



**Official Website
Lao Services
Portal**



Register (</index.php?r=site/register>) | Login

(</index.php?r=site%2Flogin>)

[Home \(/index.php\)](/index.php) >> [Search Legal Documents \(/index.php?r=site%2Fsearchlegal\)](/index.php?r=site%2Fsearchlegal) >> [View](#)

Legal

Document

Title: Law on Electronic Data Protection 25/NA, Date 12 May 2017

Type: Law

Responsible Agency: Ministry of Posts and Telecommunications

Issuing Date: 2017-11-15

Click here to see the measures contained in this document

Lao people's Democratic Republic

Peace Independence Democracy Unity Prosperity

The President

No. 117/P

Vientiane Capital, Date 23rd June 2017

The Decree of the President

of the Lao People's Democratic Republic

On the Promulgation of the Law on Electronic Data Protection

- Pursuant to Chapter VI, Article 67, Section 1 Constitution of Lao People's Democratic Republic (Amendment 2015);
- Pursuant to the Resolution of the National Assembly, No. 012/NA, dated 12th May 2017.
- Pursuant to the Letter of Proposal by the Standing Committee of the National Assembly, No. 107/STC, dated 12th June 2017.

The President of the Lao People's Democratic Republic issues this Decree:

Article 1 The Law on Electronic Data Protection is hereby promulgated.

Article 2 This decree enters into force from the date of signature.

The President of Lao PDR

(Signature and Sealed)

Bounnhang Vorachith

Lao People's Democratic Republic
Peace Independence Democracy Unity Prosperity

National Assembly No. 012/NA

Vientiane Capital, Date 12th May 2017

**The Resolution of
The National Assembly
on the Certification of the Law on Electronic Data Protection**

Pursuant to Article 53, Section 1 of the Constitution of Lao People's Democratic Republic (Amendment 2015) and Article 11, Section 1 of the Law on the National Assembly (Amendment 2015).

After in-depth and broad Deliberation and Consideration of the content of the Law on Electronic Data Protection by the National Assembly in 3th Ordinary Session of its 8th Legislature, on 12th May 2017.

The National Assembly Agrees that:

Article 1 The Law on Electronic Data Protection is certified with majority vote.

Article 2 This Resolution enters into force from the date of signature.

The President of the National Assembly

(Signature and Sealed)

Pany Yathotou

Lao People's Democratic Republic

Peace Independence Democracy Unity Prosperity

The National Assembly

No. 25/NA

Vientiane Capital, Date 12th May 2017

**The Law on
Electronic Data Protection**

Chapter 1

General Provisions

Article 1 Purpose

The law on Electronic Data Protection defines the principles, regulations and measures regarding to the administration, monitoring, inspection and activation of Electronic Data Protection in order to ensure the collection, accessing, usage, and disclosing of data are safe and correct. It is also focused on the protection of rights and benefits of the state, individual, legal entities or organizations; and it aims to contribute in Socio-Economic Development of the nation, ensures the stability of the nation, peace and orderliness of the society.

Article 2 Electronic Data Protection

Electronic Data is digits, letters, motion- picture, non-motion picture, audio, video and others that keep in electronic form.

Electronic Data protection is the methods and measures to secure the data that have been administrated and stored in electronic form from accessing, using, disclosing, editing, sending, transferring and destroying without permission.

Article 3 Definitions

Terms used in this Law shall have the following meaning:

1. **Data** means the digits, letters or other symbols that can be processed by computer;
2. **Electronic** means things that relating to the technology by using electricity, digital, magnetic system, wireless system, fiber light, magnetic electric and other similarities;
3. **Database** means the systematically storage of data in electronic forms that can be managed, revised, and used;
4. **Data System** means the collection of hardware, software, and database that were created for creating, sending, receiving, managing, maintaining and exchanging of electronic data;
5. **Hardware** means physical parts or components of a computer and other electronic devices; such as the central processing unit, memory, monitor, keyboard, printer, phone, television;
6. **Software** means Command Set or Program that control the computer and other electronic devices for some specific operation;
7. **Computer System** means electronic devices or sets of computer that connect the operation system together by determining the command, Command Set or others, in order to process the data automatically in one or many computers that connect through computer network or internet.;
8. **Program** means the Command System or Command Set that the computer system can effectively operate as determined;
9. **Dangerous Program** means the program that cause some or all data systems work irregularly, copy, edit, or delete the data that stored in the data system; or send the data from one computer to another without permission;
10. **Data Owner** means individual, legal entities or organizations that own the electronic data;
11. **Official Data** means data or data technology that relating to the activation or administration of the government;
12. **Personal Data** means electronic data of individual, legal entities or organizations;
13. **Electronic Data Administration** means the administrative and management of data including saving, copying, sending, receiving, maintaining and destroying the electronic data.
14. **Electronic Data Administration Authorities** means individual, legal entities or organizations that responsible for administrating the electronic data which mainly are Ministries, Data Center through internet, telecommunication service providers, banks;
15. **Codification of Data Security** means codification by using digits, letters, symbols or other marks to secure unpermitted user to access or read that electronic data.
16. **Virus** means specific program that created for spreading, damaging and destroying computer system, computer network and computer data;
17. **Magnetic Recording** means the recording of signal such as audio, video or computer command system on magnetic surface such as gazette or dishes that covered by oxide;
18. **Computer Emergency Interception and Resolution Center** means an organization of the Ministry of Posts and Telecommunication which its roles to intercept and resolve computer emergency.

