DATA PROTECTION LAWS OF THE WORLD

Cambodia

DLA PIPER

Downloaded: 29 April 2024

CAMBODIA

Last modified 18 January 2024

LAW

The Ministry of Post and Telecommunications (**MPTC**) announced on 19 February 2021 their intention to prepare a comprehensive personal data protection law after finalizing the draft cybersecurity law.

On 22 December 2021, the Royal Government of Cambodia issued Sub-Decree No. 252 on the Management, Use, and Protection of Personal Identification Data (only available in Khmer) (Sub-Decree 252) in order to promote broad policy objections, such as:

- ensuring the protection of peace and order;
- serving the public interest; and
- promoting national development by improving the provision of services.

However, Sub-Decree 252 only applies to "personal identification data" owned by the Ministry of Interior (MOI) and does not apply to personal identification data used by other entities.

In September 2023, the MPTC made available to select private organizations and companies a Draft Law on Personal Data Protection for their review and comment. However, it has not been made available to the public as of writing. Therefore, the information provided regarding the data protection law should be used as a reference and not considered final, as the draft law has not been officially released to the public. The Draft Law on Personal Data Protection establishes rules, principles, and mechanisms to govern the collection, use, and disclosure of personal data. Its main objective is to safeguard the privacy rights of individuals and encourage the lawful and responsible use of personal data.

The E-Commerce Law contains provisions for the protection of consumer data that has been gathered over the course of electronic communications. The E-Commerce Law is thereby restricted in scope to virtual and / or digital data protection.

Other matters pertaining to data protection typically fall under the right to privacy, which is protected in broad terms under the Constitution of the Kingdom of Cambodia 2010, the Civil Code of the Kingdom of Cambodia 2007, the Criminal Code of the Kingdom of Cambodia 2009, the Code of Criminal Procedure of the Kingdom of Cambodia 2010, and other specific laws such as the Banking Law.

DEFINITIONS

Definition of Personal Data

Cambodian law does not specifically define the term "personal data," or discuss what specific information constitutes personal data.

The E-commerce Law defines the term "data" as "a group of numbers, characters, symbols, messages, images, sounds, videos, information or electronic programs that are prepared in a form suitable for use in a database or an electronic system".

According to the Draft Law on Personal Data Protection, personal data is defined as information pertaining to an individual that can directly or indirectly identify them. This information includes, but is not limited to, names, identification numbers, location data, and online identifiers. As the Law on Personal Data Protection has not yet been implemented, this definition should not be regarded as official.

Therefore, due to the absence of a definition of "personal data", it remains plausible that any data of a data subject may be viewed by the regulatory and enforcement authorities as personal data of that data subject. As such, conventional data, such as full names, national identification numbers, passport numbers, photographs, video, images, phone numbers, personal email addresses, biometric data, IP addresses, and other network identifiers, etc., may arguably constitute personal data.

Definition of Sensitive Personal Data

There is no express definition of what constitutes sensitive personal data. That said, based on laws applicable to persons and entities in other sectors (such as healthcare and banking), the types of data below are generally considered to be of a more sensitive nature, and thus should be handled with more stringent data protection mechanisms:

- medical data;
- financial data;
- personal data of children; and
- personal identifiers (e.g. national identification cards and passport details).

As there is no clear limit as to the scope of what may be considered sensitive data, any data of a data subject should be prudently treated as sensitive data to the greatest extent possible.

NATIONAL DATA PROTECTION AUTHORITY

Since Cambodia does not have any dedicated laws on data protection, there are no regulatory or enforcement authorities that are specifically tasked with handling, overseeing or implementing personal data protection matters in Cambodia.

That said, the following governmental bodies may have substantial powers over data protection matters:

- the Ministry of Commerce (“**MOC**”);
- the Ministry of Post and Telecommunications (“**MPTC**”); and
- the Ministry of Interior (“**MOI**”).

REGISTRATION

Since Cambodia does not have any dedicated laws on data protection, there are no specific registration requirements for data protection. However, “Electronic Commerce Service Providers” and “Intermediaries” (in an e-commerce context), who would likely store, process and transfer the data of the data subjects, must register with the MOC and MPTC.

Under the E-Commerce Law, “Electronic Commerce Service Providers” are defined as persons who use electronic means to supply goods and / or services, except insurance institutions, and an “Intermediary” is broadly defined as a person who provides services of sending, receiving, transmitting or storing, either on a temporary or permanent basis, electronic communications, or other services relating to electronic communications, including persons who represent the originators; persons providing means of seeking any data in an electronic system; persons providing online marketing and online commercial services; and other persons as specified under the E-Commerce Law.

DATA PROTECTION OFFICERS

Since Cambodia does not have any dedicated laws on data protection, there are no specific requirements in Cambodia to appoint data protection officers who are specifically tasked with handling, overseeing or implementing data protection matters in Cambodia.

