In respect of (iii), businesses are required to manage information assets (e.g. information systems, external system services, hardware, software, data and dataflow), develop a risk management process (e.g. collect and analyse threat and vulnerability information, identify and evaluate risks, consider how to respond and continuously improve the process), manage vulnerabilities in hardware and software, diagnose vulnerabilities, conduct penetration tests, and conduct drills and training.
- In respect of (iv), businesses are required to formulate policies and regulations regarding authentication and access rights, provide security training to employees and directors, formulate data management policies and implement system security measures (e.g. manage hardware, software and log, and implement “security by design”, technical measures for infrastructure (networks, etc.) and technical measures for cloud services).
- In respect of (v), businesses are required to monitor hardware, software and networks to detect cyber attacks.
- In respect of (vi), businesses are required to develop incident response and contingency plans and follow guides regarding initial response, analysis, customer support, collaboration within and outside the organization, public relations, eradication and recovery.
- In respect of (vii), businesses are required to manage cybersecurity risks in respect of all supply chains.









## Amendment of the Information Distribution Platform Act

The Information Distribution Platform Act (“IDPA”), which is expected to come into effect on April 1, 2025, serves as an amendment to the current so-called Provider Liability Limitation Act (“PLLA”). The PLLA is often invoked by those whose rights have been infringed on the internet against online platform operators to obtain contact information relating to the infringers (e.g. name of the relevant account holder and email address).

The IDPA will impose large-scale platform operators (designated by the authority based on the average number of monthly active users in Japan or the average total number of active monthly users, etc.) additional obligations requiring them to: (i) speed up their response to deletion requests; and (ii) increase transparency in the deletion process. These additional obligations will help users to protect their rights online by facilitating access to the potential infringer’s information.

- In respect of (i), large-scale platform operators are required to: (a) define and publicise the method of responding to deletion requests; (b) establish an operational system that handles deletion requests (e.g. designate individuals with sufficient knowledge and experience); and (c) define the schedule of the deletion process within 7 days of the relevant request.
- In respect of (ii), large-scale platform operators are required to: (a) publish deletion guidelines and the operational status (e.g. number of requests received); and (b) take measures such as notifying the relevant person when the requested deletion is made.

## Cyber Security Capability Enhancement Act

On 16 May 2025, the Act on the Prevention of Damage Caused by Unauthorized Acts Against Important Electronic Computers

(commonly referred to as the Cyber Security Capability Enhancement Act) and other relevant legislation were passed by the Diet. The Act, which aims to strengthen protections for critical electronic infrastructure, is expected to come into force by the end of 2026 (though the exact date has yet to be determined). The purposes of the Acts are: (i) to strengthen the partnership between the Government and businesses; (ii) to enable the Government to acquire the analysis in respect of telecommunications information; and (iii) to implement measures to infiltrate and neutralise the source of cyber attacks. Recently, a lot of attention is being drawn to these Acts as they allow active cyber defence (i.e. neutralising the attacking servers as needed), which is not allowed under the current Japanese laws and regulations. We will continue to publish client alerts on the progress of these Acts as new developments emerge. Please subscribe to Hogan Lovells’ thought leadership platform “Our Thinking” to receive these updates.

## Amendments relating to the life sciences sector

Finally, we set out below a summary of the 2023 updates in the life sciences sector. The life science business environment in Japan has changed significantly due to the pandemic and technology developments. As such, regulations are or will be updated from various aspects as follows.

### *(a) Reinforced cybersecurity for medical/health institutions*

Effective since April 1, 2023, under the amended Ordinance for the enforcement of the Medical Care Act, administrators of hospitals, clinics, or birthing centres must take necessary measures to ensure cybersecurity to prevent the risk of significant disruption to the provision of healthcare. This amendment was due to the recent increase in cyberattacks



against medical institutions and the risk of significant damage, such as leakage of patients' personal information related to medical care.

In relation to the above, on May 31, 2023, the Guidelines for safety management of medical information systems 6.0 (the *Guidelines*) were updated and published and medical institutions etc. are expected to take "necessary measures" in accordance with these Guidelines. The Guidelines consist of an "Overview" section and "Governance", "Management" and "Control" sections divided for the respective intended readers.

The key updates to the Guidelines were to: (i) organise the use of outsourcing and external services; (ii) organise the concept of information security; and (iii) respond to new technologies and changes in systems and standards.

- In respect of (i), the Guidelines provide, for example, the approach to considering risks and countermeasures based on the features of cloud services, the arrangement of responsibilities, etc. corresponding to each type of system of medical institutions, etc.
- In respect of (ii), the Guidelines provide, for example, responses and countermeasures in the case of emergency situations, the usefulness of adopting a zero trust security model, etc.
- In respect of (iii), the Guidelines address, for example, the utilisation of eKYC (electronic Know Your Customer), potential use of new network technology (e.g. local 5G) and trends of regulations regarding sharing medical information.

*(b) Reinforced cybersecurity for medical devices*

Effective since April 1, 2024, new cybersecurity measures must be taken for

medical devices using programmes that are used in connection with other devices and networks, etc., or medical devices that may be subject to unauthorised access and attack from outside, under the amended Standard for Medical Devices specified by the Minister of Health, Labour and Welfare, based on Article 41 Paragraph 3 of the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices.

According to the new amendment, appropriate requirements must be specified based on the operating environment and network usage environment of such medical devices, and controls must be in place to identify and evaluate risks related to cybersecurity that may interfere with the functions of such medical devices or cause safety concerns, in addition to reducing such risks. Further, such medical devices must be designed and manufactured based on a scheme that can ensure cybersecurity throughout the device's entire life cycle.

*(c) Flexible usage of medical/health information*

Effective since April 2024, use restrictions on data related to medical or health information have become more relaxed under the amended Act on Anonymised Medical Information for the Purpose of Contributing to Research and Development in the Medical Field, also known as, the Next-Generation Healthcare Infrastructure Act. The key points of the amendment are: (i) introduction of a new concept "Pseudonymised Medical Information"; (ii) linkage with public databases; and (iii) establishment of provision for businesses handling medical information to make efforts to cooperate with national policies.

- In respect of (i), Pseudonymised Medical Information is medical information relating to an individual that is processed so that it cannot identify a specific individual unless collated with other information. In

contrast, Anonymised Medical Information is medical information relating to an individual that is processed so that it cannot identify a specific individual and the personal information is non-restorable. The purpose of introducing the concept of Pseudonymised Medical Information is to address the needs of certain medical information that cannot be satisfied by Anonymised Medical Information, such as, provision of data relating to a rare condition of illness.

- In respect of (ii), linkage of Anonymised Medical Information and public databases, such as the national database enable more sophisticated research and development. For example, it may be used to ascertain the types of medical examinations that were conducted at other clinics before and after a hospital visit.
- In respect of (iii), due to the small number of cooperating institutions and lack of medical information provided, a new effort provision was established.









# Indonesia

2025 marks the new phase of Indonesia's Law No. 27 of 2022 on Personal Data Protection (*PDP Law*) as the sunset period of it ends on October 2024 where all obligations thereto have become effective. The law aims to raise awareness among the public about the significance of protecting personal data. While the PDP Law outlines general provisions for data protection, more specific details are expected to be added through a government regulation.

While PDP Law enters into the formal implementation phase, there are certain practical uncertainties. This is due to PDP Law only outlining general provisions for data protection, while the specific details are expected to be added through a more technical regulation.

