DATA PROTECTION LAWS OF THE WORLD

Laos

LAOS

Last modified 28 December 2022

LAW

In Laos, the comprehensive regulatory framework on data privacy focuses on data in its digital form – electronic data – and none other.

From 2012, Laos has introduced this framework by circulating relevant information only. This trend has accelerated since 2015 with the publication of the Law on Cyber Crime. Issues pertaining specifically to the protection of electronic data are regulated by the Law on Electronic Data Protection and the subsequent Instructions on the Implementation of the Law on Electronic Data Protection, as follows:

- Law on Electronic Transactions (2012)
- Law on Cyber Crime (2015)
- Decision on the Penalties of the Law on Cyber Crime (2017)
- Law on Electronic Data Protection (2017)
- Penal Code (2017)
- Instructions on the Implementation of the Law on Cyber Crime (2018)
- Instructions on the Implementation of the Law on Electronic Data Protection (2018)

In addition, for both professionals or non-professionals, the authorities have provided a series of guidelines of best practices for the use of software and hardware, social media platforms, and better protection of electronic data.

The two main pieces of regulation relating to data privacy are the Law on Electronic Data Protection and the Instructions on the Implementation of the Law on Electronic Data Protection.

DEFINITIONS

Definition of Personal Data

Article 3, Section 12 of the Law on Electronic Data Protection defines "personal data" to mean electronic data of an individual, legal entity, or organization.

Definition of Sensitive Personal Data

The Law on Electronic Data Protection aims to protect any type of electronic data. The law categorizes electronic data roughly into three types: (i) general data, (ii) sensitive data (a literal translation would be "specific data"), and (iii) prohibited data. Depending on its nature, personal data may fall under one these three categories. Accordingly, there is no "sensitive personal data" so to speak. Given this, personal data may fall under the category of sensitive data.

Sensitive data is information "that an individual, legal entity, or organization cannot access, use, or disclose if [they] have not received consent from the Information Owner, or the relevant organization" (Article 10).

A list of examples of sensitive data is provided in the Instructions on the Implementation of the Law on Electronic Data (2018), which includes "information on customers, financial information, CV, history of medical treatment, race, religion, project plan, budget plan, official servant secret, etc." (Section 3). The list is not exhaustive, and there is no official guidance to anticipate what other data may be considered sensitive data apart from these examples.

NATIONAL DATA PROTECTION AUTHORITY

The Law on Electronic Data Protection (2017) originally delegated the Ministry of Post and Telecommunications (MPT) to handle matters related to the protection of electronic data. The MPT has now been renamed Ministry of Technology and Communication (MTC) and is the main administration in charge of issues pertaining to electronic data privacy across the country. The MTC is assisted by its departments located in each of the 17 provinces that compose Laos.

In its tasks to analyze and respond to digital issues and threats, the MPT was originally assisted by the Lao Computer Emergency Response Team (LaoCERT), which was established in 2012. LaoCERT no longer exists and was replaced by the Department of Cyber Security under the direct supervision of the MPT and is the agency on the front lines that receives reporting of security breaches from individuals or legal entities operating in Laos and/or complaints of offenses committed online.

REGISTRATION

There is no registration required for Data Protection Officers in Laos, or for any legal entities or individuals with a national data protection authority, as the case may be in other jurisdictions.

DATA PROTECTION OFFICERS

Under the Law on Electronic Data Protection, there is no data protection officer so to speak. The law introduces the idea that a team or an employee is required to supervise the protection of sensitive data; no information is provided on the duties and rights of such team or employee, or their scope of work. Moreover, the team or employee in charge of the protection of sensitive data is not required to register with any authority.

COLLECTION & PROCESSING

The collection of information is defined under the Instructions on the Implementation of the Law on Electronic Data Protection as "*the compiling of information in a database...for the convenience of access, monitoring, and use...*".

The Law on Electronic Data Protection speaks literally of "administration" of data. Administration of electronic data refers to the management and arrangement of data, which includes the collection, copying, submission, receipt, maintenance, and destruction of electronic data. This administration of data is carried out by the Data Administrator, which is defined as an "individual, legal entity, or organization which has the duty to administrate electronic data, such as: a Ministry, an Internet Data Center, a Telecommunications Service Provider, an Internet Service Provider, or a Bank." Apart from this definition, and the examples provided in the law, the Lao regulatory framework does not provide official guidance on who may or may not fall under the definition of Data Administrator.

By law, all data, general or sensitive, requires consent from the Information Owner to be collected. However, there is noinformation on how this consent may be collected.

Information Owner is defined as the individual, legal entity, or organization who / which is the owner of the electronic data. In this regard, the law does not necessarily identify the Information Owner as an individual only, or an individual who may be identified according to personal data that relates to him / her. The law only provides that the Information Owner is the entity that "owns" the information.

Sensitive data is more regulated as it requires the approval from the Information Owner for the access, use, and disclosure of sensitive data. At the time of the collection, the Information Owner must be informed of:

- the identity of the Data Administrator;
- the purpose of the collection of the information;

- the type of information that will be collected;
- the rights of the Information Owner, which include:
    - the right to amend the information provided;
    - the right to stop the sending or transfer of information to third parties;
    - the right to delete the information collected per request, or at the time that the purpose of the collection of the information expires.

Also, the Data Administrator and the Information Owner have the duty to ensure that the information provided is correct – it does not contravene local regulations, and does not affect the country's socio-economic development, national stability, or social order.