COLLECTION & PROCESSING

As Cambodia has not enacted any dedicated or comprehensive data protection laws, there are no laws or regulations in Cambodia that explicitly and specifically discuss the concept of collection and processing of data.

However, under the Draft Law on Personal Data Protection, the term “data controller” is defined as a natural person, private legal entity, public establishment of administrative character, or public entry that determines the purpose and means of collecting, using, or disclosing personal data. On the other hand, a “data processor” is defined as a natural person, private legal entity, public establishment of administrative character, or public entry that processes personal data on behalf of a data controller or public authority.

Based on Cambodia’s existing legal framework for data privacy, seven data protection obligations are either implied or explicitly imposed. Those obligations are discussed below.

1. Consent Obligation: There is no explicit statutory requirement to obtain consent, or penalty for failing to obtain such consent under Cambodian law when collecting and processing of data. However, the Civil Code and several other pieces of legislation indicate that there is a general recognition of the protection of the right to privacy and the obligation to protect data from unauthorized access. That being said, under a conservative approach, an organization may decide to obtain consent from a data subject before collecting, using, or disclosing personal data for a purpose in order to completely minimize future risks. Organizations should allow an individual who previously gave consent to withdraw his / her consent.
2. Purpose Limitation Obligation: Collect, use, or disclose personal data about an individual only for purposes that are reasonable and that have been disclosed / notified to the individual concerned.
3. Disclosure / Notification Obligation: Disclose to or notify the individual of the purpose(s) for which the organization intends to collect, use or disclose the individual’s personal data on or before such collection, use or disclosure of the personal data. The purposes notified must be reasonable.
4. Correction Obligation: Correct any incorrect or inaccurate personal data of a data subject that is in the possession or under the control of the organization upon request of the data subject.
5. Access Obligation: Allow data subjects to access their personal data in the possession or under the control of an organization for correcting the information under the Correction Obligation.
6. Protection Obligation: Protect personal data in its possession or under its control by taking necessary measures to prevent loss, unauthorized access, use, alteration, leak, disclosure, or otherwise.
7. Retention Obligation: Retain all personal data that is in its system, and that may give rise to civil and criminal liability.

The Draft Law on Personal Data Protection also supports these general principles and stipulates that the principles of personal data protection include:

- lawfulness, fairness, and transparency;
- purpose limitation;
- accuracy of personal data;
- retention limitation;
- security safeguards; and
- accountability.

TRANSFER

While Cambodia does not have comprehensive data protection legislation that explicitly prohibits an organization from transferring data, there is a general recognition of the protection of the right to privacy and the obligation to protect data from unauthorized access under the Civil Code and several pieces of legislation, although none of them imposes or implies any restrictions on the transfer of data. Therefore, personal data should only be collected, used, or disclosed for purposes that the individual understands and has given consent to at the time of giving initial consent or a new consent. Such purposes should be disclosed or notified to data subjects in a reasonable manner based on the circumstances.

Where the use and disclosure of the personal data is for a purpose different from that for which it was initially collected, it is recommended to notify the individual of the new purpose and obtain a new consent unless:

- the new purpose is within the scope of the original consent; or
- implied consent can be established.

Implied consent refers to any act that is generally recognized as consent under applicable trade practices. However, it is recommended that a new consent that is express and written be obtained once service providers use or disclose personal data for a purpose different from that for which it was collected.

When a service provider is seeking consent from the data subject, the service provider should disclose or notify the data subjects of the purpose(s) for which it intends to collect, use or disclose the data subjects' personal data before such collection, use or disclosure of the personal data. Cambodia's laws related to data protection do not prescribe how an organization should notify individuals. Organizations must determine what would be the most appropriate form of notification. The form of the disclosure / notification to obtain each data subject's consent should be as close to a formal contract as possible. Moreover, requirements such as clicking on the consent button, typing a full legal name for the signature, and / or scrolling through all terms of the disclosure / notification should be implemented. Furthermore, disclosures / notifications to the individuals regarding the purpose of the collection, use, and disclosure of personal data must not be too vague or broad in scope; an appropriate level of specificity should be provided.

In addition to laws of general application, the Draft Law on Personal Data Protection specifically mandates the requirement of consent for the collection, use, or disclosure of personal data. Furthermore, consent for the collection, use, or disclosure of personal data is only considered valid if the data controller provides notification to the data subject and the data subject gives their consent for that specific purpose.

Therefore, where the organization will be disclosing or transferring personal data to third parties, the organization should notify the individuals of such disclosure or transfer. Any consent provided by the individual without first being disclosed or notified of the purposes would not be valid.

SECURITY

Article 32 of the E-Commerce Law directly addresses matters of data protection in the course of electronic communication.

