Tilleke & Gibbins

RESPONDING TO A

Data Breach

in Southeast Asia

CAMBODIA • INDONESIA • LAOS • MYANMAR • THAILAND • VIETNAM

www.tilleke.com

When your company suffers a data breach, taking prudent, careful action can limit and perhaps even rectify some of the damage.

First of all, it is important to document everything, starting with the time the data breach was discovered. Secure the data systems and preserve all evidence so that investigators can determine what happened, and begin following the protocol that all companies handling personal data should have in place to guide their data breach response. It is also crucial to seek timely legal assistance to ensure that every aspect of the response is planned and carried out according to the law.

While applicable legal advice for each situation can only be obtained by consulting a legal advisor, this guide gives an overview of what companies in Southeast Asian jurisdictions can expect if they suffer a data breach.

Notifying the Regulators

1. Are companies required to notify a regulator of certain data breaches—and if so, who is the regulator in your jurisdiction?	
Cambodia	No. Matters pertaining to data protection fall under the right to privacy guaranteed in broad terms under Cambodia's constitution, and under some specific laws—none of which impose data breach notification obligations.
Laos	No. The Law on Electronic Data only suggests that companies can voluntarily report data breaches to the Department of Cyber Security (DCS) in the Ministry of Technology and Communications (MTC) to receive technical assistance. The Law on Cybercrime does not require data breach notification.
Myanmar	No.
Thailand	Yes. The Office of the Personal Data Protection Commission (PDPC) is to be notified of all reportable data breaches. Some sector-specific notification requirements may also apply.
Vietnam	Yes. The regulators include the Vietnam Computer Emergency Response Team (VNCERT) under the Ministry of Information and Communications, the Department of Cyber Security and High-Tech Crime Prevention under the Ministry of Public Security, the Ministry of Public Security (privacy regulator) and other industry-specific regulators.

2. What types of data breach would trigger the reporting obligations?

Cambodia	N/A
Laos	N/A
Myanmar	N/A
Thailand	All confidentiality, integrity, or availability breaches must be reported, unless the breach does not risk affecting a person's rights or freedom.
Vietnam	A data breach must be reported if: • There is any violation of laws pertaining to personal data protection in Vietnam; • Any affected data system is in Vietnam; • The affected data system is used for online services specified by the Law on Cybersecurity; or • The rights and interests of the affected persons are (or are likely to be) damaged.

3. Is there any exemption to the breach notification requirement?

Cambodia	N/A
Laos	N/A
Myanmar	N/A
Thailand	Yes. A data controller may seek an exemption from the requirement to notify the PDPC if it can prove with proper information, documents, or evidence that there is no risk of adversely affecting the rights and freedoms of persons.
Vietnam	No.

4. What is the required timeline for reporting a breach to the regulator?

Cambodia	N/A
Laos	N/A
Myanmar	N/A
Thailand	Without delay and within 72 hours upon becoming aware of the data breach.
Vietnam	Within five days from the date the incident is detected, unless industry-specific laws indicate otherwise. For breaches involving personal data, within 72 hours from the occurrence of the incident.

5. Is there a required specific form to be used for reporting a breach to the regulator?

Cambodia	N/A
Laos	N/A (except for DCS notification—see Q1)
Myanmar	N/A
Thailand	No.
Vietnam	In certain situations, yes, a specific form is required.

6. What must be included in the report to the regulator?

Cambodia	N/A
Laos	N/A
Myanmar	N/A
Thailand	The notification must contain the following details, as far as practicable: • Brief information about the nature and type of the breach; • Name, contact details, and contact method of the data protection officer (DPO) or other person designated by the data controller as a coordinator; • Information about possible consequences of the breach; and • Information about the relevant measures taken by the data controller to prevent, cease, or correct the breach, or to mitigate damage.
Vietnam	Generally, the report should include the following: • Name and address of the submitter and the DPO; • Name, domain name, and IP address of the affected information system; • Names and addresses of the owner and the operator of the information network; • Description of the incident and time of detection; • Affected data subjects, types of personal data, and amount involved; and • Results and recommendations, including measures for handling and minimizing the harm caused by the incident.

7. Is it required to use local language when reporting a breach to the regulator?

Cambodia	N/A
Laos	N/A (but DCS notification must be in Lao).
Myanmar	N/A
Thailand	It is expected to be in Thai, though this is not addressed in the law.
Vietnam	Yes. Though not clearly specified in the law, the authorities usually require all submitted information and documents to be in Vietnamese.

Notifying Customers

8. What types of data breaches is a company legally required to notify its customers about?

Cambodia	None, but see Q1.
Laos	None, under the Law on Electronic Data Protection. However, financial institutions may need to report certain breaches under a decree of the Bank of Lao PDR.
Myanmar	None
Thailand	Data breaches with a high risk of affecting the rights and freedom of the data subject.
Vietnam	Data breaches with a high risk of affecting the data subject's legitimate rights and interests.

