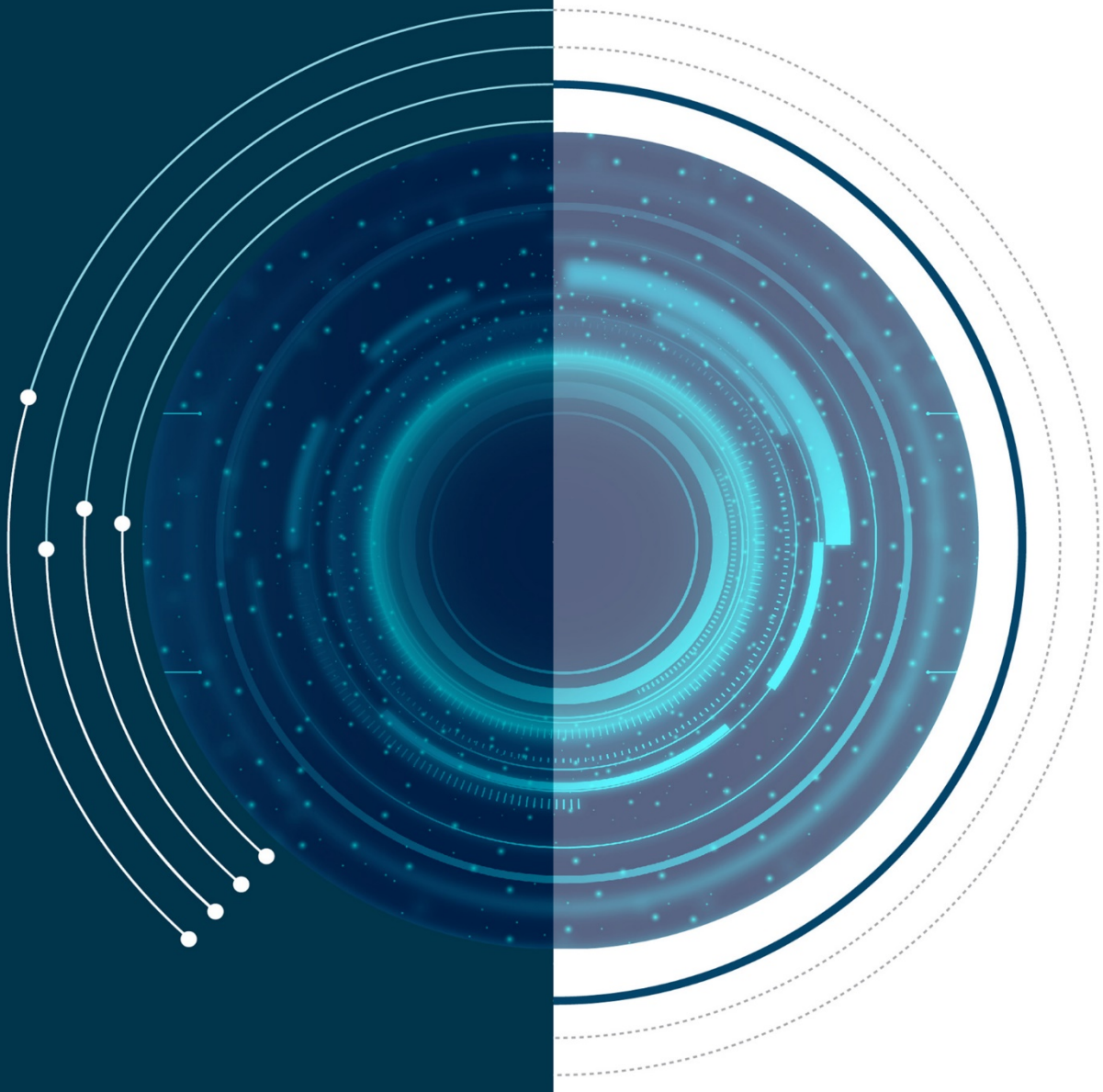
Tilleke & Gibbins

Regional Guide to Cybersecurity and Data Protection in Mainland Southeast Asia



Data protection matters in Cambodia fall broadly under the right to privacy as addressed in Cambodia's constitution, and certain provisions under the Civil Code, the Penal Code, and the recently enacted Law on Electronic Commerce (E-commerce Law). Several laws for specific industries also deal with data protection issues.

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.

Civil Code

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.

The Civil Code also potentially affects contractual agreements on personal data. If personal data is protected as part of an individual's personal rights, then accessing, obtaining, processing, or otherwise commercializing personal data must be contractual, and thus requires the data owner's consent in a valid agreement.

