Tilleke & Gibbins

Regional Guide to

CYBERSECURITY AND DATA PROTECTION

IN MAINLAND SOUTHEAST ASIA

CAMBODIA • INDONESIA • LAOS • MYANMAR • THAILAND • VIETNAM

CAMBODIA

Jay Cohen • Pichrotanak Bunthan

Cambodia has not yet enacted 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 finalizing the draft Cybersecurity Law. In November 2022, the MPTC announced that it had completed the first draft of the draft Personal Data Protection Law and planned to hold internal discussions. The MPTC's draft Cybersecurity Law is also still being discussed and refined.

Under current practices, matters pertaining to data protection and privacy fall broadly under the right to privacy as addressed in Cambodia's constitution and certain provisions under the Civil Code, the Penal Code, and other specific laws, such as the Law on Electronic Commerce (E-commerce Law) and the Law on Banking and Financial Institutions. These laws generally protect the right to privacy, which could cover personal data.

Constitution

Cambodia's constitution generally recognizes citizens' right to privacy in broad terms. It provides that all Cambodian citizens have the right to privacy of residence, and to the secrecy of correspondence by mail, telegram, fax, telex, and telephone. However, Cambodia does not yet have any specific laws elaborating on the meaning or scope of this provision or providing any implementing measures.

Civil Code

An individual's personal data may be protected under the Civil Code, dated December 3, 2007, as part of "personal rights," which include the right to privacy and other personal benefits and interests, as well as the rights to life, personal safety, health, freedom, identity, and dignity. This right to privacy may be interpreted as including the protection of individual personal data.

The Civil Code gives a person the right to an injunction where an infringement of that person's personal rights may occur (or continue). Assuming that personal data constitutes personal rights, an owner may seek a court order to stop any unlawful infringement of his or her personal data (e.g., data collection without consent).

Further, the Civil Code states that a rights owner may seek the elimination of effects stemming from an infringement. In the context of data privacy, this potentially means that a person can seek an order to remove, for example, storage of his or her personal data collected unlawfully.

Finally, a person is allowed to seek compensation for damage suffered from an infringement of his or her personal rights.

Penal Code

The Penal Code criminalizes the following activities relevant to the collection of personal data:

- Intercepting or recording private conversations and images without consent (unless otherwise authorized by law). Consent is presumed to be given if the concerned person does not object to the notification of the interception or recording.

- Unauthorized breaches of professional secrecy. This does not apply to the disclosure of confidential information required or authorized by law, or to sharing information on mistreatment of a child under 15 with governmental authorities.
- Violating the secrecy of correspondence and telephone conversations.
- Fraudulent access or connection to an automated data processing system.

The above violations may incur imprisonment for between one month and one year and a fine of KHR 100,000–2 million (approx. USD 25–500). For the violations below, imprisonment may be increased to between one and two years and a fine of KHR 2–4 million (approx. USD 500–1,000):

- Fraudulent access or connection to an automated data processing system that damages or alters data in that system or the functioning of the system itself.
- Obstruction of the functioning of an automated data processing system.
- Fraudulent introduction, deletion, or modification of data in an automated data processing system. Participation in (or helping to plan) any of these information technology crimes.

Law on Electronic Commerce 2019 (E-commerce Law)

On November 2, 2019, Cambodia adopted the E-commerce Law to govern all commercial and civil acts, documents, and transactions executed via an electronic system, except those related to powers of attorney, wills and succession, and real estate. The law came into force on May 23, 2020. In addition to providing legal certainty for electronic transactions, the E-commerce Law regulates domestic and cross-border e-commerce activities in Cambodia and enacts important protections for consumers, including the protection of consumer data.

The provision in the E-commerce Law that mentions data protection broadly requires any person who stores electronic data to establish all necessary measures to ensure that the data is reasonably protected from loss, unauthorized access, use, alteration, leaks, or disclosure. In addition, people who mistakenly enter the wrong details into an automated system must be allowed to correct or delete the data, unless they have benefited or caused damage to others by inputting the inaccurate information.

The E-commerce Law also prohibits the following actions:

- Electronically accessing, downloading, copying, obtaining, leaking, deleting, or altering data possessed by another person, maliciously or without consent;
- Encrypting electronic communications data or electronic evidence related to an offense or accusation thereof;
- Using another person's data for any reason with malicious intent or without authorization;
- Creating, enabling, or sharing malicious codes; and
- Creating electronic systems for purposes of falsification or causing confusion in order to obtain benefits or to attract users or transactions, and causing damage to others;

To strengthen the security of electronic transfers and payments, the E-commerce Law prohibits payment service providers from issuing a payment instrument to a consumer unless another has or needs to be replaced, or the consumer requests one.

Customers must notify service providers of any unauthorized transactions or errors in their accounts. Consumers must also notify their payment service providers electronically or in writing within two days of becoming aware of any loss or theft of electronic fund transfer instruments (or data for using them).

Additionally, payment service providers must identify consumers and verify the correctness of electronic fund transfer transactions before processing them. Unless it is a case of force majeure or there is sufficient evidence proving that the customer is at fault, payment service providers must be responsible for unauthorized transactions, fraudulent activity after a customer's notification (see above), or otherwise failing to comply with customers' orders, as well as some other technical irregularities or misuse. If payment service providers are liable in any of these circumstances, they must pay damages to customers within 30 days of receiving a consumer's notification.

The E-commerce Law also sets conditions for recognizing the security of electronic records and electronic signatures. It is legally assumed a secured electronic record is unaltered, and a secured e-signature belongs to the signatory unless proven otherwise. The E-commerce Law empowers the Ministry of Posts and Telecommunications as the competent authority to govern the security procedures for electronic records and e-signatures.