As of the date of this update, Indonesian government has yet to formally enact the implementing regulation of PDP Law in the form of Government Regulation (*Draft Regulation*). The Draft Regulation is currently under review and expected to bring more clarity on the practical aspects of the PDP Law. It is still unclear when the government will pass the Draft Regulation into a formal law.

Although subject to potential changes, the Draft Regulation spans 188 pages with 245 articles. Below is a brief summary of some key matters addressed in the Draft Regulation:

## **Classification of personal data: specific personal data**

Under the PDP Law, Indonesia now recognizes two types of personal data: specific and general. Specific personal data includes health, biometrics, genetics, crime records, children's information, personal financial details, and other data as per existing laws. The Draft Regulation specifies that determining "other data" considers the potential impact on the

individual, such as discriminatory actions, losses, or other impacts against the laws.

Processing specific personal data is considered high risk under the law, requiring the Data Controller to conduct a data protection impact assessment (*DPIA*) before carrying out such activities. More details on DPIA will be discussed below.

## **Data Protection Impact Assessment**

The Data Controller must perform a DPIA if it processes personal data with a high-risk potential impact on the individual. This includes automated decision-making with legal consequences, processing specific personal data, large-scale data processing, systematic evaluation or monitoring of individuals, matching or merging data groups, using new technology, or processing data that limits the individual's rights. It's crucial to note that the DPIA should be conducted before the Data Controller carries out any processing activities.

In accordance with the Draft Regulation, the DPIA should include a systematic description of the data processing activities and their purposes, an assessment of the necessity and proportionality of the processing, an evaluation of the risks to the individual's rights, and the measures the Data Controller takes to protect the individual from these risks.

If the Data Controller has a data protection officer (*DPO*), the DPO's input should be considered and documented during the DPIA implementation. More information on the DPO will be discussed later.

Additionally, the Data Controller has other obligations regarding the DPIA, such as revisiting it if there is a change in the risk of data processing activities, implementing the measures mentioned above during processing activities, and keeping records of the DPIA and these measures.



## Data Protection Officer

The Draft Regulation emphasises that a Data Controller and Data Processor must appoint a DPO under certain circumstances. These include processing personal data for public service, engaging in core activities involving regular and large-scale systematic monitoring of personal data, and conducting large-scale processing of personal data related to specific personal data and/or criminal offenses. All three conditions must be met for DPO appointment to be mandatory. However, this viewpoint may change when the Draft Regulation is formally issued as a government regulation.

The DPO should be chosen based on their professionalism, legal knowledge, expertise in data protection practices, and their ability to perform their duties. The appointment should align with the organisational structure, size, and needs of the Data Controller and/or Data Processor. The DPO can be an individual or several persons from inside and/or outside the organisation.

The minimum tasks of a DPO include informing and advising the Data Controller or Data Processor to comply with laws and regulations on personal data protection, monitoring and ensuring compliance, providing advice on impact assessments, and coordinating and acting as a contact person for personal data processing issues.

In fulfilling the DPO's tasks, the Data Controller and Data Processor are required to involve the DPO correctly and promptly in all personal data processing matters, provide reporting access to the highest management level, ensure the DPO operates objectively and is protected from dismissal or penalties, allocate adequate resources and expertise, grant appropriate access to processing activities, provide access to other services for essential information, seek advice for personal data protection impact

assessments, and document the details and activities of the DPO.

## Offshore personal data transfer

Prior to the enactment of PDP Law, Indonesia permitted the transfer of personal data to other countries. Generally, Data Controllers needed to follow specific requirements for offshore data transfer:

1. Ensure that the recipient country's data protection level is equal to or higher than that under the PDP Law.
2. If (1) cannot be met, the Data Controller must establish adequate and binding protection, similar to Binding Corporate Rules (BCR) under GDPR.
3. If both requirements under (1) and (2) cannot be satisfied, the Data Controller needs a consent from Data Subjects for the transfer.

Concerning point (1), the Draft Regulation specifies that data protection agency that will be authorised and tasked to supervise the implementation of PDP Law (*Agency*), which has not been yet established as of now, will determine if a country provides an equal or higher level of personal data protection. It is expected that the Agency will issue a list of such countries.

Even without the list, the Draft Regulation outlines the framework for the determination process. This involves checking if the receiving country has a personal data protection legal framework, a supervising agency for data protection, and international commitments related to personal data protection. How these measures will be carried out is currently unclear, possibly relying on a self-assessment by the Data Controller.

If the receiving country does not meet Indonesia's data protection standards, the Data

Controller must guarantee adequate and binding personal data protection, similar to BCR under GDPR. If these obligations cannot be fulfilled, the Data Controller needs the Data Subject's consent for the offshore transfer, subject to certain conditions such as non-recurring transfers, involving a limited number of Data Subjects, being necessary for specific purposes, assessing risks, informing the PDP Agency and the Data Subject, and fulfilling legitimate interests.

## **Mandatory notification**

There are several mandatory notifications that need to be submitted to the data subject, among others:

### *Personal Data Protection Failure*

If there is a failure in protecting personal data, the Data Controller must notify the Data Subject and the Agency within 72 hours of being certain about the incident. This notification should include information about the disclosed personal data, how and when it was disclosed, the impact, recovery efforts, and a contact person. If no personal data was disclosed during the breach, the Data Controller is not required to file the notification

The Draft Regulation also introduces a new obligation for the Data Controller to inform the public if the breach disrupts public services, has a serious impact on the public's interests, or if the Data Subject cannot directly receive the notification. Additionally, the Data Controller must record the breach and have policies, procedures, and guidelines for preventing and handling personal data breaches.

### *Corporate Actions of Data Controller*

The Draft Regulation specifies that the current Data Controller must inform Data Subjects before a merger, separation, acquisition, or consolidation. This notification, made before the completion of such actions, should include







information about the transfer of personal data to the new Data Controller, data processing activities related to the corporate action, the name and contact information of the new Data Controller, procedures for objecting to data transfer, when data processing will start, access to personal data by the new Data Controller and relevant parties, and a statement that the current Data Controller will erase transferred personal data at the end of the corporate action.

During the corporate action, the current and new Data Controllers will be joint Data Controllers and must establish an agreement governing the rights and obligations related to the transfer of personal data.

#### *Indonesia's Future Personal Data Protection Agency*

As to regulate further Agency's conducts in supervising the implementation of personal data protection in Indonesia, the Draft Regulation specifies that the Agency's tasks are to:

- a) Formulating and stipulating policies in the field of personal data protection;
- b) Supervising the compliance of Data Controller to the relevant regulations;
- c) Imposing administrative sanctions for violations committed by Data Controller and/or Data Processor;
- d) Assisting the law enforcement officials (i.e., carried out through giving opinions and recommendations) in handling allegations of Personal Data criminal offenses as referred to in this bill;
- e) Cooperating with personal data protection institutions of other countries in order to resolve alleged violations of cross-border personal data protection;
- f) Conducting an assessment of the fulfilment of the requirements for the transfer of Personal Data outside the jurisdiction of the Republic of Indonesia;
- g) Giving orders in the context of follow-up on the supervision results to the Data Controller and/or Data Processor;
- h) Publishing the results of the supervision of personal data protection in accordance with the provisions of laws and regulations;
- i) Receiving complaints and/or reports regarding alleged violations of personal data protection;
- j) Conducting examination and tracking of complaints, reports, and/or supervision results on the alleged violation of personal data protection;
- k) Summoning and present any person and/or public body related to the alleged violation of personal data protection;
- l) Requesting information, data, and documents from any person and/or public entity related to the alleged violation of personal data protection;
- m) Summoning and present experts required in the examination and investigation related to the alleged violation of personal data protection;
- n) Conducting examination and search of electronic systems, facilities, spaces, and/or places used by the Data Controller and/or Data Processor, including obtaining access to data and/or appointing third parties; and
- o) Requesting legal assistance to the prosecutor's office in the settlement of disputes over personal data protection.