The confirmation of an offer and an acceptance is a requirement for an agreement to be valid. This means that express consent must be obtained from data owners for the purpose for which their data is used, potentially creating proper disclosure obligations for obtaining data owners' consent.

The Civil Code also allows a person to rescind an agreement under certain circumstances, and it appears that this can apply to data subject consent if it was the result of mistake or misunderstanding (e.g., misleading material terms to obtain a user's consent); fraud; misrepresentation; or exploitation of the situation, such as failing to explain technical provisions.

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. 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. Under the E-commerce Law, which came into force on May 23, 2020, any person who privately stores electronic data must 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 from 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.

The Law on Consumer Protection was also enacted on November 2, 2019, and came into force on November 3, 2019. Though it does not contain any provisions that specifically address cybersecurity and data protection, this law establishes widely applicable rules to guarantee the rights of consumers and to ensure that businesses conduct commercial activities in Cambodia fairly. It is plausible that Cambodia's governmental bodies will issue related implementing regulations that address these issues.

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 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 stipulates 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 choses 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 case 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

Dino Santaniello

Since around 2015, Laos has committed to protecting data—especially information that is 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 data subjects. The law also defines the "data manager" as the individual, legal entity, or organization with the duty to manage electronic data. Government ministries, data centers, telecommunications service providers, and banks are all example of data managers.

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 on 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 manager. One of the lynchpins of these standards is the requirement for consent, which must be made in writing or via electronic means. The information manager must provide 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. Note that if consent is given and then the purpose changes, additional consent may need to be sought from the data subject. Consent can be withdrawn at any time, and the stored information must remain accessible to the data subject at all times.

The rights accorded to the data subject 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 manager, 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 data subject 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.
- Taking action in the event of a data breach by notifying the relevant authorities and the data subject, as well as providing the data subject with remedial measures.

The law also provides additional general prohibitions for individuals, legal entities, and organizations; data subjects; and data managers.

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 data subject;
- 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.

Data subjects 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 managers 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 manager 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 1,690).

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 110

The Law on Cybercrime provides a broad legal apparatus for many types of cybercrimes. 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 System 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 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 in using servers or storage equipment to keep 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 Post and Telecommunications 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 Post and Telecommunications 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.

In addition, the law 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 violation 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 330–1,100).

MYANMAR

Nwe Oo

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).

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) in section 81 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 Financial Institutions Law, such as by the issuing of 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.

THAILAND

Athistha (Nop) Chitranukroh
Gvavalin Mahakunkitchareon

Cybersecurity

The Cybersecurity Act B.E. 2562 (2019) took immediate effect upon being enacted in late May 2019. The Office of 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). Initially, most of its provisions were scheduled to take effect on May 27, 2020. However, in the aftermath of the COVID-19 pandemic, an extensive list of organizations and business activities were granted an extension to the compliance deadline until May 31, 2021. As a result, most of the PDPA's provisions will now be enforceable from June 1, 2021, onward.

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, 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 fulfilment 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 commonly used machine-readable format. This right 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 circumstance 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 case of data breach, the data controller must report the breach to the office of the Personal Data Protection Commissions 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 that has 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 • Thao Thu Bui

Vietnam's Law on Cyber-Information Security (LCIS), which took effect on July 1, 2016, is Vietnam's first comprehensive law on the security of "cyber-information," or information exchanged in a telecommunications or computer network environment. Previous rules on the subject had been scattered throughout different legislation and information security regulations for specific sectors. The key aspects of the LCIS include:

- assurances for the safety and security of cyber-information;
- protection of personal information in the network environment;
- protection of information systems and infrastructure;
- production, trading, and use of civil ciphers;
- standards and technical regulations on information security;
- provision of information security services;
- prevention of spam, computer viruses, and harmful software; and
- emergency responses.

In addition, the use of encryption products and services in the private sector is regulated under the LCIS. Individuals and organizations using encryption are obligated to provide necessary information on the encryption keys to the authorities if requested. Likewise, they must cooperate with the authorities to carry out actions that prevent criminals from stealing information or encryption data and using encryption products for illegal purposes. Finally, use of encryption products not provided by permitted enterprises (except for foreign diplomatic and consulate organizations and international organization representative offices) must be reported to the Government Cipher Committee.

While the LCIS and its guiding decree do not clarify in which specific circumstances the government may request encryption keys from a private entity, authorities might be able to base their request on various other legislation, depending on the matter at hand.
A separate Cybersecurity Law came into effect on January 1, 2019. The law 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 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 new 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).