Article 4 Government Policies on Electronic Data Protection

The government considers Electronic Data Protection as one of the most important tasks in order to ensure

the use of data are in security and limit of taking individual, legal entities or organizations data to use and disclose in public without permission.

The government supports and promotes Electronic Data Protection by facilitating, providing budget, building infrastructure, human resource development, researching and using modern technology for efficient and effective performance.

The government supports and enhances domestic and international individual, legal entities or organizations to contribute and investment on Electronic Data Protection.

Article 5 Principles of Electronic Data Protection

Electronic Data Protection shall base on the following principles:

1. Consistent with policies, laws, strategy plans, National Socio-Economic Development Plan;
2. Ensure the stability of the nation, peace and orderliness of the society;
3. Keep the data of the state, individual, legal entities or organizations in confidential and security;
4. Ensure rights and benefits of data owner;
5. Consistent with international treaties and agreements that the Lao PDR is a party.

Article 6 Scope of Application

This law is applicable to domestic and international individuals, legal entities or organizations that located or activated within the territory of the Lao PDR.

Article 7 International Cooperation

The government promotes international relations and cooperation with foreign countries, regional and international on Electronic Data Protection by exchanging experience, information, and technology; upgrade knowledge and technical capacity for the effectiveness of the tasks, and shall comply with international treaties and agreements that the Lao PDR is a party.

Chapter 2

Types of Electronic Data

Article 8 Types of Electronic Data

There are two types of electronic data:

1. General data;
2. Specific data.

Article 9 General Data

General data is the data of individual, legal entities or organizations which able to access, use and disclose, and must indicate sources of data correctly.

Article 10 Specific Data

Specific data is the data that not allow individual, legal entities or organizations to access, use or disclose without permission from the owner or relevant organizations.

Specific data includes official data and personal data.

Data Security must be ranked in official data and the procedure of accessing, using and disclosing as specified in the Article 22 in this law.

Chapter 3

Electronic Data Protection Tasks

Article 11 Electronic Data Protection Tasks

Electronic Data Protection Tasks are as following:

1. Data collection;
2. Inspection of electronic data;
3. Depositing of electronic data;
4. Maintenance of electronic data;
5. Using or disclosing of electronic data;
6. Sending or transferring of electronic data;
7. Accessing of electronic data;
8. Updating or editing electronic data;
9. Deleting of electronic data.

Article 12 Data Collection

Individual, legal entities or organizations who would like to collect data must inform the purpose and detail of the data collection to the data owner, and data administration authorities.

The collection of data must be approved by data owner and must not dissimulate or use other methods that causing misunderstanding of propose and detail of data collection.

Article 13 Inspection of Electronic Data

Data owner and data administration authority must inspect and ensure the correction and completion of data in order to ensure that the content of data is not contradict with the laws and regulations, and shall not impact on the Socio-Economic Development, the stability of the nation, peace and orderliness of the society.

Article 14 Deposit of Electronic Data

Individual, legal entities or organizations are objective to deposit or backup the electronic data with data authority for its safety must perform as following:

1. Fill the information correctly and completely in accordance with the form or agreement that specified by the data authority;
2. In case of the electronic data is changing, the owner must inform the administration authority in order to update and edit the data correctly and completely; and
3. Comply with bilateral agreement.

Article 15 Maintenance of Electronic Data

Data administration authority can maintain electronic data when necessary from the collection purpose and other purposes. Following by the personal data may be deleted or blocked from accessing, except the law specified in others.

Data administration authority must create a list of electronic data maintenance which can be easily check and the maintenance measures and methods must be safe.

Data administration authority is able to handover electronic data to other authorities and shall be agreed from the data owner.

Article 16 Using and Disclosing of Electronic Data

Data administration authority can use or disclose personal data that they collected, maintained or administrated when have been approved by data owner, except the law specified in others.

Data administration authority cannot provide personal data that they collected, maintained or administrated to a third person if unapproved by data owner or have been proposed from the relevant authorized government organization as specify in the law.

