

November 2022

1. Governing Texts

Data protection legislation in Lao People's Democratic Republic ('Lao PDR') mainly refers to the protection of data in the electronic format, which can be found in the Law on Electronic Data Protection No. 25/NA dated 12 May 2017) (only available in Lao [here](#)) ('the Law'), Law on Resistance and Prevention of Cybercrime No. 61/NA dated 15 July 2015 ('the Cybercrime Law'), Penal Code No. 26/NA dated 17 May 2017 (only available in Lao [here](#)) ('the Penal Code'), and other general legislation.

1.1. Key acts, regulations, directives, bills

The legislation related to data protection are as follows:

- the Law, which governs the collection, accessibility, use, and disclosure of electronic data, protection measures, rights, and obligations of data subject and data controller;
- the Cybercrime Law, which regulates rules and measures for database system, computer system data, and server system protection;
- the Penal Code, which sets out the punishable offence and its corresponding penalties and fines for offences related to data protection;
- Law on Telecommunications No. 09/NA dated 21 December 2011 (only available in Lao [here](#)), among others, prohibits telecommunication service providers from disclosing State or governmental classified information and telecommunications consumers' confidential matters;
- Law on Commercial Bank No. 56/NA dated 7 December 2018 (only available in Lao [here](#)), among others, prohibits commercial banks from disclosing customer's data without their permission;

- Law on Electronic Transactions No. 20/NA dated 7 December 2012 ('the Law on Electronic Transactions') provides the prohibition not to disclose consumer's data, digital signature, or electronic signature certificate;
- Decision on the Penalties in Cybercrime No. 3624/MPT dated 11 December 2017, which sets out fine measures for offenders that delete computer data without permission or provide inaccurate computer data to authorities;
- Instruction on Maintaining Safety of Computer System No. 3623/MPT dated 11 December 2017, which clarifies specific measures for maintaining the safety of computer system;
- Instruction on the Implementation of the Law on Electronic Data Protection No. 2126/MPT dated 8 August 2018 ('Instruction 2126'), which clarifies and provides details on some provisions of the law;
- Instruction on the Implementation of the Law on Cybercrime No. 2543/MPT dated 24 September 2018, which clarifies and provides details on some provisions of the law; and
- Instruction on the Use of Social Media No. 1561/MTC dated 26 August 2020.

1.2. Guidelines

The Ministry of Technology and Communications ('MTC') is directly responsible for issuing guidance related to electronic data protection and cybercrime.

The Lao Computer Emergency Response Team ('Lao CERT'), established under the direct supervision of MTC, is responsible for receiving reports of security breaches and complaints of offences committed online by individuals and legal entities operating in Lao PDR.

1.3. Case law

Not applicable.

2. Scope of Application

2.1. Personal scope

The Law and the Cybercrime Law are applicable to individuals, legal entities, and organisations, both domestic and international.

2.2. Territorial scope

The Law and the Cybercrime Law are applicable within Lao PDR. It is important to note that these laws may be applicable to foreign entities without physical presence in Lao PDR, but who engage in activities that are subject to the application of its provisions.

2.3. Material scope

The Law divides electronic data into:

General data: General data is defined as data which may be accessed, used, and disclosed upon correct identification of the source by the relevant controller or processor. Instruction 2126 provides a non-exhaustive list of general data which includes name, position, address, telephone number, email address, incorporation details, general statistic, and academic publications.

Specific/private data: Specific data is broadly identified as data that must not be accessed, used, and disclosed unless with permission of relevant data subjects. The example of private data provided under Instruction 2126 includes customer information, financial information, personal background, health information, nationality, religion, project plan, budget plan, and governmental classified information.

In addition, specific data splits into two types, government data and personal data. Lao law does not differentiate between personal data and sensitive data.

Data processing activities include the following:

- data collection;
- electronic data verification;
- deposit of electronic data;

- electronic data storage;
 - use and disclosure of electronic data;
 - delivery and transfer of electronic data;
 - access to electronic data;
 - improvement and amendment of electronic data; and
 - deletion of electronic data.
-

3. Data Protection Authority | Regulatory Authority

3.1. Main regulator for data protection

The MTC is the supervisory authority for electronic data protection and cybercrime, but also coordinates with Ministry of National Defence, Ministry of Public Security, and other concerned authorities.

