



The Guide to Cyber and Data Privacy Investigations - Fourth Edition

**Unlocking Asia's data protection
landscape: essential insights on
breach notifications and cybersecurity
obligations**

The Guide to Cyber and Data Privacy Investigations - Fourth Edition

Data breaches and similar incidents pose a unique challenge to organisations – those targeted must both respond and investigate in a tightly regulated, timely manner or face significant penalties. Written by leading contributors with broad experience of handling serious data incidents, the *Guide to Cyber and Data Privacy Investigations* is an invaluable resource for businesses around the globe. It identifies the most urgent issues to consider when creating and implementing a response template, and provides both legal and practical advice.

This edition of the Guide also features a new Spotlight section, which takes a deep dive into the cyber and data protection regimes of key jurisdictions around the world.

Generated: October 31, 2025

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2025 Law Business Research

Unlocking Asia's data protection landscape: essential insights on breach notifications and cybersecurity obligations

Lim Chong Kin, David N Alfred and Anastasia Su-Anne Chen

Drew & Napier LLC

Summary

INTRODUCTION

BRUNEI DARUSSALAM

CAMBODIA

CHINA

HONG KONG

INDIA

INDONESIA

JAPAN

KOREA

MALAYSIA


MYANMAR

PHILIPPINES

SINGAPORE

TAIWAN

Unlocking Asia's data protection landscape: essential insights on breach notifications and cybersecurity obligations

Explore on **GIR** 

[THAILAND](#)

[VIETNAM](#)

[CONCLUSION](#)

INTRODUCTION&NBSP;

Cyberthreats are rising sharply across Asia, exposing businesses to data breaches with serious regulatory, financial and reputational consequences. As attacks grow more frequent and complex, it is critical for organisations to secure personal data and be prepared to respond.

While the region is broadly moving toward stronger data protection and cybersecurity standards, jurisdictions differ significantly in approach and maturity. Some jurisdictions in Southeast Asia remain in the early stages of developing their data protection laws. For example, Brunei has only recently enacted its Personal Data Protection Order, while Cambodia's draft law remains pending with no clear implementation timeline. Others, like Thailand, are slowly maturing and progressing towards more robust enforcement. Even jurisdictions with longstanding data protection laws continue to evolve. Malaysia, for instance, has recently introduced data breach notification rules to strengthen accountability. Beyond Southeast Asia, other key Asian markets such as China, India and South Korea have only enacted comprehensive data protection laws since 2020.

Businesses operating or planning to expand in the region must stay informed as data breaches cross international borders and regulatory expectations continue to rise across Asia. The varying approaches and stages of maturity in data protection laws highlight the need to understand these differences to manage legal risk and respond effectively to incidents. This chapter seeks to provide an overview of the key obligations across 15 jurisdictions in Asia, with a focus on security requirements, cybersecurity incident response and data breach notification rules.

BRUNEI DARUSSALAM

The general data protection law in Brunei is the Personal Data Protection Order (BN PDPO), which was enacted in January 2025 and will be administered by the Authority for Info-communications Technology Industry (AITI) of Brunei. The BN PDPO governs the collection, use and disclosure of personal data by the private sector. The AITI has confirmed in the Consultation Paper and Response that it will release advisory guidelines to support the interpretation, application and administration of the BN PDPO. However, these advisory guidelines have yet to be released.

Cybersecurity in Brunei is generally regulated under the Cybersecurity Act (Chapter 272) (the Cybersecurity Act) and various criminal activities are prohibited under the Computer Misuse Act (Chapter 194).

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Under Section 22 of the BN PDPO, an organisation is required to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, modification, disposal or similar risks, and the loss of any storage medium or device on which personal data is stored. In the Consultation Paper, the AITI stated that it intends to provide more detailed guidance on the types of security measures, which will include administrative/organisational, physical and technical security measures, in due course.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

Under the Cybersecurity Act, owners of critical information infrastructure (CII) are required to put in place systems and procedures to detect cybersecurity threats and incidents, in accordance with any relevant codes of practice. Specifically, the Cybersecurity Code of Practice for CII obliges these owners to apply baseline security configurations to all operating systems, applications, network devices and other CII-related assets. These configurations must reflect the CII's level of cybersecurity risk and must, at a minimum, cover essential security measures. These include:

- removal of inactive or unused accounts;
- password management (default passwords must be changed, and passwords shall be stored in their hash forms);
- removal of unnecessary services and applications;
- closure of unused or unnecessary network ports and services;
- enabling only external physical connections necessary for the operation of the CII;
- protection against malware; and
- timely update of software and security patches.

DATA BREACH NOTIFICATION REQUIREMENTS

In brief, the BN PDPO defines a data breach as unauthorised access, use or disclosure of personal data, or the loss of a device containing such data where unauthorised access, use, etc. is likely. The BN PDPO states that organisations will be required to notify the AITI as soon as is practicable, but in any case, no later than three calendar days after making the assessment that a data breach: (1) will result, or is likely to result, in significant harm to the affected individuals; or (2) is, or is likely to be, of significant scale.

While the terms 'significant harm' and 'significant scale' are not defined in the BN PDPO, the AITI intends to take into account international norms and issue guidelines and regulations on the interpretation of these terms.

Organisations must also notify the affected individuals on or after notifying the AITI if the data breach will result, or is likely to result, in significant harm to the affected individuals. This obligation is subject to waiver and exceptions (which are not stated in the Consultation Paper).

Section 16 of the Cybersecurity Act requires owners of CII to notify the Commissioner of Cybersecurity of the occurrence of any of the following:

- prescribed cybersecurity incident in respect of the CII;
- prescribed cybersecurity incident in respect of any computer or computer system under the control of the owner that is interconnected with or that communicates with the CII;
- any other type of cybersecurity incident in respect of the CII that the Commissioner of Cybersecurity has specified by written direction to the owner.

At the time of writing, the specific incident types and reporting timelines have not yet been defined.

CAMBODIA

Cambodia does not currently have comprehensive cybersecurity and data protection legislation, although the Ministry of Post and Telecommunication (MPTC) announced in 2021 that it would be drafting the Personal Data Protection Law after finalising the draft Cybersecurity Law.

Currently, matters relating to data protection and privacy largely fall under the right to privacy under Cambodia's constitution and certain provisions under the Civil Code, the Penal Code, and other specific laws, such as the Law on Electronic Commerce (the E-commerce Law) and the Law on Banking and Financial Institutions. While these laws generally protect the right to privacy, they potentially also regulate personal data.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Article 32 of the E-Commerce Law requires any person who stores electronic data to establish measures to ensure that the data is reasonably protected from loss, unauthorised access, use, alteration, leaks or disclosure (to or by a third party), unless authorised by the data subject or permitted by law.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

The cybersecurity law in Cambodia has not been enacted and no existing regulations address security obligations in the context of cybersecurity.