Failing to comply with the E-commerce Law is punishable by imprisonment for 1 month to 3 years and a fine from KHR 100,000 to KHR 10 million (approx. USD 25–2,500). Other disciplinary sanctions may also apply.

Industry-Specific Legislation

The Law on Banking and Financial Institutions dated November 18, 1999, is the main law governing entities licensed by the National Bank of Cambodia (NBC) to conduct banking operations in the country. It prevents anyone who participates in the administration, direction, management, internal control, or external audit of a covered entity, and employees of the latter, from providing confidential information pertaining to statements, facts, acts, figures, or the contents of accounting or administrative documents. However, the obligation of professional secrecy cannot be used as grounds for nondisclosure in relation to requests by supervisory authorities, auditors, provisional administrators, liquidators, or a court dealing with criminal proceedings.

Breaching the obligation of professional secrecy is punishable by imprisonment from one to five years, a fine of KHR 5 million to 250 million (approx. USD 1,250–62,500), or both.

The Prakas on Credit Reporting also regulates consent and data retention issues, requiring that consumer consent be obtained in advance if data will be used for anything other than the following permitted purposes:

- Evaluating the creditworthiness and over-indebtedness of a consumer in relation to a credit or loan application;
- Supporting the NBC in monitoring the credit flow of the financial system, analyzing data to produce financial stability reports, and supervising banking and financial institutions;
- Evaluating credit risks or to review or give a line of credit or a loan;
- Evaluating risks associated with transactions of deferred payments;
- Letting a consumer confirm the accuracy of his or her information in a credit report; and
- Auditing the efficiency, reliability, and legal compliance of the Credit Reporting Service (CRS).

Using credit information from the CRS for a purpose other than these is punishable by an administrative fine of KHR 5 million to 250 million (approx. USD 1,250–62,500).

All data collected by the CRS will be made available to data providers for the following periods:

Positive information	Ten years from the payment or settlement deadline
Court judgment data	Three years from the execution date
Bankruptcy data	Five years from the date of discharge
Negative information	Three years from the payment deadline

Banks and financial institutions should retain records, documents, and copies of documents involved in all forms of transactions for at least five years after the date of the transaction, and all data on a customer must be maintained for at least five years after the accounts have been closed or the business relations with the customer have ended.

The Law on Anti-Money Laundering and Combating the Financing of Terrorism permits international data transfer from the Financial Intelligence Unit to foreign financial investigators if a reciprocity agreement exists, or if the confidentiality requirements and the nature of the foreign financial investigator are similar. In addition to the penalties already mentioned, any person (including covered entities) who does the following is liable to an administrative fine of KHR 4 million to 10 million (approx. USD 1,000–2,500):

- Infringes a code of conduct or fails to provide complete and accurate credit information to the CRS within the required timeframe;
- Fails to respond to a request for information by the NBC within the timeframe specified;
- Knowingly provides the CRS with inaccurate or incomplete information regarding a consumer complaint or investigation; or
- Fails to comply with the deadlines for consumers' rights.

The Technology Risk Management Guidelines become mandatory for banks, deposit-taking financial institutions, and payment institutions on January 10, 2023. The guidelines require regulated entities to put in place an information security policy that satisfies certain conditions and to take measures to maintain the privacy of data in the context of cloud computing.

The Law on the Management of Private Medical, Paramedical, and Medical Aid Profession sets up a separate council for each of the five independent health professions recognized in the Cambodian health and pharmaceutical sector:

- Dentists
- Medical Professionals
- Midwives
- Nurses
- Pharmacists

Each professional council is empowered by an establishing royal decree to monitor professional conduct for compliance with codes of ethics to take related action as necessary. The Ministry of Health works with these councils to supervise the five professions.

The Subdecree on the Code of Medical Ethics requires medical professionals and their staff to maintain patient confidentiality, and physicians may only provide essential information and documents regarding treatment to other medical professionals involved in treating the patient, or to those professionals that the patient chooses for a consultation, and only with the patient's consent.

Dentists, nurses, midwives, and pharmacists are all subject to similar requirements under legislation specific to each profession, albeit with minor variations. Failure to comply incurs penalties under the Penal Code, which prohibits disclosing any information that falls under professional confidentiality to an unauthorized person. The prescribed penalties include imprisonment from one month to one year and a fine of KHR 100,000 to KHR 2 million (approx. USD 25–500).

The Law on Telecommunications (Telecom Law) was enacted on December 17, 2015, and guarantees telecommunications subscribers the right to privacy, security, and safety in using telecommunications services, except as otherwise determined by other laws. Subscribers are also entitled to damages caused by telecommunications operators and persons involved in the telecommunications sector in cases of breach of contract.

The Telecom Law does not contain any specific data breach provisions or limitations on data transfer, nor does it specifically require data retention. The rights mentioned above need to be upheld, however, and nothing prevents ISPs or other telecom operators from disclosing information to a government authority when requested.

LAOS

Naiyane Xaechao • Dino Santaniello

Since the enactment of the Law on Combatting and Preventing Cyber Crime No. 61/NA of July 15, 2015, which has since been mostly codified in the Penal Code No.26/NA, dated May 17, 2017, Laos has committed to protecting data circulated electronically. Though a unified data privacy regime has not been codified in a single piece of legislation, there are a number of legal instruments giving a reasonably clear picture of cybersecurity and data protection requirements and practices in the country.