Noting the above tasks, it is worth closely monitoring the formal establishment of the Agency which as of the date of this article, has yet to be formed by the Indonesian government.

### *Administrative Sanctions*

In line with the PDP Law, the Draft Regulation specifies that administrative sanctions will be then imposed by the Agency for non-compliance to the provisions relating to personal data protection. These administrative sanctions include:

- a) Written reprimand;
- b) Temporary suspension of personal data processing activities;
- c) Deletion or destruction of personal data; and/or
- d) Administrative fines – the amount shall be a maximum of 2 (two) percent of the annual revenue or annual receipt in relation to the violation variable (e.g. impact, duration, type and number of affected data/person, scale of business).

The imposition of administrative sanctions shall be carried out by considering the Data Controller's or Data Processor's extent or effect of the breach, the business continuity, compliance history, and clear considerations and reasons.

Particularly for the imposition of administrative fines by the Agency, if the non-compliant Data Controller or Data Processor is not willing to pay the determined amount, the Agency is authorized to coordinate with other law enforcers to collect such fines, to be further stored as non-tax state income.

### *Dispute Resolution*

Under the Draft Regulation, any dispute arising between Data Subject, Data Controller, or Data

Processor may be reported to the PDP Agency. The report shall be made in writing and shall provide accurate and complete documents and information pertaining to the issue of the dispute. The report will then become a basis for the PDP Agency to verify the documents and information.

### *Mediation Mechanism*

The Draft Regulation would mandate that dispute resolution through mediation is prioritized. This mediation will be facilitated by the PDP Agency based on the report and verification result. However, if the nature of the dispute is not within the competence of mediation, or the disputing parties have previously determined the dispute resolution mechanism in the agreement, then settlement through mediation by the PDP Agency shall be exempted.

The mediation process shall be carried out within 30 (thirty) days from the first meeting of mediation. This period is subject to additional 30 (thirty) working days' extension based on a mutual agreement of the disputing parties and is submitted to the Head of PDP Agency no later than 7 (seven) days before the end of mediation period, accompanied by:

- a) Agreement to extend the mediation period; and
- b) Reason for the extension.

If the disputing parties were unable to resolve the dispute within the extension period above, the Draft Regulation authorises the mediator to declare that the mediation proceedings have failed. In this case, the Head of PDP Agency will inform the disputing parties that they may proceed to arbitration or lawsuits in the courts.

Please note that the above might still subject to changes as the Draft Regulation is not in its final form. It is worth to watch the development

of the Draft Regulation closely as it will have an impact on the way businesses navigate their conduct to ensure compliance with the prevailing laws and regulations.







# Vietnam

The Vietnamese Government has recently promulgated a number of normative documents implementing the 2025 national cybersecurity strategy with a vision to 2030 as outlined in Prime Minister Decision No. 964/QĐ-TTg, which together creates a new regulatory framework for data protection and cybersecurity. At the time of publication of this guide, the legal framework for data privacy and information security includes: (i) Law No. 86/2015/QH13 dated November 19, 2015 on Cyber Information Security, as amended by Law No. 35/2018/QH14 dated November 20, 2018 (*Law on Cyber Information Security*); (ii) Law No. 24/2018/QH14 dated June 12, 2018 on Cybersecurity (*Law on Cybersecurity*) and Decree No. 53/2022/ND-CP dated August 15, 2022 of the Government detailing certain articles of the Law on Cybersecurity (*Decree 53*); (iii) Decree No. 13/2023/ND-CP dated April 17, 2023 of the Government on personal data protection (*Decree 13*); (iv) Decree No. 147/2024/ND-CP dated November 9, 2024 on the management, provision and use of internet services and cyberinformation (*Decree 147*); (v) Law No. 60/2024/QH15 dated November 30, 2024 on Data (*Law on Data*); and (vi) Decree No. 24/2025/ND-CP dated February 21, 2025 amending Decree No. 98/2020/ND-CP on administrative penalties in various sectors, including commerce, production and trade in counterfeit and prohibited goods, and protection of consumer rights (*Decree 24*).

The increasing pace of legal and regulatory developments has combined to create substantial compliance challenges for both foreign and domestic information technology service providers with clients in Vietnam. Below, we provide an overview and introduction of this framework.

## 1. Law on Cyber Information Security

The Law on Cyber Information Security became effective on July 1, 2016 and

primarily regulates cyber information security, personal data protection, classification of information systems, and information conflict monitoring. The Law on Cyber Information Security was the most detailed and comprehensive law on personal data protection in Vietnam until the promulgation of Decree 13.

### 1.1 Responsibilities of information system owners

The Law on Cyber Information Security requires information system owners to observe key responsibilities of: (i) determining information security levels; (ii) assessing and managing security risks; (iii) ensuring adequate protective and monitoring measures; and (iv) following a mandatory reporting regime with respect to their information systems. The Law on Cyber Information Security establishes a five-tier classification of information security systems, with classifications reflecting the potential harm that a cybersecurity breach could cause to other entities, social order, and national security. Private-use information systems may only be classified as up to Tier 3, and shall not be subject to further appraisal and approval from government agencies. For example, providing online information services which are classified as “conditional business services” or that process private or personal information of 10,000 users or more would be classified as Tier 3.

### 1.2 Personal data protection

The Law on Cyber Information Security restates and emphasises the core principle of consent under existing data privacy regulations: there must be prior informed consent from the data subject for the collection, processing, and use of personal data. The Law on Cyber Information



Security previously prescribed rights and obligations on updating, amending, or deleting personal data, and data processors were entitled to certain statutory deferrals for reporting cybersecurity incidents, such as due to “technical reasons” or “other reasons”. However, Decree 13 now supersedes these more flexible provisions and mandates a strict 72-hour response time as described below.

### 1.3 Cyber information protection

Depending on the industry sector, the Law on Cyber Information Security mandates certain obligations on: (i) managing information delivery; (ii) preventing, detecting, blocking and handling malware; (iii) ensuring the safety of telecommunications resources; and (iv) responding to data security breaches on an extra-territorial basis. For example, the Law on Cyber Information Security requires that internet service suppliers must coordinate with competent state authorities to prevent and handle any cyber information security threats originating from their Internet resources or customers upon request, and to work to ensure the safety and stability of server systems using Vietnam’s national domain name (.vn). Within 5 (five) days from the date of occurrence of a data security breach, system information operators must send written notice of the breach to both information system owners and to the Vietnam Computer Emergency Response Team (VNCERT).

## 2. Law on Cybersecurity and Decree 53

The Law on Cybersecurity was enacted effective on January 1, 2019, with the policy goals of enhancing national security in cyberspace with stringent rules regulating online speech, data localisation and combating cybercrimes. Four years after the enactment of the Law on Cybersecurity, the Government provided further guidance on

its implementation with the enactment of Decree 53.