DATA BREACH NOTIFICATION REQUIREMENTS

There are currently no laws or regulations that address cybersecurity incident or data breach notification or procedures.

CHINA

China has three main laws on data protection and cybersecurity: the Cybersecurity Law (CSL), the Data Security Law (DSL) and the Personal Information Protection Law (PIPL).

Cybersecurity is governed by the CSL and focuses on network infrastructure security within China. The DSL covers all data-handling activities, all types of data and generally applies to data-handling activities within China. The DSL will also apply when data-handling activities outside China may potentially harm China's national security. The PIPL applies to the processing of personal information of natural persons by both the public and private sector within China and extra-territorially where it concerns Chinese individuals or if provided by other laws and administrative regulations.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Under Article 27 of the DSL, data handling activities must comply with laws and administrative regulations, establish a data security management system covering the entire workflow, conduct data security education and training and adopt technical and other necessary measures to ensure data security. Where data handling uses the internet or other information networks, obligations shall be fulfilled based on the cybersecurity Multi-Level Protection System. Important data handlers must designate responsible persons and management bodies for data security.

Under Article 73 of the PIPL, 'personal information processor' refers to any organisation or individual that independently determines the purpose and method of personal information processing (i.e., a data controller). Under Articles 9 and 51 of the PIPL, personal information

processors are responsible for their processing and must take necessary measures to ensure security of the personal data they process. These include formulating internal management systems and procedures, implementing classified management, adopting technical measures such as encryption and de-identification, determining operational authority, conducting regular safety training, formulating contingency plans and other measures required by law. Where a data processor is engaged, Article 59 requires that they take measures to ensure adequate security of the personal data they process.

Article 42 of the CSL further provides that network operators shall adopt technical measures and other necessary measures to ensure the security of personal information they gather and to prevent personal information from leaking, being destroyed or lost.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

Under Article 40 of the CSL, network operators must maintain the confidentiality of user information they collect and establish systems to protect personal data. Apart from this, Article 42 of the CSL requires the adoption of measures to ensure the security of personal information as mentioned above.

DATA BREACH NOTIFICATION REQUIREMENTS

Pursuant to Article 57 of the PIPL, where personal information has been or may be leaked, falsified or lost, the data controller shall immediately take remedial measures and inform the 'personal information protection departments', which are yet to be established, and the individuals concerned. The notice shall include the types and causes of personal information leakage, falsification and loss that has occurred or may occur, the possible harm caused, remedial measures to mitigate harm and the processor's contact details. Data controllers may choose not to notify individuals if harm by the data breach has been effectively avoided.

The Cybersecurity Incident Reporting Management Measures (Draft for Comments) (CIRMM) provides guidance on reporting cybersecurity incidents and specifies the related procedure and requirements. Depending on the category of an incident, the reporting obligation shall be performed within one hour or 24 hours if the earlier is not possible. A subsequent report must be submitted within five working days. Reports should cover matters such as incident details, impact, measures taken, analysis of causes and further action plans. The full list of reportable matters may be found in Article 5 and Annex 2 of the CIRMM.

Separately, under Article 42 of the CSL, network operators are required to take immediate remedial measures and promptly inform users and authorities where personal information has leaked, been destroyed or lost.

Article 29 of the DSL also requires the reporting of data security incidents to users and relevant authorities.

HONG KONG

The Personal Data (Privacy) Ordinance (HK PDPO) governs the usage and processing of personal data in Hong Kong. The Office of the Privacy Commissioner for Personal Data (PCPD) has also issued the Guidance Note on Data Security Measures for Information and Communications Technology (the Advisory Guidelines) as an advisory guide to the HK PDPO. In terms of cybersecurity, Hong Kong has just passed the Protection of Critical Infrastructure

(Computer System) Ordinance (the PCICS Ordinance), which is set to come into effect on 1 January 2026.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Principle 4(1) of the First Schedule to the HK PDPO provides that all practicable steps shall be taken to ensure that any personal data held by a data user (i.e., data controller) is protected against unauthorised or accidental access, processing, erasure, loss or use. The data user must have regard to:

- the kind of data and the harm that could result if any of those things should occur;
- the physical location where the data is stored;
- any security measures incorporated into any equipment where the data is stored;
- any measures taken to ensure the integrity, prudence and competence of persons having access to the data; and
- any measure taken for ensuring the secure transmission of the data.

The Advisory Guidelines state that it is incumbent upon a data user to show that all reasonably practicable steps have been taken to safeguard the security of personal data. In assessing whether 'all practicable steps' have been taken by a data user to safeguard the security of personal data in its possession or control, the PCPD will adopt a totality approach, taking into account the following factors (which are non-exhaustive, and the weight of each factor varies between cases):

- volume, kind and sensitivity of the personal data involved, and the harm that could result in the event of a data security incident;
- physical location where the data is stored;
- nature and complexity of the ICT used;
- whether security measures are sufficiently robust in relation to the resourcefulness of the data user concerned;
- familiarity of the data security issues in question among the ICT community and the relevant industry, and the availability of solutions; and
- state of development of ICT and data security.

Principle 4(2) of the First Schedule to the HK PDPO provides that if a data user engages a data processor to process data on the data user's behalf, the data user must adopt contractual (or other relevant means) to prevent unauthorised or accidental access, processing, erasure, loss or use.

In the Advisory Guidelines, the PCPD recommends that a data user should establish clear internal policy and procedures on data governance and data security, covering the following areas:

- respective roles and responsibilities of staff in maintaining the information and communications systems and safeguarding data security;
- data security risk assessments;
- accessing data in and exporting data from the information and communications systems;

- outsourcing of data processing and data security work;
- handling data security incidents including an incident response plan and reporting mechanism; and
- destruction of data that is no longer necessary for the original purposes of collection or related purpose.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

The Protection of Critical Infrastructures Computer Systems (PCICS) Ordinance sets out a framework of obligations for Critical Infrastructure (CI) operators to safeguard the cybersecurity of their critical computer systems. Generally, CI operators are required to establish a dedicated unit responsible for managing the cybersecurity of their systems and ensuring compliance with the PCICS Ordinance. This unit must be supervised by a qualified employee, and the appointment must be formally notified.

Operators must prepare and submit several key documents to their relevant regulatory authorities:

- Security management plan – a detailed plan for protecting the cybersecurity of critical systems, to be submitted within three months of being designated as a CI operator (or within an extended period if granted). This plan must cover all areas listed in Schedule 3.
- Risk assessment – an initial assessment of cybersecurity risks must be conducted within 12 months of designation, followed by annual assessments. Reports of these assessments must be submitted within three months of completion (or within an extended period), addressing all items in Schedule 4.
- Security audit – an audit must be carried out within 24 months of designation and then biennially. The corresponding audit report must also be submitted within three months of the audit period's end (or within an extended time frame), covering all areas in Schedule 5.
- Incident response plan – a protocol for responding to cybersecurity incidents must be prepared and submitted within three months of designation (or extended deadline). It must include all matters specified in Part 2 of Schedule 3.