The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017, and its attendant implementing regulations set rules for handling personal data in digital form. The law specifies that both individuals and legal entities can be "information owners," which are similar to data subjects under the General Data Protection Regulation (GDPR). The law also defines the "data administrator" as an individual, legal entity, or organization with the duty to manage electronic data. Government ministries, data centers, telecommunications service providers, and banks may all qualify as data administrators, which can be compared to data processors under the GDPR. The Instructions on the Implementation of the Law on Electronica Data Protection No. 2126/MPT, dated August 8, 2018, provide a nonexhaustive list of examples of those who are considered data administrators.

The law also establishes two categories of electronic data: general and specific. Specific data includes "personal information" (not further defined), health information, financial information, information on clients, and so on. It may also include state information. Specific data may not be circulated without the owner's authorization. General data can be circulated and used by anybody, as long as the source is indicated. General data is not defined by the law, but the Instructions on the Implementation of the Law on Electronica Data Protection No. 2126/MPT, dated August 8, 2018, subsequently provided some selected

practical examples of general data, such as the name of a person or legal entity, position, phone number, email address, information on the organization, general statistics, academic articles, and so on.

The Law on Electronic Data Protection imposes liability and standards on the data administrator. One of the lynchpins of these standards is the requirement for consent that must be provided by the information owner. Prior to collecting the data, the information owner must have been provided with information on the purpose (i.e., how the data will be used), relevant third parties to whom the data will be disclosed, and the period of retention. If consent is given and then the purpose changes, additional consent may need to be sought from the information owner. Consent can be withdrawn at any time, and the stored information must remain accessible to the information owner at all times.

The rights accorded to the information owner include the right to object to data collection, processing, and disclosure; the right to access a copy of the data at any time (as well as to know the source of that data); and the right to have the data manager erase or anonymize the data. These rights generally correspond to the obligations of the data administrator, which include the following:

- Ensuring that the personal data remains correct, up-to-date, complete, and not misleading.
- Implementing suitable measures for preventing loss of, unauthorized access to, alteration of, or disclosure of personal data. These measures must be reviewed when necessary, such as following a change in technology.
- Recording information relating to data in writing, or in an electronic system, which can be inspected by the information owner and relevant authorities.
- Erasing personal data when the storage period expires, the personal data becomes irrelevant, the data exceeds the scope of necessity, or consent is withdrawn.

The law also provides additional general prohibitions for individuals, legal entities, and organizations; information owners; and data administrators.

Individuals, legal entities, and organizations are prohibited from:

- doing anything to electronic data relating to secrets about the state, individuals, legal entities, or organizations—such as accessing, manipulating, sharing, or otherwise tampering—without consent;
- submitting or transferring electronic data without the consent of the information owner;
- submitting unsourced electronic information, dangerous programs, or viruses;
- creating false or dangerous electronic data that creates damage to other persons; and
- exploiting loopholes or weaknesses in electronic data systems.

Information owners are prohibited from:

- obstructing the submission of data, or improperly intercepting, accessing, destroying, or falsifying electronic data;
- intruding on or disrupting a security system's functioning;
- submitting unsourced electronic data, dangerous programs, or viruses;
- creating false or dangerous electronic data that causes damage to an individual, legal entity, or organization; and
- exploiting loopholes or weaknesses in electronic data systems.

Data administrators are prohibited from:

- doing anything to electronic data relating to secrets about the state, individuals, legal entities, or organizations—such as accessing, manipulating, sharing, or otherwise tampering—without consent;
- doing anything to electronic data (e.g., accessing, collecting, utilizing, etc.) normally managed by the data administrator without consent; and
- collecting, utilizing, or circulating electronic data about race, ethnicity, political opinion, religious belief, sexual behavior, criminal records, health records, or any other information that could influence the stability of the state or the peace and orderliness of society.

Violations of the above prohibitions may lead to fines of up to LAK 15 million (approx. USD 700).

The Law on Combatting and Preventing Cybercrime No. 61/NA (Law on Cybercrime), dated July 15, 2015, along with its related implementing instructions and decisions, is targeted primarily at hackers and actors seeking to do harm via computers.

The law provides a list of offenses regarded as cybercrimes. This list, along with the accompanying penalties, has been replicated in the Penal Code No. 26/NA, dated May 17, 2017, and is provided below.

Offense	Imprisonment term	Fine (LAK)
1. Disclosing computer access prevention measures	3 months–1 year	1–4 million
2. Accessing a computer system without authorization	3 months–1 year	2–5 million
3. Editing textual or audiovisual content without authorization	3 months–2 years	3–10 million
4. Intercepting computer data without authorization	3 months–3 years	4–20 million
5. Creating damage by means of social media	3 months–3 years	4–20 million
6. Disseminating obscene content	1–5 years	5–30 million
7. Disrupting computer systems (e.g., by using computer programs, viruses, or other instruments)	1–5 years	5–30 million
8. Forging computer data	1–5 years	5–30 million
9. Destroying computer data	3–5 years	10–50 million
10. Carrying out other activities related to cybercrimes	3–5 years	10–50 million

Note: LAK 1 million = approximately USD 47

The Law on Cybercrime provides a broad legal apparatus for many types of cybercrime. The law may prevent the circulation of inappropriate information, such as "fake news," as per items 3 and 5, as well as more technical cyberattacks on computer security systems. The law also defines principles and measures for managing, monitoring, and protecting database systems, servers, and computer data, and addresses

issues relating to the management of information collected from users on the internet. These principles are further detailed in the Recommendations on Maintaining Safety of Computer Systems No. 3623/MPT, dated December 11, 2017. These recommendations are an extension of the Law on Cybercrime and provide detailed precautions from the Ministry of Technology and Communications (previously the Ministry of Post and Telecommunications), which is in charge of such issues. These recommendations can be interpreted as the minimum security measures that must be taken by the private sector when using servers or storage equipment to store personal data. These recommendations cover five areas:

- Creation and protection of a computer network;
- Management and utilization of a computer network;
- Safe maintenance of data;
- Cooperation (with the relevant authority in charge); and
- Monitoring the safety of a computer system or network.