### 2.1 Data localisation

The Law on Cybersecurity generally requires both domestic and foreign service providers to store data in Vietnam for a specified period of time if they: (i) provide services through a telecoms network, the internet and value-added services on cyberspace in Vietnam (*Cyberspace Service Providers or CSPs*); or (ii) are involved in the collection, exploitation, analysis or processing of personal information, data about users’ relationships, or data generated by users in Vietnam. Decree 53 further specifies that the following types of data must be stored in Vietnam: (a) personal information data of service users in Vietnam; (b) data generated by service users in Vietnam, such as account names, service use time, credit card information, email addresses, log-in and log-out IP addresses, and registered telephone numbers associated with the relevant accounts or data; and (c) data on relations among service users in Vietnam, such as linked or interactive friends and groups. However, relevant stakeholders shall be entitled to determine the form of such data storage, and the Ministry of Public Security (*MPS*) may request evidence of such data storage in writing on a case-by-case basis.

### 2.2 Local presence requirements

The Law on Cybersecurity generally requires that foreign service providers must establish branches or representative offices in Vietnam. However, Decree 53 limits and clarifies the local presence requirement, providing that a foreign entity will only be required to store regulated data and establish a branch or representative office in Vietnam if it: (i) operates in one of 10 (ten) regulated businesses listed in Decree 53, including e-commerce, social networks, online payment, online video

games, and storing and sharing data on cyberspace; and (ii) has been warned by the MPS that its provided services have been used to commit a breach of cybersecurity regulations, but it has not taken any remedial measures to avoid, deal with, combat, or prevent such breaches, or it has resisted, obstructed, or ignored requests from the relevant authorities.

### *2.3 Cybersecurity audit of information systems*

The specialised cybersecurity taskforce of the MPS may carry out an audit of information systems that are not on the “List of Information Systems Critical to National Security” in the following circumstances: (i) there is an act violating the laws on cybersecurity that prejudices national security, or causes serious harm to social order and safety; or (ii) there is a request from the information system owners. Cybersecurity audits may involve review of: (a) hardware and software systems and digital devices used in the information system; (b) information stored, processed, and transmitted on the information system; (c) measures for protecting state secrets, and for preventing and combating revelation and loss of state secrets via technical channels. At least 12 (twelve) hours prior to the audit, the MPS taskforce shall issue written notice to the information system owner. Within 30 (thirty) days after the audit, the taskforce will notify the subject of the audit result and issue requests to the information system owner upon detection of any security vulnerability or flaw. In practice, these cybersecurity audits are rather uncommon with limited publicly available information on their implementation.

### *2.4 Handling illegal content in cyberspace*

Domestic and foreign CSPs are required to: (i) prevent sharing and ensure deletion







of information containing any illegal content on the services or information systems directly managed by the CSPs within 24 hours upon request from the competent authorities under the MPS and/or the Ministry of Information and Communications (MIC); (ii) record system logs to assist government investigations and handling of violations of laws on cybersecurity in a timely manner as required by the government; (iii) refrain from providing, or cease providing services to organisations or individuals that upload cyberspace information containing any illegal content following a request from the competent authorities under the MPS and/or the MIC. In practice, enforcement tends to occur on an ad hoc basis.

Please note that effective from March 1, 2025, the Ministry of Information and Communications has been merged into the Ministry of Science and Technology. Following this merger, the consolidated authority will operate under the name the Ministry of Science and Technology (MST).

## 2.5 Child protection

The Law on Cybersecurity was the first law in Vietnam to mandate protection of children against online content that can cause harm to or mistreatment of children or infringe on children's rights (*Child-Inappropriate Content*). Information system owners and CPSs are required to: (i) monitor Child-Inappropriate Content on their information systems or services; (ii) block the sharing of and delete Child-Inappropriate Content; and (iii) notify and cooperate in a timely manner with the cybersecurity force under the MPS for further handling.

## 2.6 Data retention period and compliance timing

Relevant stakeholders shall retain mandated data under Decree 53 (as noted

above) from their receipt of a data storage request until the end of such request. The data retention period is a minimum of 24 (twenty four) months. Within 12 (twelve) months after the written request of the MPS, relevant stakeholders must fulfil the requirements on storing data and establishing a local presence in Vietnam. System logs for investigation and handling of cybersecurity violations must be stored for at least 12 (twelve) months.

## 2.7 Sanctions to be determined

Currently, the Government has not issued further legal instruments detailing administrative penalties for non-compliance with Decree 53. In order to facilitate the enforcement of Decree 53 and Decree 13, the Government is expected to issue a decree on administrative penalties in the cybersecurity sector, this first draft of which was published in November 2021 and the most recently published draft of which was issued in June 2023.

## 3. Decree 13 on Personal Data Protection

Decree 13 is the first consolidated and targeted regulation of Vietnam focused on personal data protection requirements, and entered into effect on July 1, 2023.

### 3.1 Extra-territorial effect

Although Decree 13 is ambiguous on its scope of application, on its face it applies to both domestic entities and foreign entities that directly process or are involved in processing personal data in Vietnam. In an official workshop on Decree 13 in June 2023, the MPS indicated that Decree 13 would apply regardless of the data processing location or whether an entity has a local presence in Vietnam. However, in practice extraterritorial enforcement may be unlikely.



### 3.2 Processing requirements

Under Decree 13, obtaining the consent of the data subject is a strict legal requirement for the collection, processing, storage, and transfer of personal data. The key requirements of consent under Decree 13 are as follows:

- a) The consent of a data subject shall only be valid if the data subject voluntarily consents to and acknowledges: (1) the category of personal data to be processed; (2) the purpose of the personal data processing; (3) the organisation or individual who processes the personal data; and (4) the rights and obligations of the data subject.
- b) The consent of a data subject must be clearly and specifically stated in writing, by voice, by ticking a consent box, in the syntax of consent via text message, by selecting technical settings manifesting consent, or through another action that demonstrates consent.
- c) The consent of a data subject shall be expressed in a format that can be printed or reproduced in writing, including in electronic or verifiable formats; and the silence or non-response of a data subject is not considered as consent.
- d) In case of processing “sensitive personal data”, the data subject must be informed that the data to be processed is sensitive personal data.
- e) If there are multiple purposes of data processing, all such purposes must be listed for the data subject to consent to one or multiple purposes.
- f) A data subject is entitled to revoke its consent, unless otherwise provided by law. Such revocation must be made in a format that can be printed or reproduced

in writing, including in electronic or verifiable format.

### 3.3 Consent exemptions

Although Decree 13 allows personal data to be processed without prior consent in five circumstances, Decree 13 does not share the same “legitimate interests” exception recognised under the GDPR as providing a basis for data processing without consent where obtaining consent is not practical. Accordingly, the practical use of these permissible exemptions for the private sector is rather limited and difficult. Private entities may only be able to apply the following exemptions during the normal course of business:

- a) Performing contractual obligations of the data subjects to relevant entities.
- b) Processing personal data obtained from audio and video recording activities in public places to protect lawful rights and interests of an organisation or individual. However, private entities must notify the data subjects that they are being recorded or videotaped, unless otherwise provided by laws. Although regulators have not yet provided any examples, processing personal data for security purposes such as monitoring devices or CCTV cameras likely would be permissible.
- c) Processing relevant personal data to protect the life and health of the data subject or other people in an emergency situation, in which the personal data controller, personal data processor, personal data controller and processor, and third-parties would bear the burden of proof.

### 3.4 Advance processing notice

Before personal data is processed, a data subjects must be notified by the personal

data processor. This notification must be made once before the processing occurs and include the following details: (1) purposes of data processing; (2) category of personal data used and its relation to the processing purposes; (3) method of data processing; (4) information about other organisations and individuals related to the processing purposes; (5) unexpected consequences and damage that are likely to occur upon processing; and (6) start time and end time of data processing. Such prior notice shall be given in a format that is available for printing or reproducible in writing, including in electronic form or verifiable format.