9. Is there any exemption to the breach notification requirement?

Cambodia	N/A
Laos	N/A
Myanmar	N/A
Thailand	If the data controller can prove there is no risk of adversely affecting persons' rights and freedoms, the data controller is not required to notify the PDPC or the data subjects (e.g., customers).
Vietnam	No.

10. Which customers must be notified (e.g., only customers whose identifying data was compromised, all customers, etc.)?

Cambodia	N/A
Laos	N/A
Myanmar	N/A
Thailand	Only customers whose identifying data was compromised.
Vietnam	Generally, only affected customers whose legitimate rights and interests are very likely to be seriously damaged. Generally, only affected customers whose legitimate rights and interests are very likely to be seriously damaged.

11. What is the timeline for sending a required notification to customers?

Cambodia	N/A
Laos	N/A
Myanmar	N/A
Thailand	Without delay upon becoming aware of the data breach.
Vietnam	Without delay upon becoming aware of the data breach.

12. What must be included in the notification to customers?

Cambodia	N/A
Laos	N/A
Myanmar	N/A
Thailand	The notification must contain the following details, as far as practicable: • Brief information about the nature of the breach; • Name, contact details, and contact method of the DPO or other person designated by the data controller as a coordinator; • Information about possible consequences of the breach on data subjects; and • Information about remedial actions to mitigate damage to data subjects, and brief information about initiated or planned measures to prevent, cease, or correct the breach, including recommended measures that data subjects should take to prevent, cease, or correct the breach, or to mitigate damage.
Vietnam	Not specifically prescribed, but regulators suggest it should match the list in Q6.

Operational Requirements

13. Who (someone within the company or a representative) is authorized to investigate and handle the evidence of a data breach?	
Cambodia	Not addressed under Cambodian law.
Laos	This is not addressed, but the data administrators can liaise with the DCS to seek advice on intrusions that cause damages.
Myanmar	N/A
Thailand	The company may appoint any person, including the DPO, to be the responsible person.
Vietnam	The company may appoint any person to be the responsible person. A data protection department and a DPO are also required if the company processes personal data, particularly sensitive personal data.

14. Besides reporting and notification requirements, are companies required to take other steps in response to a data breach?	
Cambodia	No, but see Q1.
Laos	Data administrators must take appropriate action to solve any security- or threat-related issues when they are discovered or before a problem occurs.
Myanmar	No.
Thailand	No, but the company should undertake all necessary actions to prevent a further data breach.
Vietnam	Yes. Companies must promptly take remedial or blocking measures. Serious incidents that may impact national cyber-information security require implementation of action plans according to details and procedures prescribed by law.

Preventive Security Requirements and Accountability

15. What security requirements for preventing a data breach are companies required to observe?	
Cambodia	The E-Commerce Law requires anyone who privately stores electronic data to ensure it is protected from loss or unauthorized access, use, alteration, leaks, or disclosure. However, the standard of safe protection of private information has not yet been defined. Banks and financial institutions following the government's Technology Risk Management Guidelines should have risk management practices and internal controls to achieve data confidentiality, system security, reliability, resiliency, and recoverability in the organization. These include the classification of data according to its sensitivity and criticality.

Laos	The MTC's predecessor ministry issued computer security instructions that outlined nonbinding IT safety and data protection best practices. The Law on Electronic Data Protection directs data administrators to: • Prioritize all data and adopt corresponding security; • Assign a responsible employee(s); • Maintain adequate systems for storage, use, and safeguarding of data; • Keep a backup system for destroyed or deleted data; • Ensure good maintenance by recording information using paper, magnetic storage, or other appropriate means; • Conduct annual risk assessment of the protection system and correct any issues uncovered; • Protect system access from intrusion, viruses, and other risks; • Remedy adverse events that have occurred or are about to occur. The transfer of financial, banking, investment, or accounting data, and passwords using digital certificates, must receive MPT approval.
Myanmar	Various laws and regulations impose an obligation on the relevant entities to keep certain information confidential, thus requiring that they have adequate security measures to ensure this. For instance: • Financial institutions must maintain banking secrecy. • Telecommunications licensees must keep confidential and personal information secure. • Health care providers must keep patients' personal health information confidential. • Personal data administrators (PDAs) must keep personal data secure The Telecommunications Law (2013) prohibits disclosure of information kept on a secure or encrypted system to any "irrelevant person," implying that companies must provide adequate security measures to ensure this does not happen. Under the 2021 amendment to the Electronic Transactions Law (ETL), PDAs must maintain, protect, and manage personal data systematically in line with law and with a level of security appropriate to the type of data. They may not provide personal data to third parties without the data owner's consent unless otherwise permitted by law.
Thailand	A subordinate regulation issued in 2022 sets the minimum required security measures for data controllers in processing personal data. Accordingly, a company, as a data controller, must maintain security of personal data in relation to confidentiality, integrity, and availability in order to prevent loss, unlawful access, use, alteration, modification, or disclosure. Security measures must at least: • Cover collection, use, and disclosure of personal data, regardless of form (e.g., documents or electronic data); • Include organizational and technical measures—and potentially physical measures—accounting for the risk level according to the nature and purpose of the data-processing activity and potential for, occurrence of, and impact from a personal data breach event; • Cover every component of an information system in relation to personal data collection, use, and disclosure; • Maintain access control in accordance with the list in the minimum required security measures under the subordinate regulation.