3.2. Main powers, duties and responsibilities

To protect the electronic data, the MTC has the following rights and duties:

- review and create policies, strategic plans, laws, and regulations related to electronic protection to propose to the government for consideration;
- amplify policy, strategic plans, and laws to work plans and projects related to electronic data protection and implement such plans;
- promote, disseminate, and educate on the laws and regulations related to electronic data protection throughout the nation;
- supervise, manage, follow up, and inspect the services as to the laws and regulations related to electronic data protection and their implementation;
- review, create, and use technical standards for data security;
- manage the national electronic security code approval system;
- inspect the gaps in data system security;
- create, improve, and develop human resources in the electronic data protection field;
- consider and resolve requests related to electronic data protection;
- coordinate with other ministries concerned with electronic data protection;

- collaborate and cooperate with other countries on electronic data protection matters;
 - summarise and report the electronic data protection work operations to the government regularly; and
 - use other rights and perform other duties as defined by law.
-

4. Key Definitions

Data controller: Refers to individuals, legal entities, or organisations that are responsible for managing electronic data, such as ministry, internet data centre, telecommunication service provider, internet service provider, and banking.

Data processor: Lao law does not differentiate between data controller and data processor.

Personal data: Refers to data that relates to, or identifies the character, appearance, or performance of individuals, legal entities, or organisations in a direct or indirect way¹.

Sensitive data: The law does not define sensitive data. We are of the opinion that this may refer to specific data as discussed in section on material scope.

Health data: Not applicable.

Biometric data: Not applicable.

Pseudonymisation: Not applicable.

5. Legal Bases

5.1. Consent

For the data processing activities outlined in section on material scope above, the data controller must have a data subject's consent in order to access, use, disclose, provide, update, terminate, edit, or delete electronic data.

5.2. Contract with the data subject

Not applicable.

5.3. Legal obligations

Not applicable.

5.4. Interests of the data subject

Not applicable.

5.5. Public interest

Not applicable.

5.6. Legitimate interests of the data controller

Not applicable.

5.7. Legal bases in other instances

Please refer to previous discussions under sections consent to legal obligations.

6. Principles

Electronic data protection must be handled in accordance with the following principles:

- compliance with policy, laws, strategic plans, and the national socio-economic development plan;
- ensuring national stability, security, and social order;
- ensuring confidential and safety for government, individual, legal entity, or organisation data;
- ensuring the rights and interests of the data subject; and

- compliance to treaties and international agreements which the Lao PDR is a party to.
-

7. Controller and Processor Obligations

Data controllers have the following obligations:

- secure specific data of the data subject, for government data they must have the maintenance and administration system in accordance with the level of data security as specified in the Law;
- accessing, using, disclosing, providing, updating, terminating, editing, or deleting the electronic data on the request of data subject;
- responsibility for data that has been damaged;
- provide information to relevant officers for finding offenders;
- administrate the maintenance system and equipment for storing electronic data;
- ensure the access, use, disclosure, sending, and transfer of electronic data without effecting the stability of the nation and the orderliness of society;
- create and update the database system, database backup system, secured system, automatic data searching system, data restoring system, among others;
- coordinate with post and telecommunication sectors regarding security from data attacks;
- ensure measures on resolution of technical problems;
- research and use information technology to approach the social demand; and
- comply with other obligations as specified in Lao PDR law.

7.1. Data processing notification

There are no registration requirements for data processing.

7.2. Data transfers

The Law specifies that the delivery or transfer of data must be performed as follows:

- with the consent of the data subject and guarantee that the transferee can protect such data;

- with the encryption of important information, such as financial, accounting, and investment data;
- without forging the source of data sent or transferred;
- that the transfer must be in accordance with the agreement of the transferee and transferor; and
- that the transfer must be stopped upon refusal by transferee.

The transfer of private data outside of Lao PDR is subject to the express consent of data subject and compliance with law. There is no specific form in which consent must be given under the Law and other relevant regulations.