### *3.5 Rights of the data subject*

Under Decree 13, data subjects are entitled to: (1) know about, consent to or revoke their consent to the processing of their personal data, (2) access their collected personal data to review and revise or request the revision of their personal data, (3) delete or request the deletion of their collected personal data, (4) restrict the processing of their personal data, (5) request the provision of their personal data, (6) object to the processing of their personal data, and (7) initiate complaints, denunciations, lawsuits, and compensation claims.

### *3.6 Mandatory impact assessment dossiers to be filed with the MPS*

Decree 13 provides for two types of impact assessment filings: Processing Impact Assessments (*PIAs*) and Offshore Transfer Impact Assessments (*OTIAs*). A PIA applies to data processing activities while an OTIA applies to the offshore transfer of Vietnamese citizens' personal data.

- a) At the June 2023 MPS workshop it was expressed that: (1) the MPS shall conduct







post-examination rather than pre-examination; (2) the PIAs and OTIAs are separate administrative procedures and cannot be combined; (3) the application filing for relevant data protection procedures must be made in Vietnamese; and (4) as Decree 13 does not specify the means of offshore data transfer, any offshore data transfer would be subject to the impact assessment requirement, including automatic transfers of personal data, such as internal group transfers of employee data.

- b) The MPS may demand that a party stop offshore data transfers in any of the following cases: (1) the transferred data is used in activities violating the interests and national security of Vietnam, (2) the relevant applicant does not comply with the MPS's request of revising, updating, supplementing the TIA, or (3) there is a leakage or loss of Vietnamese citizens' personal data.
- c) Submitting a PIA and/or OTIA to the MPS is a time-consuming and complex process due to the extensive documentary requirements, involving notarisation, legalisation, and certified translation of certain materials. Currently, the Government has not yet issued any administrative penalties for non-compliance with Decree 13, and to date there have not been any publicly available instances of MPS imposing strict deadlines or enforcing compliance for submission of these dossiers.
- d) It is often most efficient for businesses to submit physical copies of the relevant filings directly at the premises of the Department of Cybersecurity and Prevention of Hi-tech Crimes under the MPS.

### *3.7 National portal on personal data protection*

Under Decree 13, the MPS is the principal agency overseeing personal data protection using the national portal on personal data protection, through which the reports, dossiers and information prescribed under Decree 13 can be submitted, processed, and published. This portal is available at <https://baovedlcn.gov.vn>, but applicants often encounter operational issues to access the portal and submit filings.

### *3.8 Data protection department or officer*

While Decree 13 requires the designation or disclosure of contact details for the data protection department or data protection officer in certain instances (e.g., processing sensitive personal data, ensuring personal data protection activities or completing a PIA or OTIA), there is currently no specific qualification for this department or position. Decree 13 provides for a two-year grace period following establishment in which micro-enterprises, SMEs and innovative start-ups are exempted from the obligation to designate both a department and personnel in charge of personal data protection. The Law on Support for SMEs provides that micro-enterprises and SMEs generally should have on average no more than 200 employees participating in a compulsory insurance regime, and have either total equity not exceeding VND100 billion (approx. USD4.26 million) or total revenues in the preceding year not exceeding VND300 billion (approx. USD12.78 million). The definition of innovative start-ups varies depending on industry sector.

### *3.9 Mandatory 72-hour response time*

Decree 13 sets out a challenging 72-hour response deadline in various circumstances, such as once the data



subject has made a request regarding the restriction of, objection to, edit of or deletion of their personal data or the processing, or provision of such data. The MPS has confirmed that the 72-hour deadline is calculated from the moment of receiving the relevant request, and shall not be understood as only counting regular business hours.

### *3.10 Other management requirements*

Decree 13 requires relevant stakeholders to: (1) implement appropriate organisational and technical measures and safety and security measures to demonstrate that data processing activities have been carried out in accordance with the law on personal data protection, and to review and update these measures when necessary; (2) record and store system logs of personal data processing; and (3) give notice of violations of personal data protection regulations as prescribed under Decree 13.

### *3.11 Prohibition on the sale and purchase of personal data*

Although there is a level of ambiguity in Decree 13 as to whether the sale and purchase of personal data is permitted, the MPS has clarified that the sale and purchase of personal data would not be fully prohibited if the law expressly provides for permissible cases of selling and purchasing personal data, but mere consent of the data subject is not a basis to justify whether the sale and purchase is permissible. Currently, there are no regulations expressly allowing purchase and sale of personal data, but the Law on Data expressly recognises property rights in personal data, creating a legal framework for such transactions.

### *3.12 Sanctions*

It remains unclear when the government will approve and promulgate a decree detailing the administrative penalties for failure to comply with Decree 13. As noted above, the draft decree has been in the works since 2021, with the latest public update in June 2023.

## *4. Law on Data*

The Law on Data will come into effect on July 1, 2025 and will govern digital data and digital data-related activities.

### *4.1 Scope of application*

The Law on Data governs digital data-related activities with the focus on: (i) digital data management; (ii) construction, management and operation of the National Data Centre and the National General Database; (iii) digital data products and services; and (iv) the rights, obligations and responsibilities of relevant agencies, organisations and individuals regarding digital data. The Law on Data applies to: (a) Vietnamese agencies, organisations, and individuals; (b) foreign agencies, organisations, and individuals in Vietnam; and (c) foreign agencies, organisations, and individuals directly participating or otherwise involved in digital data activities in Vietnam.

### *4.2 Broad definition of “digital data”*

“Digital data” is defined under the new Law as “data about objects, phenomena, or events, comprising one or a combination of audio, visual, numerical, written, or symbolic forms expressed in digital format”. This broad definition covers any information recorded or represented in digital format, including personal and non-personal data, such business data.

#### 4.3 Recognition of “property rights” of data owners

- a) The Law on Data establishes for the first time, an express “property right” of data owners over their data, with broad consequences resulting from generally applicable provisions of the Civil Code which apply to property rights.
- b) Articles 105 and 115 of the Civil Code provide that property rights are a type of asset having monetary value. Article 450 of the Civil Code allows for the purchase, sale, and transfer of ownership of property rights. Accordingly, data owners will have the right to sell, transfer, or otherwise commercially use their data and take anti-infringement measures to legally protect their data.
- c) Pending further guidance on the Law on Data to be provided in an implementation decree, a draft of which was made publicly available on January 16, 2025, there is still significant ambiguity regarding the precise scope and limitations of the property rights of data owners. For example, it is unclear how the Law on Data will apply to emerging AI technologies which use and incorporate data without permission from data owners.

#### 4.4 Cross-border transfer and processing of “important data” and “core data”

- a) The Law on Data introduces two new legal concepts for classifying data:
  - (i) “Important data” is defined as data that can potentially impact national defense, security, foreign affairs, macroeconomics, social stability, and health and public safety pursuant to lists to be promulgated by the Prime Minister; and









- (ii) “Core data” is defined as important data that directly impacts national defense, security, foreign affairs, macroeconomics, social stability, health, and community safety pursuant to lists to be promulgated by the Prime Minister.

b) The Law on Data regulates cross-border transfer and processing of important and core data in the following circumstances:

- (i) Transfer of such data stored in Vietnam to storage systems outside Vietnamese territory;
- (ii) Transfer of such data from Vietnamese agencies, organisations and individuals to foreign individuals and entities; and

- (iii) Use of overseas platforms by Vietnamese agencies, organisations and individuals for processing such data.

c) In principle, cross-border data transfers and any processing of data from Vietnam must not affect the country’s national defense, security, national interests, public interests, or the legitimate rights of data subjects and owners. Further details and guidance on these requirements have yet to be determined by the Government.