This means websites and social networks must not post or allow their users to post "anti-state," "offensive," or "inciting" content. Furthermore, service providers must develop mechanisms to monitor, verify, and take down prohibited content posted by their users within 24 hours after receiving a request from government authorities. Similar but conflicting requirements exist in other legislation; for example, regulations on general websites and social networks set a time limit of three hours for service providers to take down violating content.

These requirements may diminish the website or social network operators' "safe harbor" under other valid legislation that protects them from the responsibility to monitor or supervise their users' digital information, or investigate breaches of the law arising from the process of transmitting or storing their users' digital information.

In addition, domestic and foreign companies providing services over telecommunications networks, the internet, or value-added services in cyberspace in Vietnam must:

- authenticate users' information upon registration;
- keep user information confidential;
- cooperate with Vietnamese authorities to provide information on their users when such users are investigated or deemed to have breached laws on cybersecurity;
- store, in Vietnam, for a to-be-determined period of time, users' personal information, data on service users' relationships, and data generated by service users in Vietnam (definitions and scopes of all such user-related data are not clearly provided under the Cybersecurity Law, but will be further detailed in subsequent legislation—see below); and,
- for foreign service providers, maintain branches or representative offices in Vietnam.

The controversial provision on local data storage mentioned above has a very broad scope and vague requirements, and has not yet been enforced in practice. The government has assigned the Ministry of Public Security (MPS) to draft a decree to narrow down the scope of application and provide more-detailed definitions.

A draft decree dated August 2019 sets the scope of service providers subject to the data localization and local establishment requirements to include:

- telecom services;
- data storage and data sharing services in cyberspace;

- services of provision of national or international domain names for users in Vietnam;
- e-commerce services;
- online payment providers;
- payment intermediary services;
- transportation connection services through cyberspace;
- social network services and social communication services;
- online game services; and
- email services.

Under the draft decree, service providers that fail to undertake measures to stop and apprehend acts that violate Vietnamese law (or that resist, obstruct, or ignore requests from the relevant authorities) would trigger the data localization and local establishment requirements. Service providers will have a six-month grace period upon receiving a request from the authorities to comply with the data localization and local establishment requirements.

The draft decree also specifies the data that may be required to be stored in Vietnam. This comprises:

- Personal information that can identify service users in Vietnam;
- Data generated by service users in Vietnam (e.g., account name, duration of use, credit card information, email address, IP address, etc.); and
- Data on the relationships of service users in Vietnam (e.g., friends and group memberships).

The period for storing data in Vietnam starts from the date on which the service provider receives a request for storage of data. The draft decree stipulates that the period for storage must be at least 12 months, but it does not provide further guidance on the duration.

The penalties for noncompliance with the requirements of the Cybersecurity Law are still unclear, as are measures for the Vietnamese authorities to enforce against offshore service providers. It is expected that subsequent subordinate legislation will provide more details on the law's implementation.

Inspections and investigations are authorized in a number of Vietnamese laws, which empower certain government authorities—such as the Inspectorate of the Ministry of Information and Communications and the investigation agencies of the People's Police—to obtain access to private communication. In particular, government authorities may have the power to access and examine information, equipment or systems of the relevant parties if there is a suspected violation of relevant laws and regulations. The inspectorate and the investigation agencies, with proper search warrants, may also access systems of telecom companies to intercept communications for a particular individual.

AUTHORS

CAMBODIA

Jay Cohen	jay.c@tilleke.com
Pichrotanak Bunthan	pichrotanak.b@tilleke.com

LAOS

Dino Santaniello	dino.s@tilleke.com

MYANMAR

Nwe Oo	nweoo@tilleke.com

THAILAND

Athistha (Nop) Chitranukroh	nop.c@tilleke.com
Gvavalin Mahakunkitchareon	gvavalin.m@tilleke.com

VIETNAM

Thao Thu Bui	thao.b@tilleke.com
Waewpen Piemwichai	waewpen.p@tilleke.com


Athistha (Nop) Chitranukroh

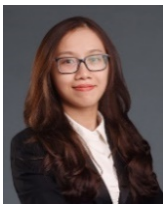

Dino Santaniello


Gvavalin Mahakunkitchareon


Jay Cohen


Nwe Oo


Pichrotanak Bunthan


Thao Thu Bui


Waewpen Piemwichai

bangkok • hanoi • ho chi minh city • jakarta • phnom penh • vientiane • yangon