The Law on Cybercrime also clarifies the role of the Ministry of Technology and Communications as the authority responsible for supervising the law's implementation. One important player within the ministry is the Lao Computer Emergency Response Center (LaoCERT). For instance, in the case of a cybercrime committed by malware, a ransomware notification must be made to the Ministry of Technology and Communications at the provincial or district level. The LaoCERT will then identify the appropriate solution for dealing with this issue. The Law on Cybercrime and the Recommendations on the Implementation of the Law on Cybercrime No. 2543/MPT, dated September 24, 2018, does not seem to impose an obligation to notify the relevant authority in order to inform the public of a breach. This differs from what is required in some other jurisdictions, but the law and the recommendations only state that notification must be made in order to seek appropriate remedies from the authority in charge. There is no mention of whether the notification must be made public.

Additionally, there may be specific regulations that regulate certain industries—one example is the banking industry. In 2020, the Bank of Lao PDR issued the Decree on Consumer Protection Concerning Financial Services No. 225/GOV, dated April 6, 2020, which requires financial service providers to immediately notify affected customers if there is a data breach involving customer information. If the breach has an important adverse impact or is large in scale, a report must be submitted to the Bank of Lao PDR.

The law also sets out a series of requirements and prohibitions for service providers, including some data retention requirements: ninety days for computer traffic data, in the case of a connected system, and one year for offline traffic data.

In addition, the Penal Code addresses violations of privacy in general by prohibiting disclosure of "private confidential information" regarding another person (the statute's wording implies trade secrets) that came to the offender's knowledge during the performance of his or her profession or duties. The same article also outlaws unlawfully opening another person's correspondence or listening in on telephone conversations. Any of these acts may be punished by 3–6 months' imprisonment and a fine of LAK 3–10 million (USD 140–468).

In Myanmar, basic communications privacy and security guarantees are provided in the constitution. This seems to include a form of data privacy, as section 357 of the constitution states, "The Union shall protect the privacy and security of home, property, correspondence and other communications of citizens under the law subject to the provisions of this Constitution."

The Law Protecting the Privacy and Security of Citizens (2017) was enacted based on the above constitutional statement. Section 8 of the law contains provisions regarding communications, telecommunications, and private correspondence. This prohibits interception of or interference with personal communications and communications equipment. It also makes it a crime to demand or obtain personal telephonic and electronic communications data from telecommunication operators, or to open, search, seize, or destroy another person's private correspondence. Violators can face up to three years' imprisonment and a fine of MMK 300,000–1,500,000 (approx. USD 200–1,005).

In addition, a state of emergency has been in place since the military takeover of the government on February 1, 2021, and section 8 of the Law Protecting the Privacy and Security of Citizens, which restricted state access to private information and correspondence, was suspended by the ruling State Administration Council (SAC).

The Competition Law (2015) also contains some provisions related to data protection, with section 19 referring to the disclosure or use of another business's secrets. This specifically includes:

- using or circumventing security protocols designed to protect business secrets;
- revealing business secrets without the owner's permission;
- deceiving others into divulging these secrets;
- leaking economic information obtained illegally from a state enterprise; and
- conducting business or applying for a business license using improperly obtained information.

Violators of this section can be punished with up to two years imprisonment, a fine of up to MMK 10 million (approx. USD 6,500), or both.

The Financial Institutions Law (2016) requires banks to maintain the secrecy of information relating to customers' affairs, accounts, records, and transactions. It likewise bars directors, officers, or employees of licensed banks from disclosing any of this information, whether during the person's tenure or after. Likewise, such information that was improperly obtained should also not be further disclosed.

The subsequent section of the law does provide some limited exceptions to the duty to maintain banking secrecy. For example, the requirements do not apply to licensed credit bureaus or to the Central Bank of Myanmar (CBM) and its directors, officers, and employees when exercising the bank's powers and duties, including authorizing others to obtain bank information. In addition, the law exempts banking information from being divulged in certain circumstances, such as bankruptcy or dissolution of a business; criminal or civil proceedings; some audit and outsourcing activities; business transfer, merger, or restructuring; disclosure under the Anti-Money Laundering Law or Counter Terrorism Law; and so on.

The CBM may also share consolidated supervisory information with other financial supervisory and regulatory agencies, and the CBM is granted the power to regulate and enforce the provisions of the Financial Institutions Law, such as by issuing instructions that must be observed by banks in the country. For instance, CBM Instruction 3/2008 is on data retention, and it stipulates that banks must retain all documents related to customer accounts and transactions for at least five years after the closing of accounts or completion of a transaction.

The CMB may also impose administrative penalties against banks or relevant individuals (e.g., directors, officers, employees, etc.) for breach of any provisions of the Financial Institutions Law. Potential punishments can include warnings, fines, restriction of a bank's operations, and suspension or permanent termination from duties in the financial institution.