#### 4.5 Mandatory risk assessments

Data administrators of important data and core data must periodically conduct risk assessments of their data processing activities, and notify specialised task units on cybersecurity and information security of the MPS, the Ministry of National Defense, and other relevant authorities for coordinated implementation of data safety and security protection. Further details and guidance on these requirements have yet to be determined by the Government.

#### 4.6 Data-related products and services

The Law on Data does not provide any specific definition of “data-related products and services”, but recognises the following as data-related products and services within its ambit: (i) data intermediary products and services; (ii) data analysis and synthetic products and services; and (iii) data platforms provided by eligible public units or state enterprises. Depending on the specific nature of the products or services in question, they may be subject to registration or licensing requirements as stipulated under the Law on Data and its forthcoming guiding decree.

#### 4.7 Establishment of the National General Database and the National Data Centre

The Law on Data provides the legal basis for the establishment of a National General Database under the management of the National Data Centre in Vietnam. The National Data Centre is scheduled to be launched by the end of 2025, with the mission of managing data integration for the National General Database, ensuring data quality and protection, and facilitating international cooperation, with implementation details to be specified by the Government. Data derived from administrative procedures, public services, and other public databases will be collected, updated, and integrated into the National General Database. Access to the National General Database is granted to government entities for their official duties, to data subjects for access to their own personal data, and to others for open data or with consent from the National Data Centre for other data types.



## 5. Decree 147 on Internet Services and Cyberinformation

### 5.1 Management of cross-border information provision

Foreign entities providing cross-border information services into Vietnam are subject to Decree 147 if they: (a) lease space in Vietnamese data centres; or (b) receive 100,000 or more monthly visits from Vietnam for six consecutive months. Decree 147 outlines the following obligations imposed on such foreign entities:

- a) *Content Moderation:* Prompt removal of violating content (within 24 hours), immediate blocking of content threatening national security, and temporary or permanent suspension of repeatedly offending accounts.
- b) *User Verification:* Mandatory verification of user accounts using phone numbers or personal identification numbers before posting or sharing.
- c) *Data Provision:* Provision of information on violating users to regulatory authorities upon request.
- d) *Account Authentication:* Authentication of accounts of organisations, enterprises, and influencers in Vietnam.
- e) *Notification Requirement:* Foreign websites hosted in Vietnam or exceeding 100,000 monthly visits from Vietnam must notify the MST and comply with Decree 147.
- a) *Offshore providers:* Must adhere to the same obligations as cross-border information providers.”
- b) *Onshore providers:* “High-traffic” providers ( $\geq 10,000$  monthly visits or  $> 1,000$  regular users averaged over six consecutive months) must obtain a license to operate. “Low-traffic” providers need only a notification confirmation from the authorities. Only licensed providers can offer live-streaming or monetise their services.
- c) *User verification and reporting:* By March 25, 2025, all licensed onshore and offshore providers must verify user identities. Licensed onshore providers must also report monthly visit statistics and the number of regular users in Vietnam.
- d) *Content removal:* Onshore and offshore service providers must suspend the accounts posting content that violate the law at least five times in 30 (thirty) days or ten times in 90 (ninety) days within 24 (twenty four) hours of a request from a competent authority, such as the MPS and the MST. These accounts must be permanently shut down after three suspensions. Non-compliance with suspension and permanent shutdown requests may result in service suspension or license revocation of the provider.

### 5.3 Online Games

- a) *Cross-Border Provision:* Decree 147 provides that offshore entities providing online gaming services to users in Vietnam must establish an enterprise in compliance with the decree and with regulations on foreign investment to provide such services. As a result, the cross-border provision of online games remains prohibited.

### 5.2 Management of social networks

Decree 147 introduces a regulatory framework for the management of social networks.

- b) *Game Categorization:* Games are categorised (G1-G4) based on the way players interact with game servers and with other players: G1 games allow interaction among multiple players via game servers; G2 games only allow interaction between players and game servers; G3 games have interactions among multiple players without interaction between players and game servers; and G4 games are downloaded from the internet without interaction among players or between players and game servers.
- c) *Prohibited Games:* Games resembling casino games or using card imagery are prohibited.
- d) *Provider Responsibilities:* These include maintaining a server in Vietnam, operating an informative website, implementing measures to reduce negative impacts of games, enforcing technical measures to manage interactions, obtaining advertising approvals, submitting regular reports, and complying with regulatory inspections. Providers must also store user data for six months beyond service termination and provide access to the national population database upon request.

#### 5.4 App Stores

- a) *Cross-Border Regulation:* Offshore app stores meeting the visit thresholds described in section 6.1 are considered cross-border services.
- b) *Additional Obligations:* Offshore app stores must:
  - (i) Remove illegal applications upon request of the authorities;
  - (ii) Comply with Vietnam's payment regulations; and









- (iii) Require game publishers to provide relevant licenses before making gaming apps available on the app store.

## 6. Decree 24 on New

### *Administrative Sanctions*

The recently issued Decree 24 amending Decree No. 98/2020/ND-CP significantly increased the severity of administrative fines for violations related to consumer information protection. Previously, fines for consumer information protection violations did not exceed VND20 million (approximately US\$790). Below are the main new sanctions:

#### *a) Sanctions applicable to individuals*

- (i) Administrative fines from VND20 million to VND30 million (approximately US\$790 - US\$1,180) apply to various violations, including:
  - a) Collection and use of consumer information without consent; and
  - b) Inappropriate use of consumer information and not in accordance with the announced purposes and scope.
- (ii) Fines are increased to VND30 million to VND40 million (approximately US\$1,180 - US\$1,600) for:
  - a) Failure to implement safety measures for consumer information when collecting, storing, or using it, or lacking preventive measures against violations regarding the safety and security of consumer information; and
  - b) Transferring consumer information to third-parties without consent.

#### *b) Sanctions applicable to organizations*

Organisations committing the same violations as described in paragraph (a) will be subject to fines of twice the amount applied to individuals.

If the object of breaches are “sensitive personal data”, the amount of fines will be doubled for individuals and quadrupled for organisations operating large digital platforms.

## 7. Future trends

The Government is in the process of developing a Draft Law on Personal Data Protection, which aims to further regulate the processing of personal data in specific contexts, such as marketing, big data processing, artificial intelligence, cloud computing, recruitment and employment monitoring, banking and finance, as well as social networks, and media services. This Draft Law on Personal Data Protection is scheduled to be enacted in 2025, with implementation to commence in January 2026. In parallel, a Draft Decree to guide the implementation of the Law on Personal Data Protection is also being drafted: after enactment, these are expected to further regulate data protection and management in Vietnam.



# 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 have become reliant on mobile and cloud-based operating platforms and so expect to be in a position to transfer data across borders on a routine basis.

An effective data protection and cybersecurity compliance programme 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, 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, and new operating models?
- What data protection and cybersecurity regulatory regimes apply to the organisation's personal data holdings, bearing in mind both the location in or from which the data was collected, and the location or locations where it is being processed?
- Are the business's existing policies and procedures compliant? Where are the gaps

and what are the practical options for achieving compliance?

Each of these steps is explored in more detail below.

## A personal data audit

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

### *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 organisation's customer data holdings is that databases are not always clearly marked out as such, particularly now in the era of cloud computing and widespread use of mobile devices.

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

Data that has been anonymised or aggregated for profiling or analytics purposes, may not, strictly speaking, be "personal data", but this data should nevertheless be included as part of the audit. Data protection laws generally look at data from an entity-wide or group-wide perspective, meaning that de-personalised datasets that can be linked to identities will not avoid compliance requirements.