Together, these provisions aim to ensure that CI operators proactively manage, assess, audit and respond to cybersecurity threats in a structured and regulated manner.

DATA BREACH NOTIFICATION REQUIREMENTS

A data breach is generally regarded as a suspected or actual breach of the security of personal data held by a data user, which exposes the personal data of data subjects to the risk of unauthorised or accidental access, processing, erasure, loss or use.

While it is not a statutory requirement for data users to inform the PCPD about a data breach incident concerning the personal data held by them, data users are nevertheless advised to do so as a recommended practice for proper handling of such incident. The PCPD also provides an e-Data Breach Notification Form on its website to facilitate and encourage data breach reporting.

When deciding whether to report a breach to the affected data subjects, the PCPD and other law enforcement agencies, the data user should take into account the potential consequences of a breach for the affected individuals, how serious or substantial these are and how likely they are to happen. The consequences of failing to give notification should also be duly considered.

In general, the data user should notify the PCPD and the affected data subjects as soon as practicable after becoming aware of the data breach, particularly if the data breach is likely to result in a real risk of harm to those affected data subjects.

Under the PCICS Ordinance, if a CI operator becomes aware that a computer-system security incident has occurred in respect of a critical computer system of a CI, the operator must notify the Commissioner of Critical Infrastructure (Computer-system Security) of the incident as soon as practicable and in any event, within 12 hours if the incident disrupts or is likely to disrupt the core function of the CI, and otherwise, within 48 hours. The notification must be made in the form specified under Section 10 of the PCICS Ordinance. After this initial notification, the CI operator must submit a further written report of the incident in the specified form 14 days after the date on which the CI operator became aware of the incident.

INDIA

The Digital Personal Data Protection Act (DPDPA) forms the personal data protection and regulatory regime in India. The Draft Digital Personal Data Protection Rules 2025 (the DDPDP Rules) provide further guidelines on the DPDPA.

The cybersecurity law in the jurisdiction is the Information Technology Act 2000 (the IT Act). However, the upcoming Digital India Act is expected to supersede the IT Act. The IT Act creates obligations for government agencies in respect of critical information infrastructure.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Section 8(4) of the DPDPA provides that a data fiduciary (i.e., data controller) shall implement appropriate technical and organisational measures to comply with the DPDPA and the rules made thereunder. Section 8(5) of the DPDPA further provides that a data fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a data processor, by taking reasonable security safeguards to prevent personal data breach.

Rule 6 of the DDPDP Rules provides guidance on these safeguards, requiring a data fiduciary to adopt adequate security measures to protect personal data and prevent breaches during any processing, including that by a data processor. Such safeguards shall include, at a minimum, the following:

- adequate data security measures, including securing such personal data through techniques like encryption, anonymisation, masking;
- access controls to computer resources used by the data fiduciary or the data processor;
- verification of access to the personal data through appropriate logging, monitoring and review to detect, investigate and prevent unauthorised access;
- backup and recovery measures to maintain data availability and integrity during incidents;

- retention of such logs and personal data for a period of one year for detection, investigation and prevention of unauthorised access, unless longer retention is otherwise required under applicable law;
- adequate provisions in agreements between the data fiduciary and the data processor to implement appropriate security safeguards; and
- adequate technical and organisational measures to ensure the effective implementation of security safeguards.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

Section 70 of the IT Act provides that the appropriate government may, by notification in the Official Gazette, declare any computer resource that directly or indirectly affects the facility of CII, to be a protected system. Information security practices and procedures for such protected system are outlined in the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018.

Under Rule 3, organisations managing a ‘protected system’ must establish strong cybersecurity governance led by top leadership through a dedicated committee. They must appoint a chief information security officer (CISO) and implement a formal, well-documented security management system aligned with national or approved standards.

Key responsibilities include approving major security decisions, regularly reviewing risks, maintaining detailed records and conducting periodic audits. Advanced infrastructure like security and network operation centres must be in place to monitor threats, manage incidents and ensure system stability. All activities must be continuously reviewed and improved to protect against evolving cyber threats.

DATA BREACH NOTIFICATION REQUIREMENTS

Article 8(6) of the DPDPA provides that, in the event of a data breach, the data fiduciary shall give the Data Protection Board of India (DPBI) and affected data subjects intimation of the breach in such form and manner as may be prescribed.

The DDPDP Rules provide the manner in which the notification is required to be made. Under Rule 7(1), upon becoming aware of a personal data breach, the data fiduciary must promptly inform each affected data subject through their user account or any registered mode of communication. The notification must be concise, clear, plain and must include:

- a description of the breach, including its nature, extent and the timing and location of its occurrence;
- the consequences relevant to the data subject, that are likely to arise from the breach;
- the measures implemented and being implemented by the data fiduciary, if any, to mitigate risk;
- the safety measures that the data subject may take to protect their interests; and
- business contact information of a person who can respond on behalf of the data fiduciary, to queries, if any, of the data subject.

Under Rule 7(2), on becoming aware of any personal data breach, the data fiduciary shall intimate to the DPBI: (1) without delay, a description of the breach, including its nature, extent, timing and location of occurrence and the likely impact; and (2) within 72 hours of becoming

aware of the same, or within such longer period as the DPBI may allow on a request made in writing in this behalf:

- updated and detailed information in respect of such description;
- the broad facts related to the events, circumstances and reasons leading to the breach;
- measures implemented or proposed, if any, to mitigate risk;
- any findings regarding the person who caused the breach;
- remedial measures taken to prevent recurrence of such breach; and
- a report regarding the intimations given to affected data subjects.

INDONESIA

Indonesia's main personal data protection law is Law No. 27 of 2022 on Protection of Personal Data (the PDP Law), effective from 17 October 2022, with implementing regulations still pending.

Additionally, sector-specific data protection provisions also apply. For example, banks must protect customer data under banking laws, and financial institutions must comply with privacy rules under Regulation 22/POJK.04/2023 on Consumer Protection in Financial Services. In healthcare, Law No. 17 of 2023 on Health mandates confidentiality of patient data and records.

Although no specific cybersecurity law exists, general cybersecurity provisions are included in Law No. 11 of 2008 on Electronic Information and Transactions (the EITLaw), which governs electronic transactions, systems and networks. Additionally, the Badan Siber dan Sandi Negara (BSSN), the lead government agency for cybersecurity efforts, plays a key role in cybersecurity regulation.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Under the PDP Law, personal data controllers are required to protect and ensure the security of the personal data they process, by implementing the following measures:

- developing and implementing operational technical measures to protect personal data from interference with personal data processing that is contrary to the laws and regulations; and
- determining the level of security for personal data by considering the nature and risks associated with the personal data.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

Under the EIT Law, electronic system providers must generally ensure service security and inform users of their security measures. BSSN Regulation No. 8 of 2020 expands on this by requiring providers to conduct and submit to BSSN a self-assessment to classify their electronic systems as:

- strategic: high public or national impact; must implement SNI ISO/IEC 27001 and other cybersecurity standards from BSSN and relevant ministries;
-

high risk: sector or regional impact; must implement ISO/IEC 27001 and other applicable standards; or

- low risk: electronic systems that are not categorised as strategic or high risk; must implement ISO/IEC 27001 or cybersecurity standards by BSSN.