The Telecommunication Law 2013 protects the security of telecommunications networks. Section 66 of the law specifically bars:

- unauthorized access or disturbance of a telecommunications network, including alteration or destruction of its contents or technical standards;
- causing damage to a telecommunications network by a virus or other means; and
- stealing, cheating, misappropriating, or mishandling money or property using a telecommunications network.
- Violations can be punished by imprisonment for up to three years, a fine, or both. In addition, extorting, defaming, disturbing, or intimidating a person over a telecommunications network can be punished by imprisonment for up to two years, a fine of up to MMK 1 million, or both.

Subsequent sections of the law also address data protection by outlawing:

- dishonest distribution or receipt of incorrect information;
- unauthorized interference in or stoppage of the distribution or receipt of information;
- entrance without permission into a government-approved restricted location where telecommunications services are provided;
- obstruction of a person assigned a telecommunications-related duty by a licensee from fulfilling his or her obligation; and
- disclosure of information kept in a secured or encrypted system to any irrelevant person by any means, unless authorized by a court order.

Violation of any of these prohibitions is punishable by imprisonment for up to one year, a fine, or both.

The Myanmar government's legislative agenda is currently focused on the challenge of updating the country's many old laws, but data protection is certainly on the agenda. There have been numerous discussions about the introduction of a data protection law and regime as part of a broader cybersecurity strategy, and although nothing has been introduced yet, such regulations remain on the horizon.

Cybersecurity

The Cybersecurity Act B.E. 2562 (2019) took immediate effect upon being enacted in late May 2019. The Office of the National Cyber Security Committee and the National Cyber Security Committee (NCSC) were established as the regulators to enforce the Cybersecurity Act and supervise cybersecurity matters. The Cybersecurity Act also defines what it calls critical information infrastructure (CII) organizations, which have duties or provide services in relation to the following:

- National security;
- Material public service;
- Banking and finance;
- Information technology and telecommunications;
- Transportation and logistics;
- Energy and public utilities;
- Public health; and
- Others as prescribed by the NCSC.

Under the Cybersecurity Act, CII organizations must protect, manage, and reduce cyber risks by complying with NCSC guidelines and adhering to the duties prescribed in the act.

The act sets three levels of cybersecurity threat, based on severity. To deal with these threats, the act empowers officials to access communications information for the purpose of cybersecurity, according to rules promulgated by the cabinet. The act also features a reporting mechanism for state agencies to feed information back to the secretary of the NCSC. Where a threat could affect financial and commercial stability or national security, the NCSC is empowered to order a state agency to take action.

Personal Data

The Personal Data Protection Act B.E. 2562 (2019) (PDPA), which was enacted in tandem with the Cybersecurity Act, is the country's first unified data privacy legislation for personal data. It seeks to align with international data protection standards such as the EU's General Data Protection Regulation (GDPR). The PDPA became fully effective and enforceable on June 1, 2022, and it has extraterritorial effect, which means that data controllers and data processors located outside Thailand could also be obligated to comply with the PDPA if their processing activities fall within the extraterritorial scope of the PDPA.

While some sectors operate under their own regulations concerning data protection, they must still ensure compliance with the PDPA in specific circumstances. This is especially crucial in areas not covered by specific laws or where the sector-specific laws differ from the PDPA requirements. Since the PDPA became fully effective, various subordinate regulations have been issued to provide further clarifications on complying with the legal requirements.

The PDPA's definition of "personal data" includes any data pertaining to a living natural person that enables the identification of the data subject—the person directly or indirectly linked to the information in question.

The PDPA lays out two main roles relating to the handling of others' personal data: the data controller and the data processor. The data controller is a person or entity with power to make decisions regarding collection, use, and disclosure of personal data. The data processor is a person or entity that collects, uses, or discloses personal data on behalf of, or under the instructions of, the data controller. The data controller carries significant liability and obligations, while the processor's obligations and liabilities are very limited in comparison.

A collector of personal data must request the data subject's consent either in writing or in electronic form, unless otherwise impossible or exemptions apply (see below). Consent requests must be clear and must not be deceptive or cause the data subject to misunderstand. The data controller seeking consent must inform the data subject of the purpose of collection, the type of personal data being collected, relevant third parties to whom the data will be disclosed, the rights of the data subject, and the period of retention. Any changes to the purpose of collection, use, or disclosure will generally require further consent.

Some exceptions exist, such as when the personal data is for research or statistical analysis (provided appropriate personal data protection measures are in place) or when it helps to prevent or suppress danger to a person's life, body, or health. Also, further consent is not needed for the fulfillment of a contractual obligation. For instance, an agreement to sell goods and deliver them to various locations or email addresses would not need consent for handling each separate delivery address or email.

Data subjects are accorded a number of rights over their personal data:

Objection. The right to object to any collection, use, or disclosure of personal data at any time.

Access. The right to ask a data controller to provide a copy of the data subject's personal information and disclose where they obtained it. The data controller will now be obligated to disclose, upon request, how they obtained the data subject's personal data.

Erasure. The right to ask a controller to anonymize or delete personal data at any time.

Data portability. The right to obtain the data in a commonly used machine-readable format. This lets a data subject, for example, ask a hospital to transfer all personal data to the subject or to another hospital.

Suspension. The right to request that the collection, use, or disclosure of personal data be suspended.

Rectification. The right to request that personal data be corrected or amended.

Withdrawal of consent. The right to withdraw consent at any time.

Complaint. The right to lodge a complaint with the local authority.