With the proliferation of social media and online public data sources, the risk of "re-identifying" individuals from anonymised or aggregated datasets has never been higher. Assessing data protection compliance will involve assessing the procedures for creating and maintaining the de-personalisation of these datasets.

### *Employee data*

As APAC region businesses grow in scale and geographical 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 organisations will also hold personal data about individuals who are not their direct customers, such as shareholders, directors, and company officers of corporate customers and suppliers, as well as family members and other individuals who are connected to customers or employees. In the context of social media and cloud services businesses, there are often holdings of user contacts or "refer a friend" data that has not been directly obtained from









the business's customers. This personal data will nevertheless be subject to regulation.

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

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

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

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

### **Mapping data transfers**

A related task in the fact gathering process is to understand where personal data is being transferred to from its points of collection, both in terms of transfers to entities within the wider business group and transfers to unrelated third-parties. The geographical transit of personal data will also be important given the proliferation of data export controls across the APAC region and the introduction of localisation 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 cease processing 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 erase personal data once the purposes for having it have been fulfilled.

## An eye to the future

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

## Assessing regulatory requirements

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

### *1. Leveraging what's already there*

The regulatory analysis will not necessarily be a matter of re-inventing the wheel, in particular for EU-based multinationals who have invested years of effort in constructing policies and procedures that meet European standards. European standards often (but do not always) meet or exceed national requirements across many jurisdictions in the APAC region, and so it can be efficient to leverage global or regional policies from elsewhere in the organisation if they are transportable having regard to the nature of the business and the data processing taking place. As the APAC region's data protection and cybersecurity regimes proliferate and develop, however, there are more and more local distinctions that will need to be 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 organisations have completed a "global upgrade" of their data protection compliance programmes. However, simply rolling out an EU-based compliance programme in the APAC region will likely represent "over compliance" in a number of areas and under-compliance in others. Our recommended approach is to carefully distinguish where the GDPR applies (and

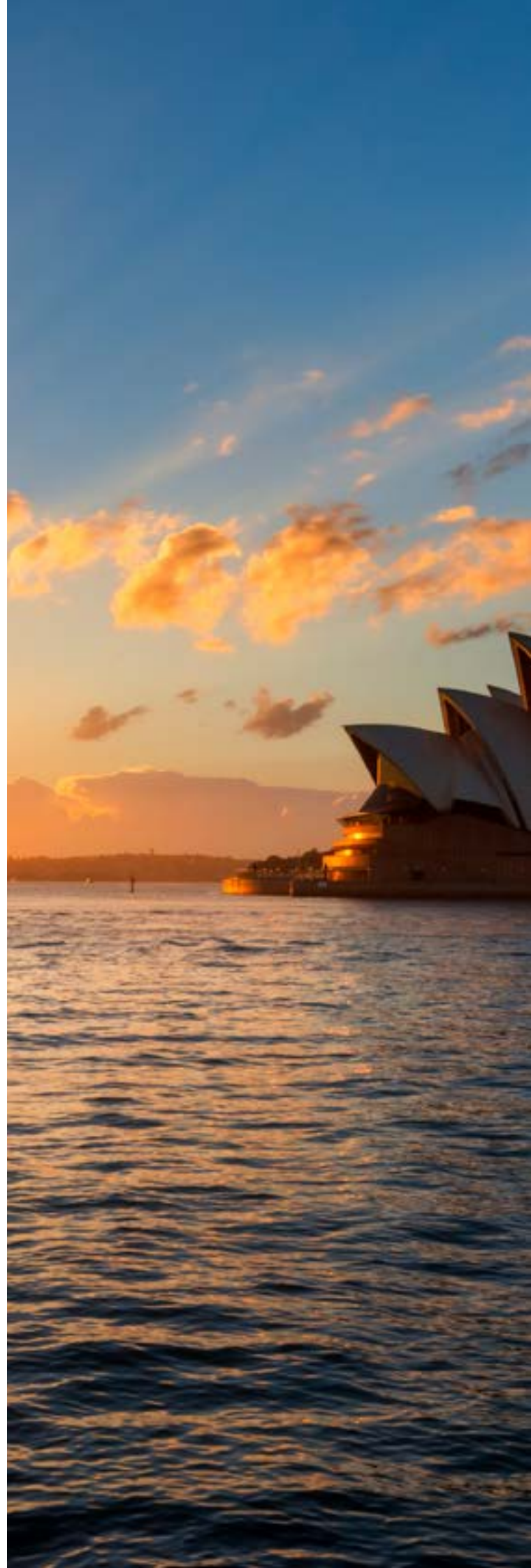
where it does not) and craft an efficient compliance solution that involves consistency of approach with EU standards, where appropriate, but fixes a general “APAC standard” that applies with limited exceptions across the region.

“Levelling up” to the “APAC standard” in jurisdictions without data protection laws often make good business sense, given the obvious trend towards comprehensive regulation across the region. 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 Vietnam’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. Vietnam's Decree 13 on Personal Data Protection is forcing the same considerations there.

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. Organisations 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 organisations 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 websites and apps, employment terms and conditions, and other interfaces with data subjects.
- *Data processing policies and procedures* for internal stakeholders to understand and administer, including policies and procedures dealing with:
  - Data collection and capture, including policies concerning the use of appropriate

PICS and the mechanics of collecting consents, and the usage of third-party data sources;

- Direct marketing, including alignment of PICS with direct marketing activities, implementation of “opt in”/“opt out” mechanisms, prior consultation with applicable “Do Not Call” registries and compliance with direct marketing formalities, such as consumer response channels and any required “ADV” indicators;
- Human resources management, including policies dealing with job applicant data, retention of and access to employee files, notification and consent to data privacy policies, employee monitoring, management of sensitive employee data, and the use of external vendors for functions such as payroll and counselling;
- Data analytics, including policies specifying the types of profiling data that may be used, anonymisation/aggregation principles and policies around “enhancing” datasets through the use of publicly available data or third-party datasets;
- Data commercialisation, which looks more broadly for the potential use of the organisation's data to collaborate with other businesses in marketing initiatives and consumer profiling;
- Security, including technical standards applicable to various types of internal and external data processing, data access and permissioning, the use of encryption technologies and policies around the use of data in cloud services and other technologies;
- Business continuity and disaster recovery, including data back-up procedures, the use of redundant storage and contingency planning;
- Data subject access, including procedures for assessing and verifying requests,



considering the legal implications of requests and managing costs of responding to requests;

- Complaints handling, including complaints from customers, employees, and other affected individuals;
- Data quality management, including procedures for updating and correcting databases and determining if data is to be erased;
- Data processing and outsourcing, including vendor due diligence policies and standard contract clauses and templates for onshore and offshore processing, 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 programmes to identify and review cyber threats across the organisation, allocation of responsibilities for escalation of and response to incidents;
- Data breach management, including policies for escalating, containing and remediating data breaches and evaluating the need for regulatory or data subject notifications, as well as procedures for assessing any need for change to policies and procedures following the occurrence of a breach; and
- Privacy impact assessment, which includes a general framework for the organisation to assess privacy impacts due to proposals for organisational, technological, or policy change.

## **Management oversight and review**

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

Regulators in the region are becoming increasingly conscious of the degree to which data protection and 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 organisation will be necessary in order to lend context and emphasise the importance of compliance to the business. The policies will need to be seen to have been acted upon in order to be evidence of due compliance, and so enforcement procedures will be critical. Policy breaches will need to be examined after the fact with a view to understanding whether or not any organisational change is needed in response.