DATA BREACH NOTIFICATION REQUIREMENTS

Under the PDP Law, in the event of a failure to protect personal data, the data controller must provide written notification within 72 hours to both the affected data subject and the Ministry of Communications and Digital Affairs (MOCDA), pending the establishment of the Personal Data Protection Agency. A failure to protect data refers to breaches of confidentiality, integrity or availability, including both intentional and unintentional incidents that lead to the destruction, loss, alteration, disclosure or unauthorised access to data that is sent, stored or processed.

The notification must include at minimum: (1) details of the data breach; (2) when and how it occurred; and (3) the impact of the breach and measures taken to address or recover from it.

Following the notification, MOCDA may request further information or clarification as needed. It may also require the data controller to publicly disclose the breach if: (1) it disrupts public services; and/or (2) it seriously affects public interests.

The EIT Law does not mandate reporting of cybersecurity events. However, BSSN Regulation No. 1 of 2024 requires electronic system organisers to establish a cybersecurity response team and register it with the National Cybersecurity Response Team. While no general reporting timeline is provided, incidents in strategic sectors must be reported within 24 hours. If personal data is involved, separate data breach notification rules under the PDP Law apply.

JAPAN

The principal data protection legislation is the Act on the Protection of Personal Information (APPI), which applies to both the public and the private sectors.

The Personal Information Protection Committee (PPC) is the main agency that enforces the APPI and issues general guidelines on the implementation of the APPI. Guidelines that apply specifically to certain industries (e.g., financial, healthcare and telecommunication sectors) are jointly issued by the PPC and the government body that supervises the relevant industry.

The cybersecurity law in Japan is the Basic Act on Cybersecurity (BAC) which, among other things, stipulates the obligation of CII operators, cyberspace-related business providers and research institutions to exert efforts to maintain cybersecurity. Sector-specific regulators for sectors such as healthcare and finance may also impose additional security obligations.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Article 23 of the APPI provides that data controllers must take the necessary and appropriate measures for managing the security of personal data, including preventing the leaking, loss or damage of the personal data they handle. Further, data controllers are required to exercise necessary and adequate supervision over their employees and service providers to ensure the secure management of the personal data.

The PPC guidelines further illustrates that data controllers should establish basic policies for handling of personal data, establish internal rules regarding handling of personal data, organisational security control measures, human security control measures and technological security control measures considering the risks arising from the personal data.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

While the BAC does not mandate detailed technical standards or specify minimum security requirements for CII operators, they are expected to adhere to sector-specific guidelines and best practices set out by the relevant authorities.

DATA BREACH NOTIFICATION REQUIREMENTS

Data controllers are required to report material data breaches involving personal data to the PPC.

Article 26(1) of the APPI provides that, businesses handling personal information must report leaks, loss or damage and other situations concerning the security of the personal data they handle to the PPC. However, this obligation does not apply to data processors where they have notified the data controller of the breach.

Article 26(2) of the APPI further requires that, in the cases mentioned above, the business must notify the affected individuals, as prescribed by the PPC. This notification may be waived if it is difficult to do so and alternative measures are implemented to safeguard the individual's rights and interests.

Article 7 of the Enforcement Regulations of the APPI provides that reportable incidents include:

- actual or suspected leakage of, loss of or damage to personal data including sensitive personal data;
- actual or suspected leakage of, loss of or damage to personal data that can be abused for economic gains;
- actual or suspected leakage of, loss of or damage to personal data caused by a malicious act; and
- actual or suspected leakage of, loss of or damage to personal data where more than 1,000 principals are affected.

There is no general regulation imposing a mandatory reporting obligation for a cybersecurity incident that does not involve a personal data breach.

KOREA

The Personal Information Protection Act (PIPA) forms the personal data protection and regulatory regime in Korea. The PIPA applies to 'personal information controllers' (i.e., data controllers), which includes public institutions, legal persons, organisations, individuals, etc. that process personal information directly or indirectly to operate the personal information files (i.e., personal information arranged or organised in a systematic manner for the personal information to be readily retrievable) as part of its activities. The Enforcement Decree of the Personal Information Protection Act (the Enforcement Decree of PIPA) is the subsidiary legislation to the PIPA.

Cybersecurity law in Korea is governed by a patchwork of laws and their respective enforcement decrees. They are as follows:

- the Act on the Promotion of Information and Communications Network Utilisation and Information Protection (the Network Act) and the Enforcement Decree of the Act on Promotion of Information and Communications Network Utilisation and Information Protection (the Enforcement Decree of the Network Act);
- the Act on Protection of Information and Communications Infrastructure (APICI) and the Enforcement Decree of the Act on the Protection of Information and Communications Infrastructure (the Enforcement Decree of APICI); and
- the Electronic Financial Transactions Act (ETA) and the Enforcement Decree of the Electronic Financial Transactions Act (the Enforcement Decree of ETA).

Other sector-specific legislations are also applicable in relation to data protection and cybersecurity, for example, in the financial services and healthcare sectors. This chapter will only focus on the Network Act and the APICI.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Article 29 of the PIPA requires data controllers to take such technical, managerial (e.g., establishing an internal management plan) and physical measures that are necessary to ensure safety as prescribed by Presidential Decree to prevent the loss, theft, disclosure, forgery, alteration or damage of personal information.

As prescribed under Article 30 of the Enforcement Decree of PIPA, data controllers shall take measures to ensure safety of personal information including but not limited to:

- formulating and implementing an internal management plan to safely process personal information;
- restricting and controlling access to personal information; and
- implementing security measures such as encryption for storage.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

Under Chapter VI of the Network Act, specifically Article 45, providers of information and communications services and manufacturers/importers of connected devices are required to implement protective measures for network security and stability. These entities are also required to comply with any guidelines on protective measures as issued by the Minister of Science and ICT.

These guidelines would include:

- technical and physical protective measures, including installation and operation of an information security system, to prevent or counteract unauthorised access to the network;
- technical protective measures for preventing unlawful leakage, forgery, alteration or deletion of information;
- technical and physical protective measures for ensuring the continuous use of information and communications networks; and
-

administrative protective measures for stabilisation of information and communications networks and protection of information, including securing human resources, organisation and expenses and establishing related plans.

Under Article 9(1), the APICI requires regular vulnerability analysis and evaluation. Based on these evaluations, the management organisation must formulate and implement physical and technological measures to protect critical infrastructure per Article 5 of the APICI. These measures must be submitted to the relevant central administrative agency, which may order or recommend additional protection measures based on the submissions.