Exactly how these rights may be exercised is further detailed in the PDPA. Data controllers take principal responsibility for ensuring that operations fulfill all their obligations for handling personal data, including collection, use, disclosure, and transfer. One of their duties is to ensure that throughout these steps, the personal data remains correct, up-to-date, complete, and not misleading. The data controller must also implement suitable measures for preventing loss, unauthorized access, alteration, or disclosure of personal

data. These measures must be reviewed whenever changes in circumstances make doing so necessary, such as after the implementation of technological developments.

Data controllers might be obligated to prepare and maintain records of their processing activities in a form—either written or electronic—that can be inspected by the data subject or an authority. When the storage period expires, the personal data stops being relevant, the personal data exceeds the scope of necessity, or consent is withdrawn, the data controller is also responsible for ensuring that the personal data is erased.

Data processors are required to strictly comply with the controller's lawful instructions—and conversely, not take action outside those instructions. The data processor will be responsible for implementing the measures described above, and must also record the processing of information by maintaining an inventory of the collection, transfer, and use of personal data.

Data controllers whose activities consist of collecting, using, and disclosing personal data, or if these activities require regular monitoring due to the large scale of personal data (to be set by the Personal Data Protection Commission), also have to appoint a data protection officer to conduct compliance audits or inspections.

In the event of a data breach, the data controller must report the breach to the office of the Personal Data Protection Commission within 72 hours of becoming aware of the incident, unless the breach has no risk of affecting personal rights and liberties. The controller must also notify the data subject(s) of any data breach with a high risk of affecting personal rights and liberties and provide them with remedial measures.

Penalties for noncompliance are severe. An offender may face civil liabilities including both actual damages and court-ordered punitive damages of up to twice the damage caused, administrative fines of up to THB 5 million, criminal fines of up to THB 1 million, and imprisonment for up to a year.

Computer Crimes

The Computer Crimes Act (formally the Act Governing Commission of Offenses Relating to Computers) empowers officers of the Ministry of Digital Economy and Society (MDES) to send inquiry letters, summon persons for interrogation, and request various electronic and documentary evidence from service providers. These officers can also order service providers to hand over certain user data that service providers are obligated to keep under the law.

With a court order, officers can take further actions, such as copying and investigating data or ordering a service provider to surrender or decrypt data. In terms of data retention, ministerial regulations promulgated under the Computer Crimes Act set out requirements for service providers.

The Computer Crimes Act distinguishes between content data (the actual message or communication itself) and non-content data (metadata or information related to the message or communication). A court order is generally not required for obtaining non-content data. While the Computer Crimes Act does not specifically use the term "intercept" when describing the authority of the MDES in this area, such activities could be regarded as included within an officer's authority to investigate. While there is no court decision to offer guidance on this point, it appears that an officer's authority extends to both stored data and data in transmission.

The act also obligates service providers to retain necessary information on each service user, as well as specified computer traffic data. The required computer traffic data must be stored for at least 90 days from the date the data is entered into the computer system. This period may be extended, but for no more than two years. In addition, service providers must keep user identification data from the beginning of use of the service until at least 90 days after termination of the service.

Officers investigating an offense may decrypt encrypted computer data or order its decryption. Moreover, the Computer Crimes Act purports to apply both domestically and overseas, and compliance obligations are not only applicable to certain licensees. This means that an officer can order any concerned person to decrypt data or allow access to a computer system.

The Special Investigation Act generally applies to alleged criminal violations of certain laws—typically involving unusually complex matters, national security or national interests, or influential people or officials. With respect to data interception or access, the Special Investigation Act requires special case inquiry officials to obtain a court order before accessing or acquiring documents or information in transmission suspected of being connected to a Special Case Offence (as defined in the act).

The Emergency Decree on Public Administration in a State of Emergency provides for expanded investigative powers in the event of an emergency declaration by the prime minister. This decree gives broad powers to the prime minister to act in virtually any way necessary to maintain public order or otherwise maintain control in emergency situations. This could include the prime minister authorizing the inspection of any communication (including interception of and access to data) for maintaining the security of the state or the safety of the country or the people.

VIETNAM

Waewpen Piemwichai • Phuc Huu Nguyen

Cybersecurity

Vietnam's Cybersecurity Law, which came into effect on January 1, 2019, applies to domestic and foreign companies providing services to customers in Vietnam over telecom networks or the internet, such as social networks, search engines, online advertising, online streaming and broadcasting, e-commerce websites and marketplaces, internet-based voice-and-text services (OTT services), cloud services, online games, and online applications.

Focusing especially on state and national security, the Cybersecurity Law has a broad scope of application. It potentially imposes tremendous obligations on both onshore and, especially, offshore companies providing online services to Vietnamese customers. For example, the law requires that owners of websites, portals, and social networks not provide, post, or transmit any information that is propaganda against the Vietnamese government; instigates violent disturbances, disrupts security, or disturbs public order; contains humiliating or slanderous information; or contains fabricated or untrue information (in specified contexts).

The Cybersecurity Law requires that domestic or foreign service providers of telecommunications services, internet services, or value-added services in cyberspace in Vietnam that collect, exploit or use, analyze, or process personal data store certain types of data in Vietnam for a specified period to be stipulated by the government. This includes service users' personal data, data about service users' relationships, and data

generated by service users in Vietnam. These service providers must also open branches or representative offices in Vietnam.

In order to guide the implementation of the above-mentioned regulations under the Cybersecurity Law, the government issued Decree No. 53/2022/ND-CP, dated August 15, 2022 ("Decree 53"), which took effect on October 1, 2022. Decree 53 imposes data localization conditions on foreign enterprises, compared to those applicable to domestic enterprises. In addition, foreign enterprises may also be required to establish a branch or representative office in Vietnam under this requirement.