Service providers that electronically store consumers’ private information must take all reasonable security measures to avoid loss, modification, leakage, and / or unauthorized disclosure of all consumer data. The E-Commerce Law notes, however, that disclosures are allowable with the consent of authorities, or with the consent of the individual whose data is being disclosed. The E-Commerce Law does not provide specific guidelines as to how or what mechanisms are required. It is simply required that any measures could be used as long as they could reasonably protect the data from loss, or unauthorized access, use, alteration, or disclosure without authorization or illegally.

The E-Commerce Law also prohibits any encryption of data that may be used as evidence for any accusation or offence. This obligation potentially allows governmental authorities to order the decryption of data implicated in an investigation.

The E-Commerce Law also makes a blanket prohibition on certain forms of cybercrime, including interference with any electronic system for the purpose of accessing, downloading, copying, extracting, leaking, deleting, or otherwise modifying any stored data in bad faith or without authorized permission.

Article 47 of the Banking Law prohibits those who participate 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 of which they might have become aware through their functions. However, this professional secrecy obligation cannot be used as a ground for nondisclosure in relation to requests by supervisory authorities, auditors, provisional administrators, liquidators, or a court dealing with criminal proceedings.

In case the service provider is not under the scope of the E-Commerce Law or Banking Law, the obligations under the laws of general application that require protection of the right to privacy and the obligation to protect data from unauthorized access should apply when a service provider collects, uses, discloses and processes data of the subject.

Furthermore, the Draft Law on Personal Data Protection requires the data controller to protect personal data under its possession or control by setting up a security system to prevent unauthorised access, collection, use disclosure, copying, modification or disposal, or similar risks; and the loss of any storage medium or device on which personal data is stored. The data processor must also take security measures to prevent loss or unauthorised or unlawful access, use, modification, or disclosure of personal data.

BREACH NOTIFICATION

Currently, there is no breach notification requirement under Cambodian law. However, it is anticipated that the requirement for data controllers and data processors to notify the competent authority and the affected data subjects will be enforced once the Draft Law on Personal Data Protection comes into effect.

ENFORCEMENT

Since there are no regulatory or enforcement authorities that are specifically tasked with handling, overseeing or implementing personal data protection matters in Cambodia, the enforcement of the data protection would generally fall under the auspice of authorities across various sectors:

- the Ministry of Commerce;
- the Ministry of Post and Telecommunications; and
- the Ministry of Interior.

ELECTRONIC MARKETING

Since Cambodia does not have any dedicated laws on data protection, there are no special requirements when obtaining consent for marketing purposes. The E-commerce Law suggests that it is not necessary to obtain consent from the individual to send marketing communications as long as each marketing communication has clear and straightforward opt-out instructions and the individual has not previously exercised his / her opt-out right. Electronic marketing in Cambodia is subject to the general laws relating to digital marketing issues including:

- Law on Consumer Protection, which prohibits "unfair practices" in relation to consumer transactions. Unfair practices include unfair sales; bait advertising; unfair solicitation sales; demanding or accepting payments without intention to supply goods or services per the purchase order; making a false claim or representation of some business activity; coercion by force and mental threats; pyramid schemes; selling goods bearing a false trade description; and any other unfair practices.
- Law Concerning Marks, Tradenames and Acts of Unfair Competition, is relevant to comparative advertising. The following acts are considered acts of unfair competition: all acts that create confusion with the establishment, the goods, or the industrial, commercial or service activities of a competitor; false allegations in the course of trade of such a nature as to discredit the establishment, the goods, or the industrial, commercial or service activities of a competitor; and indications or allegations of the use of marks which, in the course of trade, misleads the public as to the nature, manufacturing process, characteristics, suitability for their purpose, or quantity of the goods.
- Telecommunications Law, which prohibits all activities against the principles of fair, free, equal, and effective competition.
- Other regulations on the Management of Advertisement on Website, Social Network, Mass Media and Mobile Phone Operators.

ONLINE PRIVACY

As mentioned under the Collection and Processing and Transfer sections, under a conservative approach, personal data should only be collected, used, or disclosed for purposes that the individual understands and has given consent to at the time of giving

initial consent or a new consent. Such purposes should be disclosed or notified to data subjects in a reasonable manner based on the circumstances. That said, to minimize future risks, any personal data, including location data, should only be collected and shared online through website cookies after the organization obtains consent from the data subject.

For obtaining consent from the data subject, please refer to the Transfer section.

KEY CONTACTS

Jay Cohen
Partner and Director of Cambodian Office
Tilleke & Gibbins (Cambodia) Ltd
T (+855) 17 87 57 238
jay.c@tilleke.com

Sochanmalisphoung Vannavuth
Associate
Tilleke & Gibbins (Cambodia) Ltd
T (+855) 10 61 65 91
sochanmalisphoung.v@tilleke.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.