DATA BREACH NOTIFICATION REQUIREMENTS

Article 34 of the PIPA requires a personal information controller to notify data subjects when the personal information controller becomes aware of loss, theft or divulgence of personal information. The notice to data subjects must include details of the data breach, guidance for data subjects to mitigate harm, remedial measures taken by the data controller and contact information for assistance (Article 34(1)).

Notification must be made within 72 hours unless impracticable due to unavoidable causes (e.g., natural disaster) and where harm to data subjects is substantially mitigated (Article 39(1) of the Enforcement Decree of PIPA). If all information required under Article 34(1) of the PIPA is not yet known, the controller must provide initial notice with confirmed details and update the rest of the details upon confirmation (Article 39(2) of the Enforcement Decree of PIPA). If affected data subjects are uncontactable, the controller must post the required notice on its website for at least 30 days (Article 39(3) of the Enforcement Decree of PIPA).

Separately, under Article 34(3) of the PIPA, the personal information controller must promptly report the above listed information to the Personal Information Protection Commission or a designated institution, as prescribed by Presidential Decree, considering the type, process, and scale of the breach. Under Article 40 of the Enforcement Decree of PIPA, reporting is mandatory if:

- personal information of 1,000 data subjects is affected;
- sensitive or personally identifiable information is affected; and
- divulgence occurs due to illegal external access to personal information processing systems or information technology equipment used by personal information handlers (i.e., persons who manage personal information) for processing personal information.

Reporting to the Protection Commission must be done within 72 hours unless it is impracticable to file a report within 72 hours due to a natural disaster or other unavoidable causes and where the possibility of infringing on the rights and interests of data subjects is substantially reduced through measures taken.

Article 48-3 of the Network Act stipulates that if a computer security incident occurs, a provider of information and communications services shall immediately report it to the Minister of Science and ICT or the Korea Internet and Security Agency.

MALAYSIA

Malaysia's data protection framework is primarily governed by the Personal Data Protection Act 2010 (MY PDPA), which applies to the processing of personal data in commercial transactions. The PDPA establishes a set of core data protection principles and is supported

by subsidiary legislation that clarifies compliance obligations and standards. Recognising the unique ways in which different industries handle personal data, the MY PDPA allows for the development of sector-specific codes of practice, overseen by the Personal Data Protection Commissioner (the Commissioner).

In addition to the MY PDPA, sectoral laws, such as those governing financial services and healthcare, impose data protection requirements tailored to the sensitivity of information in those fields. Data controllers are also classified by industry, with certain sectors subject to registration requirements.

Cybersecurity in Malaysia is governed by the Cyber Security Act 2024 (CSA). The CSA introduces mandatory risk assessments, incident reporting, licensing requirements for service providers and enforcement mechanisms. Sectoral regulators such as Bank Negara Malaysia also impose cybersecurity obligations within their regulated industries.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

The MY PDPA imposes an obligation on the data controller and data processor to take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction when processing personal data. The data controller/processor shall protect the personal data by having regard to:

- the nature of the data and potential harm from its misuse, loss, etc.;
- where the data is stored;
- security features of the equipment in which the data is stored;
- the measures taken for ensuring the reliability, integrity and competence of personnel with access to the data; and
- the measures taken to ensure security of data transfers.

Data controllers are also required to develop and implement a security policy that complies with the security standards as set out in the Personal Data Protection Standard 2015.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

Under Section 21 of the CSA, entities managing National Critical Information Infrastructure (NCII) must implement cybersecurity measures, standards and processes as set out in the code of practice. The NCII may also adopt other alternatives, provided they offer equal or greater protection to the NCII.

Compliance is also recognised if these entities follow cybersecurity requirements under internationally recognised frameworks, as long as they do not conflict with the code of practice. At the time of writing, the proposed code of practice has not been introduced.

DATA BREACH NOTIFICATION REQUIREMENTS

The MY PDPA defines 'personal data breach' as any breach, loss, misuse or unauthorised access of personal data. Where data controllers have reason to believe a breach has occurred, they are required to notify the Commissioner as soon as practicable (and no later than 72 hours, following the relevant guidelines and circulars). Hence, under the law, all data breaches are notifiable to the Commissioner.

Notwithstanding the above, the Personal Data Protection Guidelines on Data Breach Notification published by the Commissioner in February 2025 (the DBN Guidelines) provide that not all data breaches are notifiable to the Commissioner. Instead, a data controller is only required to notify the Commissioner if the personal data breach causes or is likely to cause 'significant harm'.

The DBN Guidelines provide that a personal data breach is considered to cause, or is likely to cause, significant harm if there is a risk that the compromised personal data:

- may result in physical harm, financial loss, a negative effect on credit records or damage or loss of property;
- may be misused for illegal purposes;
- consists of sensitive personal data;
- consists of personal data and other personal information that, when combined, could potentially enable identity fraud; or
- is of significant scale (i.e., the data breach affects more than 1,000 individuals).

If the breach causes or is likely to cause significant harm to the data subjects, data controllers must also notify the affected data subjects within seven days of informing the Commissioner. Given the guidance by the Commissioner, even data breaches of significant scale must be notified to the affected individuals.

Under the CSA, a 'cybersecurity incident' refers to any unauthorised act involving a computer or system that compromises its security. Section 23 imposes a duty on NCII entities to report such incidents. Notification must be made immediately upon discovery to the Chief Executive of the National Cyber Security Agency and the relevant sector lead. Further timelines for reporting updates are as follows.

- Within six hours, submit key incident details (type, severity, time of the incident occurrence, etc.).
- Within 14 days, provide fuller information (affected systems, threat actors, impact, response, etc.).

MYANMAR

Myanmar's legal framework addressing cybersecurity and data protection comprises several key laws. The Telecommunications Law (2013) primarily governs the telecommunications sector, with limited provisions related to cybersecurity. It aims to prevent cybercrimes involving telecommunication services and restricts the unauthorised disclosure of information stored in secure or encrypted systems.

The Electronic Transactions Law facilitates the use of electronic transactions and includes data protection and cybersecurity provisions. It imposes penalties for offences such as hacking and unauthorised access to data.

The Law for Protection of Personal Privacy and Personal Security of Citizens is designed to safeguard individual privacy and personal security. It provides rights against unauthorised surveillance and requires consent for the collection and processing of personal data. However, these protections have been suspended since 2021, limiting their current enforceability.

On 1 January 2025, Cybersecurity Law No. 1/2025 was enacted by Myanmar's State Administration Council. Though not yet in force, it is intended to regulate digital security and online activities, particularly focusing on digital platform service providers, cybersecurity service providers and VPN providers.