TRANSFER

The Law on Electronic Data Protection provides that the transfer of data must abide by the following requirements:

- the Information Owner has given its consent for the transfer of the electronic data, and the individual or legal entity;
- transferring the electronic data ensures that the receiving entity can protect the electronic data properly;
- documents concerning important information, such as financial, banking, investment, and accounting information, must be encrypted;
- information which is transferred or submitted must not be distorted;
- the transfer must be in line with the agreement between the sender and the recipient; and
- submission or transfer of data must be stopped when the receiver of the data does not intend to receive the information anymore.

The law does not address whether the requirements above should be applied to all individuals or entities, or only to the Data Administrator.

In addition, the Law on Electronic Data Protection emphasizes that any individual, legal entity, or organization contemplating sending or transferring personal data or official data (pertaining to governmental bodies) out of Laos must obtain the consent of the Data Administrator, and ensure that such submission or transfer does not contravene the Lao laws without further details.

SECURITY

Generally, the Law on Electronic Data Protection requires the Data Administrator to ensure the following regarding the storage / maintenance of electronic data:

- there is a team or employee responsible for the administration of sensitive data;
- there is, among other things, an adequate system to store or use the data, and a data safeguard system to protect the data;
- there is a backup system for destroyed or deleted data;
- information is recorded by way of another appropriate method (e.g. paper, magnetic storage), and the appropriate measure is used to guarantee good maintenance;
- a risk assessment is conducted on the protection system at least once a year, and any failures uncovered during the inspection are corrected;
- access to the system is inspected, and protected from any intrusion, virus, or other risks;
- any adverse events that have occurred or are about to occur are immediately solved; and
- the information that is under the responsibility of the Data Administrator is protected.

BREACH NOTIFICATION

There is no mandatory breach notification in Laos under the Law on Electronic Data Protection. Individuals and legal entities facing a breach may make a notification, but to seek assistance and recommendations on how to solve the breach, and not for the sake of transparency.

However, in 2020, the Bank of Lao PDR issued the Decree on Consumer Protection Concerning Financial Services. Like the Law

on Commercial Banks, enacted in 2018, the decree reiterates the importance of financial service providers (e.g. commercial banks) protecting their customer's confidential information. However, unlike the Law on Commercial Banks, the Decree does mention a duty to maintain the confidentiality of "personal information".

The Decree provides that in the event that information relating to customers is breached, the financial service provider has an obligation to record the incident and immediately notify the affected customers. No details are provided on what specifically must be recorded or notified. Likewise, the language used in the original document does not provide any assistance in interpreting the meaning of the term "affected." The term for "affected" that is used in the Lao language version of the Decree is a term that is normally used to denote persons who have suffered negative consequences or damage from an act. In the event that the breach of information causes an important adverse impact, or if there is a large-scale breach, a report must be submitted to the Bank of Lao PDR. However, there is no definition of "important adverse impact" or "large scale breach." Moreover, no specific sanction is provided for failing to submit the report.

The Law on Electronic Data Protection does not provide sanction for breach of the notification obligation. On the other hand, the Penal Code provides that any person disclosing the private confidential information of another person during the performance of their profession or duties, and who causes damages to the other person, will be liable to imprisonment of a term of three to six months and a fine between LAK 3 million (approx. USD 175) and LAK 10 million (approx. USD 580). However, Penal Code does not define "private confidential information", nor does it state whether the disclosure of information must be intentional. To date, there is no official guidance clarifying whether the Penal Code applies to scenarios where customer data is breached as a result of a technical failure or other such incidents.

ENFORCEMENT

The enforcing authorities with regard to electronic data protection are:

- Ministry of Technology and Communications (MTC);
- Economic Police; and
- Lao People's Court.

The Department of Cyber Security does not have by law the authority to issue fine or sanctions.

ELECTRONIC MARKETING

The Decision on Protection of Consumers Using Telecommunications and Internet Services (2020) regulates unsolicited commercial communications (e.g. phone calls or messages) to consumers, with the following restrictions:

- such calls and messages are prohibited from 8:00 to 17:00, Monday to Friday
- no more than 10 unsolicited commercial communications are allowed per month, per individual
- no more than two unsolicited commercial communications are allowed per day

The decision provides that any individual or legal entity intending to use unsolicited commercial communications for their goods or services must receive the consent of the telecommunications or internet service provider of the prospects they plan to call. The decision does not offer guidance on how the relevant service provider's consent may be obtained. Rather, the decision requires the telecommunications and internet service providers to ensure that unsolicited communication commercials are made by authorized persons. In addition, the decision delegates these providers to monitor the distribution of unsolicited commercial messages, thereby ensuring that these limits are not breached.

Consumers who receive unsolicited commercial communications can file a complaint with the MPT and resolve subsequent disputes with the relevant service provider. The decision also notes that consumers can voice complaints or seek guidance via one of the following official hotlines:

- 1510 – Ministry of Industry and Commerce
- 1516 – Prime Minister's Office
- 156 – National Assembly

The Ministry of Industry and Commerce's website is also expected to become an available channel for complaints in the future.

ONLINE PRIVACY

As provided, the collection of data must receive the consent of the relevant Information Owner.

On the other hand, based on the main laws and regulations above, it is difficult to anticipate the category of data cookies and location data according to the ambiguous definitions of general data, sensitive data, and personal data.

KEY CONTACTS

Dino Santaniello
Head of Office
Tilleke & Gibbins Lao Co., Ltd
T +856 21 262 355
dino.s@tilleke.com

Saithong Rattana
Attorney-at-Law
Tilleke & Gibbins Lao Co., Ltd
T +856 21 262 355
saithong.r@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.