Pursuant to Decree 53, only the following types of data are required to be stored in Vietnam:

- **Personal Data:** Data on service users' personal information (in the form of symbols, letters, numbers, images, sounds, or equivalent) capable of identifying an individual;
- **Account Data:** Data created by service users in Vietnam (in the form of symbols, letters, numbers, images, sounds, or equivalent) reflecting the service users' process of participating, operating, and using cyberspace and information on devices and network services used for connection with cyberspace in Vietnam. The information under this category of data only includes information on service account name, service usage time, credit card information, email address, IP addresses for the latest login and logout, and registered phone number associated with an account or data; and
- **Relationship Data:** Data on the relationships of service users (in the form of symbols, letters, numbers, images, sounds, or equivalent) reflecting and identifying their relationships with other people in cyberspace. Decree 53 further specifies that the information under this category of data only includes information on friends and groups with whom the service user connects or interacts in cyberspace.

Domestic companies are subject to the requirement to store these three categories of data in Vietnam if it:

- Provides services over a telecom network or the internet or provides value-added services to any customers in Vietnam; and
- Has provided services involving collecting, exploiting, analyzing, and processing any of these three categories of data.

Foreign enterprises (i.e., enterprises established or registered for establishment under the laws of foreign countries) that collect, exploit, analyze, and process service users' data in their normal business operations are required to store service users' data in Vietnam and establish a branch or representative office in the country when three additional conditions are met:

- The service it provides fall into one of the following 10 categories: (1) telecom services; (2) services of data storage and sharing in cyberspace; (3) supply of national or international domain names to service users in Vietnam; (4) e-commerce; (5) online payments; (6) intermediary payments; (7) service of transport connection via cyberspace; (8) social networking and social media; (9) online electronic games; (10) services of providing, managing, or operating other information in cyberspace in the form of messages, phone calls, video calls, email, or online chat.
- The service it provides has been used to commit a violation of the law on cybersecurity; and
- It has received a written warning about the violation from the Ministry of Public Security (MPS) and a written request for cooperation with the MPS in preventing, investigating, and dealing with the

violation, but it has failed to comply or has complied insufficiently, or has prevented, obstructed, disabled, or invalidated cybersecurity measures taken by the specialized network security force.

Upon receiving the decision above, the company has 12 months to comply with the data localization requirement. The local storage requirement starts from the company's receipt of the MPS' request for storing data, and the duration of the requirement depends on the period specified in the request (at least 24 months). The period for having a branch or representative office in Vietnam will start from the date on which the enterprise receives a request to set up such a branch or representative office and shall continue until the company no longer operates in Vietnam, or no longer provides the Regulated Services in Vietnam.

However, neither the Cybersecurity Law nor Decree 53 imposes any specific form of local data storage. Therefore, the regulated companies are free to choose the form of storage, and nothing appears to prohibit data mirroring across borders.

Personal Data

The Vietnamese government issued Decree No. 13/2023/ND-CP on Personal Data Protection (PDPD) on April 17, 2023. The PDPD took effect on July 1, 2023., without any transitional period (save in limited cases), and affects all local and foreign enterprises that directly participate in or relate to personal data processing activities in Vietnam. The PDPD is the country's most comprehensive regulation governing the field of personal data protection. It sets out key definitions for "personal data" and "consent requirements" and sets rules for personal data impact assessments.

In general, Vietnam's data protection and privacy laws apply to both Vietnamese and foreign organizations and individuals engaged in the collection, processing, use, storage, transfer, or disclosure of personal information in Vietnam.

Personal Data

"Personal data" is defined by the PDPD as electronic information in the form of symbols, letters, numbers, images, sounds, or equivalents associated with an individual or used to identify an individual. Information that helps to identify a specific individual is further clarified as information generated from an individual's activities that, when combined with other data and stored information, can identify a particular person.
The PDPD splits personal data into two categories: basic personal data and sensitive personal data.

The PDPD does not define basic personal data. Instead, it lists types of information falling into this category, including name, date of birth, gender, nationality, personal photos, phone number, identification number, marriage status, history of one's cyberspace activities, and so on. It further clarifies that any personal data not considered sensitive personal data is considered basic personal data.

Sensitive personal data, on the other hand, is defined as personal data in association with individual privacy whose infringement would directly affect the related individual's legal rights and interests. The PDPD also provides a list of sensitive personal data, including political and religious views, health status and personal information recorded in medical records (excluding information about blood type), racial or ethnic origin, data on inherited or acquired genetic characteristics, biometric data or biological characteristics, information about sex life and sexual orientation, criminal records, customer information from certain financial institutions and service providers, location data, and other personal data requiring specific protection as prescribed by law.

Consent Requirements

The PDPD's introduction of consent requirements was a remarkable change from Vietnam's existing legal regime on data privacy. Under the PDPD, consent obtained from data subjects must be clear, affirmative, and in strict compliance with the consent form under the PDPD.

Consent under the PDPD must be voluntary, based on the data subject's full understanding of

- The purpose of the personal data processing;
- The type of personal data to be processed;
- The entities authorized to process personal data;
- The data subject's rights and obligations; and
- The sensitive personal data, if any, to be processed.

In addition, consent must be expressed clearly and specifically in writing, by voice, by marking a consent box, by text message, by selecting consent technical settings, or via another demonstrative action. Moreover, consent must be expressed in a format that can be printed out or reproduced in writing, including in electronic or verifiable formats.