Additionally, the Financial Institutions Law mandates strict confidentiality for banks regarding user information, including account details, records and transactions, thereby reinforcing data protection within the financial sector.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Although the Electronic Transactions Law does not directly mandate security measures for personal data processing, it outlines clear responsibilities for the personal data management officer (PDMO). Under Section 27-A, the PDMO must securely store, protect and process personal data based on its type and sensitivity, in line with legal requirements. The PDMO is prohibited from accessing, sharing or altering personal data without the individual's consent or legal permission, and must avoid processing data in ways that conflict with the law's purpose. Additionally, personal data must be destroyed once it exceeds the retention period, forming a framework for secure data handling.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

The Electronic Transactions Law sets security standards for electronic transactions, including the recognition of electronic records, protection of personal data and regulation of electronic signatures and certification authorities. Under Section 40, individuals and entities can choose the type and level of security needed and implement suitable methods to meet those requirements.

DATA BREACH NOTIFICATION REQUIREMENTS

There are no explicit requirements for notifying regulatory authorities or affected data subjects in the event of a data breach in Myanmar. There are also no notification requirements for cybersecurity incidents.

PHILIPPINES

In the Philippines, data protection is governed by the Data Privacy Act of 2012 (DPA). The DPA regulates the processing of personal data by both public and private sectors. It is administered by the National Privacy Commission (NPC), which also issues circulars and advisory guidelines to clarify compliance expectations.

Cybersecurity is addressed under the Cybercrime Prevention Act of 2012 (CPA), which defines a broad range of cyber offences, including unauthorised access, data and system interference, computer-related fraud and identity theft. The CPA also extends to traditional crimes under the Revised Penal Code and other special laws where these are committed using ICT. This includes statutes such as the Electronic Commerce Act 2000, Anti-Online Sexual Abuse or Exploitation of Children Act and the Subscriber Identity Module (SIM) Registration Act.

A proposed Critical Information Infrastructure Protection Act (CIIPA) is currently under legislative review. The bill seeks to enhance the resilience of vital sectors such as energy, water, finance and telecommunications by introducing minimum information security standards, mandating incident reporting, establishing a computer emergency response team and building national cybersecurity capabilities.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Pursuant to Section 20(a) of the DPA read with Section 14, personal information controllers (PICs) and personal information processors (PIPs) (i.e., data controllers and processors) are required to adopt reasonable and appropriate organisational, physical and technical safeguards to protect personal data. The adequacy of these measures is assessed based on factors such as the sensitivity of the data, the risks associated with processing, the size and complexity of the organisation, prevailing best practices in data privacy and the cost of implementing such safeguards.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

Under the upcoming CIIPA, all covered CII institutions would need to adopt the Philippine National Standard (PNS) on ISO/IEC 27001 Information Security Management System and PNS ISO 22301 security and resilience – business continuity management systems.

DATA BREACH NOTIFICATION REQUIREMENTS

Under NPC Circular No. 16-03, a personal data breach refers to a security incident resulting in the accidental or unlawful destruction, loss, alteration or unauthorised access to or disclosure of personal data. A broader security incident includes any event that affects or threatens data protection, even if it does not result in a breach due to existing safeguards. Notification of a personal data breach is required when:

- sensitive personal data or other high-risk information (e.g., financial data, login credentials, biometrics, ID documents) is involved;
- the data is reasonably believed to have been accessed by an unauthorised party; and
- there is a likely risk of serious harm to affected individuals.

The PIC must notify NPC and affected individuals within 72 hours of becoming aware of a notifiable breach. Notification may be delayed only to assess the breach, prevent further harm or restore system integrity. However, immediate notification is required if the breach affects at least 100 individuals or poses a serious risk due to the sensitivity of the data. A full report must be submitted within five days, unless an extension is granted by the NPC.

PICs and PIPs are also required to file annual security incident reports with the NPC documenting security incidents that did not meet the threshold for mandatory breach notification.

Under the upcoming CIIPA, all covered CII institutions will also be required to report all information security incidents affecting their institutions to the Philippine National Computer Emergency Response Team (NCERT) within 24 hours of detection of the security incident. If requested by the NCERT, the CII institution will also be required to submit an incident progress report and post-incident report.

SINGAPORE

Singapore's data protection regime is governed by the Personal Data Protection Act 2012 (SGPDPA). The SG PDPA governs the collection, use and disclosure of personal data in the private sector. The Public Sector (Governance) Act 2018 (PSGA) governs data protection and management in the public sector. Additional sectoral laws like the Banking Act 1970, Healthcare Services Act 2020 and codes issued under statutes such as the

Telecommunications Act 1999 and Monetary Authority of Singapore Act 1970 may prescribe additional data protection requirements.

Cybersecurity is regulated by the Cybersecurity Act 2018 (the Cybersecurity Act), alongside laws such as the Computer Misuse Act. Sector regulators like the Infocomm Media Development Authority and Monetary Authority of Singapore also issue cybersecurity codes and guidelines. Amendments to the Cybersecurity Act were passed in 2024 and are set to come into effect in the near future.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Under Section 24 of the SG PDPA, organisations (i.e., data controllers and processors) must implement reasonable security measures to protect personal data in their possession or control. These safeguards are aimed at preventing unauthorised access, collection, use, disclosure, copying, modification, disposal or loss of data (including loss of devices or storage media containing personal data). Organisations should implement reasonable security arrangements, taking into account the nature of personal data held by the organisation and the possible harm that might result from a security breach. These may include administrative measures (such as contractual confidentiality obligations, policies and procedures), physical measures and technical measures.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

The Cybersecurity Act imposes duties on owners of CII. They must establish systems and processes to detect threats and incidents in respect of CII as outlined in the applicable Cybersecurity Code of Practice. This includes implementing security baselines that reflect the risk profile of their systems, with measures like enforcing least access privilege, password complexity, removal of unused accounts and services, closing unused ports, malware protection and timely application of security patches. The amendments to the Cybersecurity Act will extend similar obligations to entities such as major foundational digital infrastructure service providers and owners of essential services or systems of temporary cybersecurity concern.

DATA BREACH NOTIFICATION REQUIREMENTS

A data breach under the SG PDPA includes unauthorised access, collection, use, disclosure or loss of personal data or loss of any storage medium containing personal data in circumstances where the foregoing is likely to occur. Organisations must promptly assess if a breach is notifiable, typically within 30 days.

Data controllers are required to notify the Personal Data Protection Commission (PDPC) within three days after determining a breach is notifiable, either because it causes or is likely to cause significant harm to individuals, or because it affects or is likely to affect 500 or more individuals. On or after notifying the PDPC, where significant harm is caused or likely to be caused by the data breach, individuals must generally also be notified of the breach.

If a data processor suspects a data breach involving personal data processed on behalf of a data controller has occurred, it must promptly notify the data controller, which must then assess whether the breach is notifiable.