7.3. Data processing records

There is no expressed provision that requires data controllers to maintain data processing records.

7.4. Data protection impact assessment

There is no requirement for data controllers to carry out a Data Protection Impact Assessment.

7.5. Data protection officer appointment

There is a general obligation for a data processor or controller to maintain staff for data security administration under the Law. The Law does not explicitly state the requirements of a data protection officer ('DPO') for administrators, Article 46 of the Law references a DPO as a requirement for inspection of data protection compliance. Article 46 of the Law provides that a DPO's responsibilities, behaviour, and working methodologies are to be inspected for establishing compliance with the Law, however, there is no clarification or expansion to what that role and its responsibilities entail.

7.6. Data breach notification

The Law requires the data controller to coordinate with relevant authority when there is a cyber attack. In the event that the problem cannot be resolved, the data controller must propose to the Lao CERT. The Law does not specify the timeframe for such

notification.

7.7. Data retention

The Law provides that a data controller can retain electronic data for the necessary period for the collection purpose or other purposes. Thereafter, personal data may be deleted or inaccessible, except otherwise specified in the Law.

The data controller must delete electronic data that is collected as requested by the data subject or after the objective/purpose is terminated or the collection period has expired. They must also delete electronic data which relates to national stability, security, or social order, or data that is defamatory to other persons, as requested by authority or concerned person.

Deletion of electronic data must be notified to the data subject, except as otherwise specified in the Law.

7.8. Children's data

There are not any specific provisions in Law that regulates the processing of children's data. However, the Penal Code penalises disclosure of a child's private identity:

Any person who reveals the identity or personal information of a child (under 18 years old) victim, suspect, accused, defendant, or convicted person must be sentenced to imprisonment for a term ranging from three months to one year of imprisonment or re-educated without deprivation of liberty and a fine shall be imposed ranging from LAK 3 million (approx. €164) to KIP 10 million (approx. €547).

7.9. Special categories of personal data

Lao law does not differentiate categories of personal data.

7.10. Controller and processor contracts

There is a general requirement for a contract to be in place between a controller and processor to govern the relevant transaction of the parties. There are no particular matters that must be included other than the general requirements for a contract's execution.

8. Data Subject Rights

8.1. Right to be informed

The data controller must inform the data subject of the purpose, description of data collection, controller authority, and the data subject's right. In the event that the data controller fails to perform as request by the data subject due to technical or other factors, the data controller also has to inform the data subject of the same.

8.2. Right to access

The data subject has the right to access the data to amend, modify, or delete it when the data subject has requested this to the data controller. The data controller shall specify security standards for access to data by the data subject. The data subject also has the right to access its electronic data security code.

8.3. Right to rectification

The data subject has the right to create, access, use, disclose, provide, update, terminate, delete, and input the electronic data security code, as well as the right to access the data to amend, modify, or delete such data when the data subject has requested this to the data controller.

8.4. Right to erasure

The data subject has the right to delete the electronic data security code.

8.5. Right to object/opt-out

The data has the right to request to data controller to stop delivery or transfer their data to third party.

8.6. Right to data portability

Lao Law does not provide the right to data portability.

8.7. Right not to be subject to automated decision-making

Lao legislation does not provide the right to not to be subject to automated decision-making.

8.8. Other rights

The following are the other rights of data subjects:

- propose to the data controller and other relevant sectors to access, use, disclose, provide, update, terminate, or delete their data;
- inform the data controller and other relevant sectors to secure their electronic data when the data has been damaged or is at risk;
- complain to the relevant organisations when receiving no benefit from electronic data protection; and
- use other rights as specified in Lao PDR law.

9. Penalties

The violation of the provisions of the Law, especially collection, processing, and transfer of data without required consent, is considered a punishable offence consisting of civil, criminal, and administrative penalties, consisting of:

- warning and re-education;
- disciplinary action in case of offences committed by government officials;
- fines of LAK 15 million (approx. €821) in case of engagement in a prohibited action which does not constitute criminal offence;
- potential civil liability for incurred damage; and
- the application of criminal sanctions based on the seriousness of the wrongful act.

9.1 Enforcement decisions

Enforcement decisions are not publicly available.