Silence or nonresponse by a data subject is explicitly described by the PDPD as not constituting consent. Furthermore, consent must be made for a single purpose; multiple purposes need to be demonstrated in a way that data subjects can give consent to each purpose individually. Data subjects may also opt to provide partial or conditional consent.

However, the PDPD sets out that the processing of personal data without consent is permissible in the following circumstances:

- In urgent cases where it is necessary to immediately process relevant personal data to protect the life or health of the data subject or others;
- Where the public disclosure of personal data is in accordance with the law;
- When the processing of data is performed by competent state agencies in the event of a state of emergency related to national defense, national security, social order and safety, major disaster, or dangerous epidemic; when there is a threat to security and national defense but not to the extent that a state of emergency must be declared; or when the processing is to prevent and combat riots and terrorism, crimes, and violations of the law;
- The processing is to fulfill the contractual obligations of the data subject with relevant agencies, organizations, or individuals as prescribed by law; or
- The processing is to serve the activities of state agencies prescribed by sector-specific laws.

Data Processing Impact Assessment and Cross-Border Data Transfer Impact Assessment

Data Processing Impact Assessment

Another key requirement under the PDPD is the obligation to establish a personal data processing impact assessment (DPIA) using a statutory form. The DPIA must be submitted to the Department of Cybersecurity and Hi-Tech Crime Prevention (A05), under the MPS, within 60 days of the processing and must remain available at all times for inspection and evaluation by the MPS. This obligation is imposed on data

controllers and data processors alike, applying to any controller from the time it starts to process personal data and to any processor from the signature of a contract with a controller.

Cross-Border Data Transfer Impact Assessment

The cross-border transfer of personal data is broadly defined and includes the act of processing personal data of Vietnamese citizens using servers or automated systems located outside of Vietnam. In any such cases of cross-border transfer of Vietnamese citizens' personal data, the transferor (which could be either the data controller or the data processor) must prepare a cross-border data transfer impact assessment (TIA) based on a statutory form, covering all required information. This includes the following:

- Contact information and details of the transferor and the transferee(s);
- Name and contact details of the organization or individual under the transferor involved in transferring and receiving the data;
- Description and explanation about the objectives of the personal data processing after the personal data is transferred abroad;
- Description and clarification of the type of personal data to be transferred abroad;
- Explanation regarding compliance with the regulations on personal data protection under the PDPD, and detailed personal data protection measures;
- Assessment of the impact of the personal data processing, undesirable consequences and damage that may occur, and measures for reducing or removing such consequences and damage;
- Consent of the data subject according to the PDPD, with information on the mechanism for feedback and complaint in case of arising problems or requests; and
- Document that shows binding obligations and responsibilities between the transferor and the transferee(s) for the personal data processing.

The TIA must be available at all times for inspection and evaluation by the A05 and MPS. The data transferor must also submit an original copy of the TIA to the A05 within 60 days of its processing. The TIA is not a prerequisite for the cross-border transfer of personal data, but this requirement is rather triggered by the cross-border transfer itself. The TIA only serves as a notification to the authority of the personal data cross-border transfer activities for their subsequent inspection and cannot be considered an approval. However, failure to comply with the TIA requirements could lead to the A05/MPS ordering the data transferor to stop transferring the data across the Vietnam border.

In accordance with the TIA, the transferor and the transferee must ensure that they agree on a clear attribution of obligations and responsibilities related to personal data protection. The authorities have not issued any standard contractual clause templates or any further guidance as to what must be included in a transfer agreement.
After the personal data of Vietnamese citizens is successfully transferred outside of Vietnam, the transferor must also notify the A05 about the data transfer and contact details of the organization or individual in charge of the transfer.

Enforcement

The sanctions in relation to data protection breaches are scattered across various laws and regulations. In general, the major type of sanction is an administrative penalty. For example, failure to obtain data subjects' prior consent for the collection, processing, and use of their information is subject to a fine of VND 10–20 million (approx. USD 390–785). In serious cases, according to the Criminal Code, illegal use of information

on a computer or telecommunications network may be punished by a monetary fine of VND 30 million–1 billion, mandatory community service for up to 3 years, or 6 months–7 years' imprisonment. Offenders might also be liable for a fine varying from VND 20–200 million or be prohibited from holding certain positions or doing certain jobs for 1–5 years.

There are currently no sanctions for other violations under the PDPD (such as failure to prepare and file a DPIA/TIA with the authority). There has not yet been any enforcement of the PDPD, considering the lack of penalties or remedies. However, this is expected to soon change, as the authorities are developing a new decree on administrative sanctions for cybersecurity violations. A recent release of this draft decree includes both sanctions and remedial measures. As the planned regulation is still in the drafting stage, its final contents may be impacted by future developments and are subject to change before its official enactment.

AUTHORS

CAMBODIA

Jay Cohen	jay.c@tilleke.com
Chandavya Ing	chandavya.i@tilleke.com

LAOS

Naiyane Xaechao	naiyane.x@tilleke.com
Dino Santaniello	dino.s@tilleke.com

MYANMAR

Nwe Oo	nweoo@tilleke.com

THAILAND

Nopparat Lalitkomon	nopparat.l@tilleke.com
Gvavalin Mahakunkitchareon	gvavalin.m@tilleke.com

VIETNAM

Waewpen Piemwichai	waewpen.p@tilleke.com
Phuc Huu Nguyen	phuc.n@tilleke.com


Chandavya Ing


Dino Santaniello


Gvavalin Mahakunkitchareon


Jay Cohen


Naiyane Xaechao


Nopparat Lalitkomon


Nwe Oo


Phuc Huu Nguyen


Waewpen Piemwichai

www.tilleke.com