In order to be effective, an 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.









# Hogan Lovells' Asia-Pacific Data, Privacy and Cybersecurity Practice

## *Realising 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 data protection, privacy, 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' Data, Privacy and Cybersecurity team is uniquely placed to help clients realise 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 organisations.
- A one-stop shop for all of your data privacy needs around the globe.

## *An international perspective*

At Hogan Lovell's we bring an international perspective to advising clients on APAC data, privacy and cybersecurity laws, and the ongoing development of policy across the region.

Our on-the-ground team has experience advising on European data privacy laws and works closely with our European and wider global colleagues to 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 local experts are rooted in the domestic law and language, and are sensitive to the important emerging market nuances.

## *Integrated support*

Our integrated team of data protection and cybersecurity practitioners benefits heavily from a wider team of market-leading lawyers who are at the forefront of policy developments in Europe and the Americas, 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, privacy and cybersecurity team is also closely integrated with other relevant specialists, in particular, lawyers engaged in commercial arrangements concerning data commercialisation and processing and employment law specialists. Our seamlessness on this front means that we bring a very practical, solutions-based approach to counselling that is well informed by market practice.

### *Key points*

Our advice covers all aspects of data, privacy and cybersecurity compliance, including:

- Conducting data, privacy 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; and
- Defending companies against enforcement actions.

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

### *Our focus and experience*

The Hogan Lovells Data, 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 policymakers 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.

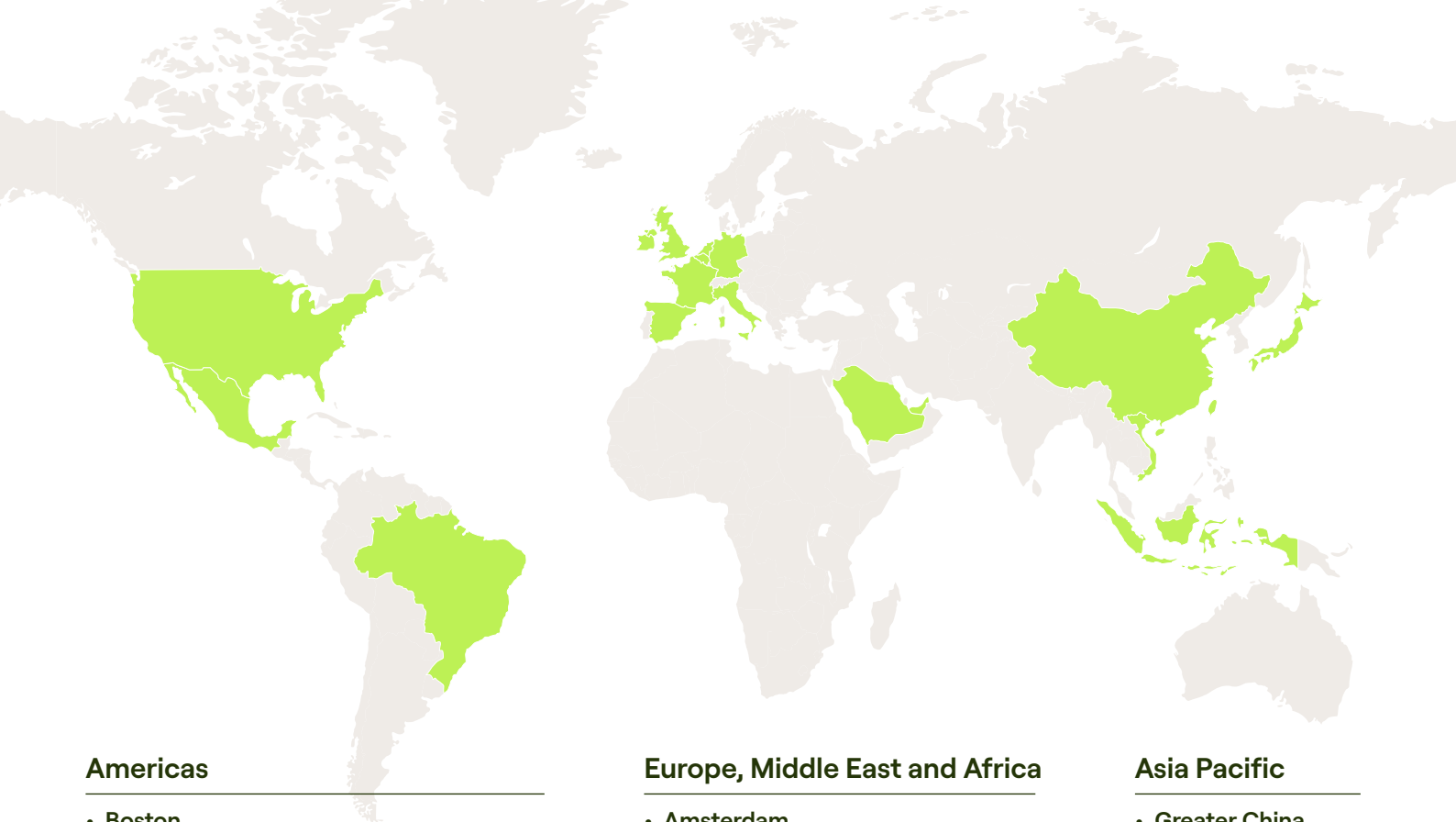
- We have surveyed in detail the laws and regulations impacting employee monitoring practices in over 60 countries, including important markets in Europe, the Americas, Asia, the Middle East, and Africa.
- We advised a number of global companies on data privacy questions arising from their migration of HR and customer data of their European subsidiaries to cloud service providers.
- We have advised many multinationals on localising website privacy policies.
- We have assisted leading global companies to adopt and implement a Pan-European strategy in respect of the EU cookie consent requirements for their website and mobile application offerings.
- We provided strategic advice to a number of clients on data breach notification requirements throughout the world.
- We have advised on complex matters ranging from the use of biometrics to the collection of mobile device data, including making submissions to multiple data protection authorities to facilitate the deployment of new data-driven technologies.

future regulation of privacy. Additionally, we provide the latest privacy and data protection legal developments and trends to our clients via our blog, Chronicle of Data Protection.

### *How we can help?*

We have a team specialising in Data, 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 Americas, 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





## Americas

---

- **Boston**
- **Denver**
- **Greater Washington, D.C.**
  - Baltimore
  - Washington, D.C. and Northern Virginia
- **Houston**
- **Los Angeles**
- **Miami**
- **Minneapolis**
- **New York**
- **Philadelphia**
- **Northern California**
  - San Francisco
  - Silicon Valley
- **Latin America**
  - Brazil
  - Mexico

## Europe, Middle East and Africa

---

- **Amsterdam**
- **Brussels**
- **Dublin**
- **Germany**
  - Berlin
  - Düsseldorf
  - Frankfurt
  - Hamburg
  - Munich
- **London**
- **Luxembourg**
- **Madrid**
- **Milan**
- **Rome**
- **Paris**
- **Middle East**
  - Dubai
  - Riyadh

## Asia Pacific

---

- **Greater China**
  - Beijing
  - Hong Kong
  - Shanghai
- **South East Asia**
  - Ho Chi Minh City
  - Jakarta
  - Singapore
- **Tokyo**

# www.hoganlovells.com

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

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

For more information about Hogan Lovells, the partners and their qualifications, see [www.hoganlovells.com](http://www.hoganlovells.com).

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

© Hogan Lovells 2025. All rights reserved. BD-REQ-195