Separately, under the Cybersecurity Act, CII owners must report specific cybersecurity incidents (e.g., any unauthorised hacking of a CII, malware installation, any man-in-the-middle attack, any denial-of-service attacks) to the Commissioner of

Cybersecurity. An initial report must be made within two hours of awareness, followed by detailed reporting within 14 days. The amendments to the Cybersecurity Act will broaden reporting obligations to additional categories of systems and providers, though the specific cybersecurity incidents, which are reportable for these new categories, have yet to be prescribed.

TAIWAN

The primary law governing data protection in Taiwan is the Personal Data Protection Act (TWPDPA). The Enforcement Rules of the Personal Data Protection Act (the Enforcement Rules of PDPA) provide further guidance on the TW PDPA.

In Taiwan, the Cyber Security Management Act (CMA) is the primary legislation governing cybersecurity in Taiwan. The Enforcement Rules of Cyber Security Management Act (the Enforcement Rules of CMA) provide further guidelines on the CMA.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

For government agencies that collect, use and process personal data, Article 18 of the TW PDPA states that they shall assign dedicated personnel to implement security and maintenance measures to prevent the personal data from being stolen, altered, damaged, destroyed or disclosed.

For non-government agencies that collect, use and process personal data, Article 27 of the TW PDPA states that they shall implement proper security measures to prevent the personal data from being stolen, altered, damaged, destroyed or disclosed. The central government authorities in charge of the industries concerned may designate and order certain non-government agencies to establish a security and maintenance plan for the protection of personal data files and rules on disposing personal data following a business termination.

Matters such as standards on setting forth the aforementioned plans and disposal regulations shall be expressly established by the central government authority in charge of the industry concerned. Thus far, industry specific guidelines have been promulgated for financial institutions, human resources recruitment business, hospitals, manufacturers and others.

Under Article 12 of the Enforcement Rules of PDPA, 'security and maintenance measures' refer to technical or organisational steps taken by public and private entities to prevent the theft, alteration, damage, destruction or disclosure of personal data. These measures must be proportionate to the purpose of data protection and may include:

- assigning management and resources;
- defining personal data scope;
- conducting risk assessments;
- establishing breach response mechanisms;
- implementing internal controls for data handling;
- securing data and managing personnel;
- providing training and awareness;
- securing facilities;

- auditing data security;
- keeping logs and evidence; and
- continuously improving security measures.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

In Taiwan, 'critical infrastructure' refers to physical or virtual assets, systems, or networks whose disruption or reduced performance could significantly impact national security, public interests, daily life or economic activity. Entities that operate or maintain such infrastructure, either in full or in part, may be designated as 'critical infrastructure providers' (CIPs) by the central authority responsible for the relevant industry, subject to ratification by the competent authority.

Under Article 16 of the CMA, CIPs must prepare, revise and implement a cybersecurity maintenance plan (CSMP), taking into account the nature and volume of information processed, as well as the scale and characteristics of their information and communication systems. CIPs must submit their CSMPs to the central industry authority, which is responsible for auditing their implementation.

Article 6 of the Enforcement Rules specifies the required content of a CSMP, which includes, for example, core functions, governance, risk assessments, incident response and continuous improvement mechanisms.

If an audit reveals shortcomings or areas for improvement, the CIP must submit an improvement report. This improvement report must identify the specific flaws, analyse their causes, outline corrective measures in terms of management, technology, personnel or resources, and provide an estimated timeline and method for tracking progress. CIPs must report on the implementation status and outcomes of each of these areas, demonstrating continuous adherence to and improvement of their cybersecurity measures.

DATA BREACH NOTIFICATION REQUIREMENTS

Currently, there is no requirement to notify regulatory authorities in the event of a data breach. However, upcoming amendments to the TW PDPA will introduce a new, general mandatory notification requirement. If a personal data incident falls within the 'specified notification scope' established by the Personal Data Protection Commission, notification must be made to the Personal Data Protection Commission. For non-government agencies, notification must also be made to the competent authority overseeing the relevant business sector.

At present, Article 12 of the TW PDPA states that if any personal data is stolen, disclosed, altered or otherwise infringed upon due to a violation of the PDPA by a government or non-government agency, the data subject must be notified via appropriate means after the relevant facts have been clarified.

Article 22 of the Enforcement Act defines 'appropriate means' for notification under Article 12 of the PDPA as prompt communication via various channels (e.g., verbal, written, digital). If costs are excessive, agencies may notify via public channels like the internet or media. The notification must detail the data breach and actions taken to respond to the breach.

Under the CMA, agencies must notify their supervisory authority or regulator when made aware of a cybersecurity incident, defined as an event where the state of a system, service or network is identified as having a potential violation of the cyber security policy or a failure of

protective measures, which affects the functionality of the information and communication system and constitutes a threat against the cyber security policy (Articles 14 and 18).

The Regulations on the Notification and Response of Cyber Security Incident expand on the CMA's reporting obligations. A 'specified non-government agency' must report an incident to the central regulator within one hour of discovery and must complete system recovery or damage control within 36 to 72 hours, depending on the nature of the incident. Reports must include the time of occurrence and discovery, a description of the incident, risk assessment, response measures taken, any external support received and other relevant details.

THAILAND

Thailand's primary data protection law is the Personal Data Protection Act BE 2562 (2019) (THPDPA). Sector-specific laws also apply, such as the National Health Act BE 2550 (2007) and Mental Health Act BE 2551 (2008) for health data and the Credit Information Business Act BE 2545 (2002) for financial data. In 2023, the Notification of the National Broadcasting and Telecommunications Commission Re: Measures to Protect Telecommunications Service Users' Rights Regarding Personal Data, Privacy Rights, and Freedom of Telecommunications issued a notification under the Telecommunications Business Act BE 2544 (2001) to strengthen protections for telecommunication users' personal data and privacy.

Cybersecurity is governed by the Cybersecurity Act BE 2562 (2019) (CA). It applies to CII organisations in sectors like national security, public services, finance, IT, transport, energy and healthcare. Not all entities in these sectors automatically qualify; eligibility is jointly assessed by the organisation, National Cyber Security Committee (NCSC) and relevant regulators based on potential national-level impacts of cyber threats.

CII organisations must follow NCSC guidelines, manage cyber risks, apply appropriate security measures and report incidents in accordance with the CA.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

Under the TH PDPA, data controllers must implement appropriate security measures that meet at least the minimum standards set by the Personal Data Protection Committee (the Committee) under the Notification re: 2022 the requirement of security measures for Data Controllers BE 2565 (2022) (the Notification on Security Measures). They must also ensure that their data processors do the same. These measures must be reviewed periodically or when technology changes to maintain effective protection.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

Under the CA, CII organisations must manage and reduce cyber risks by following NCSC guidelines and fulfil duties such as:

- implementing internal cybersecurity guidelines aligned with NCSC standards;
- notifying the NCSC of designated officers and relevant contact details; and
- conducting internal and external cyber risk assessments.