Vietnam	The construction, operation, and maintenance of a data system physically located in Vietnam must conform to cybersecurity measures and requirements set out under the Law on Network Information Security and its subordinate legislation (e.g., Decree 85). To comply with the Personal Data Protection Decree, operators must also implement organizational and technical measures and appropriate safety and security measures to prove that data processing activities are carried out in accordance with the law on personal data protection, and review and update these measures as necessary

16. Who is responsible for ensuring compliance with all data protection requirements?

Cambodia	The party in a company who is responsible for ensuring compliance with data protection requirements is not specified by law. However, the Criminal Code penalizes anyone directly involved in breaching a legal obligation or prohibition. Thus, anyone with decision-making authority over offending acts is responsible.
Laos	Lao law does not provide information on who in a legal entity is responsible for data protection. The Law on Electronic Data Protection provides that an employee or team must be appointed to ensure protection of sensitive data; however, no qualification or further information is provided.
Myanmar	N/A
Thailand	This is not specifically addressed in the PDPA. However, if the company appoints a DPO, the DPO is obligated to examine the company's operations, including employees and contractors, to ensure that collection, use or disclosure of personal data complies with the PDPA.
Vietnam	Generally, the law provides that the owner of the data system is responsible for directing and undertaking data security measures as required by law. If there is no independent unit specializing in data security, the owner must establish or designate a specialized IT unit to be in charge of data security activities. For personal data, this is the internal data protection department and the DPO.

17. What are the possible punishments and penalties for allowing a data breach or failing to maintain the required security?

Cambodia	Failure to comply with data protection obligations to ensure that private information is safely protected is punishable by imprisonment for 1–2 years and a fine of KHR 2–4 million (approx. USD 500–1,000).
Laos	The Law on Electronic Data Protection provides only that an individual or legal entity breaching the law will be subject to warnings, fines, education measures, or civil or criminal charges depending on the offense. A fine of LAK 15 million (approx. USD 1,600) will be imposed for contravention of the Law on Electronic Data Protection. Under the Penal Code, causing damage to another person through disclosure of that person's "private confidential information" during the performance of a profession or duties is subject to 3–6 months' imprisonment and a fine of LAK 3–10 million (approx. USD 170-580).

Myanmar	• For breach of banking secrecy: Fines and a license suspension or termination. • For a telecommunications licensee's failure to maintain confidentiality of personal information: Warnings, license suspensions, or license termination. • For disclosure of information in a secure or encrypted system to an irrelevant person: One year of imprisonment, an unspecified fine, or both. • For violating the obligation on health care providers: No penalty is specified in the relevant law, but applicable administrative sanctions could include withdrawal of the license to provide health care. • For a PDA's failure to meet ETL requirements for managing personal data: 1–3 years' imprisonment, a fine of up to MMK 10 million (approx. USD 5,700), or both. • For a PDA obtaining, disclosing, using, modifying, disseminating, or sending personal data to a third party without the data subject's consent: 1–3 years' imprisonment, a fine of up to MMK 5 million (approx. USD 2,850), or both.
Thailand	Civil Liabilities Violation or noncompliance causing damage to a data subject may require the relevant company to compensate the data subject for actual damages and/or punitive damages of up to twice the amount of actual damages (except in cases of force majeure, acts or omissions of the data subject, and complying with a competent authority's order). Administrative Penalties Failure to maintain appropriate security measures or to report a data breach could incur a fine of up to THB 3 million (approx. USD 90,000).
Vietnam	Civil Liabilities Violation or noncompliance causing damage to a data subject may require the data system owner to compensate the data subject for actual loss/damage and direct profit. Administrative Penalties Failure to maintain appropriate security measures or to report a data breach could subject the violator to an administrative penalty of up to VND 40 million (approx. USD 1,700). In addition, administrative sanctions may be applied.

CONTACTS

CAMBODIA

Jay Cohen — jay.c@tilleke.com

LAOS

Dino Santaniello — dino.s@tilleke.com

MYANMAR

Yuwadee Thean-ngarm — yuwadee.t@tilleke.com

THAILAND

Nopparat Lalitkomon — nopparat.l@tilleke.com

VIETNAM

Waewpen Piemwichai — waewpen.p@tilleke.com

Dino Santaniello

Jay Cohen

Nopparat Lalitkomon

Waewpen Piemwichai

Yuwadee Thean-ngarm

www.tilleke.com