According to the Notification of the Cyber Security Supervisory Committee Re: Guidelines on Code of Practice and Standard Framework for Maintaining Cybersecurity for Government

Agencies and CII Organisations, CII organisations must maintain a code of practice that includes:

- a cybersecurity audit plan;
- risk assessments;
- an incident response plan;
- threat response measures; and
- resilience and recovery strategies.

In February 2025, the NCSC also released a draft Web Security Standard to enhance CII website protection. It sets minimum standards for governance, operations and web hosting provider selection. The draft is not yet in force and may still be amended before finalisation.

DATA BREACH NOTIFICATION REQUIREMENTS

The Notification of the PDPC Re: Rules and Procedures for the Data Breach Notification (the Data Breach Notification) defines 'data breach incident' as any breach of security that leads to loss, or unauthorised or unlawful access, use, change, alteration or disclosure of personal data, whether intentional, negligent or wilful.

When a data controller becomes aware of or is notified of a breach (or suspected breach), they must assess its reliability and risk. This will determine whether they must notify the Committee or the Committee and affected individuals. Factors include the type and severity of data, status of affected individuals (e.g., minors or vulnerable persons), business impact and existing security measures. They must notify the Committee without delay and, as far as feasible, within 72 hours, unless the breach poses no risk to individuals' rights and freedoms. Additional notification must be made without delay to data subjects if there is a high risk to individuals' rights and freedoms. This must include details of the breach and remedial actions. Data processors must inform the data controller without delay and, as far as feasible, within 72 hours of becoming aware of the breach.

If a cyber threat is expected to occur, a CII organisation must inspect its data and systems to assess the threat. If confirmed or likely, it must take preventive and risk mitigation measures as per its internal cybersecurity framework and promptly notify the NCSC and the relevant regulator. No specific guidance currently exists on the required content of such notifications.

VIETNAM

Vietnam's data protection landscape is primarily governed by Decree No. 13/2023/ND-CP on Personal Data Protection (PDPD). Before the PDPD, data privacy obligations were scattered across various laws. The Ministry of Public Security (MPS) has also issued a new Personal Data Protection Law (PDPL), which is set to take effect on 1 January 2026. The PDPL builds on the PDPD. The PDPL carries over principles from the PDPD, revises existing requirements and introduces new principles and requirements (e.g., data breach notification to individuals in certain cases). The PDPL also introduces enhanced penalties for illegal data trading, cross-border transfers and other violations.

Cybersecurity regulations in Vietnam are spread across various legal instruments. However, the primary legislation governing cybersecurity is Law on Cybersecurity No. 24/2018/QH14 (LOC). Additionally, the Law on Network Information Security (LNIS) also plays a significant

role, not only in personal data protection but also in regulating the security of information systems.

The MPS is also tentatively set to release the 2025 Cybersecurity Law. The Cybersecurity Law aims to consolidate the LNIS and the LOC into a unified legal framework aimed at strengthening national cybersecurity, combating cybercrime and addressing digital threats. Key changes include the removal of data localisation requirements for both domestic and foreign service providers, updated rules for systems deemed nationally important (with the Prime Minister responsible for updating the list), new obligations for cybercrime prevention and revised licensing requirements for cybersecurity products and services carried over from the LNIS.

SECURITY OBLIGATIONS – DATA PROTECTION LAWS

The PDPD sets out general security requirements for handling personal data. These include implementing suitable management and technical safeguards from the outset and throughout the data processing lifecycle, establishing internal rules for personal data protection and conducting cybersecurity assessments of systems and devices used in processing, both before use and before permanently deleting or discarding them.

Similarly, the LNIS mandates that organisations processing personal data implement appropriate safeguards and follow relevant technical standards to ensure network security. This includes creating plans to maintain data integrity, using secure storage solutions and maintaining backups on independent systems or media. If a network security incident occurs, organisations are required to respond promptly with corrective and containment measures.

SECURITY OBLIGATIONS – CYBERSECURITY LAW

Under the existing LOC, information system administrators must implement technical measures to prevent and respond to cyberattacks, cooperate with authorities in tracing attacks and provide relevant data and evidence. Online service providers must warn users of potential risks, offer guidance on minimising them and ensure secure data collection and protection against leaks or breaches. They are also required to develop incident response plans and address system vulnerabilities. The LOC has broad applicability and mandates ongoing system monitoring, regular security reviews and cooperation with cybersecurity authorities.

DATA BREACH NOTIFICATION REQUIREMENTS

Three main laws impose data breach notification obligations: the PDPD, the LNIS and the LOC, along with some sector-specific laws.

The PDPD requires data controllers to notify the MPS' Department of Cyber Security and HiTech Crime Prevention (A05)/MPS within 72 hours of any personal data protection violations and data breaches. The notification must follow a set format and include specific details such as the nature of the violation, contact information, potential consequences and remedial measures. Data processors only need to notify the data controller and the PDPD does not require notification to affected individuals.

The LNIS defines a network incident as any event compromising data confidentiality, integrity or availability. System administrators must report such incidents within five days to multiple authorities simultaneously. This includes the Vietnam Computer Emergency Response

Team, Vietnam Internet Network Information Centre, ISPs and other relevant state agencies and members of the concerned incident response network. The report must include system and incident details. Users must also report incidents to the service provider, though no specific timeline or format is mandated. Like the PDPD, LNIS does not require notifying affected individuals.

Under the LOC, cybersecurity incidents and cybersecurity emergencies must be immediately notified to A05/MPS. The LOC defines a cybersecurity incident as a 'an unexpected event in cyberspace (itself defined as a network of IT infrastructure that includes internet, communication systems and databases, among others) that threatens national security, public order or the lawful rights and interests of an organisation or individual'; and a cybersecurity emergency as an event in cyberspace that seriously violates national security, public order or the lawful rights sand interests of an organisation or individual. The LOC also mandates immediate notification to affected entities and individuals in cases of 'cybersecurity emergencies' that pose 'very serious damage' to the legitimate rights and interests of the affected individuals located in Vietnam or threatens human lives. Notification to the regulator in the case of incident, data breach or user data loss is also required under the LOC. However, LOC does not specify notification content or format to the A05.

CONCLUSION

Data protection and cybersecurity regulation across Asia is undergoing rapid and uneven development. While some jurisdictions are still in the process of defining their legal frameworks, others have moved into active enforcement, introducing increasingly detailed and prescriptive obligations for organisations. This disparity in legal maturity presents significant challenges for businesses operating across multiple jurisdictions, where a uniform compliance approach is rarely sufficient. Businesses will thus have to familiarise themselves with the requirements in jurisdictions relevant to them to comply with regulatory requirements and respond to data incidents effectively.



Lim Chong Kin
David N Alfred
Anastasia Su-Anne Chen

chongkin.lim@drewnapier.com
david.alfred@drewnapier.com
anastasia.chen@drewnapier.com

<https://www.drewnapier.com/>

[Read more from this firm on GIR](#)