Article 17 Sending or Transferring of Electronic Data

Sending or transferring of electronic data shall comply as following:

1. Have permission from the data owner and ensure the receiver is able to secure those data;
2. Input data security for the important data which mainly are financial, banking, investment and accounting data;
3. Do not falsify data sources that have been sent and transferred;
4. Consistent with the agreement between sender and receiver;
5. Stop sending or transferring data when the receiver denies.

Individual, legal entities or organizations cannot send or transfer personal data and official data outside the Lao PDR without permission from the data owner or if contradicts with the law.

Article 18 Accessing of Electronic Data

Individual, legal entities or organizations are objective to access the electronic data that not general data, and

must propose to the relevant data administration authority as specify in the Article 16 of this law for legal consideration.

Article 19 Updating or Editing of Electronic Data

Data owner can request to data administration authority for updating or editing the electronic data, or request to stop sending and transferring the data to a third person.

After receiving the request from the data owner, the data administration authority must:

1. Proceed in updating or editing data as requested by data owner, or provide methods to data owner in order to be able to update, editing or deleting the data by themselves;
2. Inform the data owner in case of unable to activate the request regarding to the technical problem or other factors.

Article 20 Deleting of Electronic Data

Data administration authority must delete electronic data that they collected as proposed by the data owner or when using purpose is terminated, the collection is expired or as specify in the Article 29 section 3 of this law. Deleting of electronic data must inform the data owner, except the law is specified in others.

Chapter 4

The Measures on Securing of Electronic Data

Article 21 The Measures on Securing of Electronic Data

Securing of electronic data, the data administration authority must comply with the following measures:

1. Ranking of the official data security;
2. Maintenance of electronic data;
3. Data accession security;
4. Codification of data security;
5. Responding to data attacks.

Article 22 Ranking of the Official Data Security

Ranking of the official data security are as following:

1. First Level when the data have been destroyed or disclosed that damages rights and benefits of state, individual, legal entities or organizations;
2. Second Level when the data have been destroyed or disclosed which causing serious damage the rights and benefits of state, individual, legal entities or organizations, or effect the benefit of the

community;

3. Third Level when the data have been destroyed or disclosed that damages the production, peace, social security and nation-public security.

Article 23 Maintenance of Electronic Data

The data administration authority shall maintain electronic data as follow:

1. Contain specific units or staffs that responsible for the administration of data security;
2. Create the collection system, data usage system, the administration of data security system and other relevant systems;
3. Use technical system to secure the data that suitable with the system size;
4. Recheck deleting and destroying of data;
5. Record data with paper, light, magnetic or other methods, and use the suitable processes for the maintenance;
6. Inspect and evaluate the risk of data system at least once a year and must fix the detected problem including update the data system to be secured;
7. Inspect the accessing of data storage system and secure from attacking, virus or other similar risks and others;
8. Immediately solve the incident that cause or may cause serious impact when receiving permission or investigation report from the administration of data security unit or other relevant units;
9. Secure the data that in his or her responsibility in order to avoid unpermitted person to access, use, disclose, copy, change or eradicate data.

Article 24 Security of Data Accession

Data administration authority must specify measures on data accession security for the accessible of data owner safely.

Data administration authority must facilitate the data owner for inspection, monitoring, using and searching of information must be quick, safe and up-to-date.

Data owner must be responsible for maintenance, changing and protection of his or her password for unusable of other persons.

Article 25 Codification of Data Security

Sending or transferring of important electronic data which mainly are financial, banking, investment, and accounting data via computer system. The data administration authority must use the data security code, and the electronic certificate that certified by the Ministry of Posts and Telecommunication in order to secure from unpermitted person in accessing, reading, destroying, using, disclosing, sending, transferring, editing, deleting, changing, and other acts that causing damage.

Article 26 Responding to Data Attacks

Responding to data attacks shall comply as following:

1. Data administration authority uses interception and fixed methods when have been informed by individual, legal entities or organizations that relating to sending of data that cause or may cause unpeaceful of the society;
2. Data administration authority coordinates with relevant sectors to collect attacked information and evidence such as date, time, location, form, and amount of attacks; the effect and source of attack for fixing. In case of unable to fix, shall inform the Computer Emergency Interception and Resolution Center, the Ministry of Posts and Telecommunication;
3. Computer Emergency Interception and Resolution Center coordinates with the Data Security Administration Unit of data administration authority and other relevant sectors both domestic and international in order to restrain and fix the incident on time.

Article 5

Rights and Obligations of the Data Owner

Article 27 Rights of the Data Owner

Data owners have the following rights:

1. Create, access, use, disclose, provide, update, terminate, delete, input the electronic data security code;
2. Propose to the data administration authority and other relevant sectors to access, use, disclose, provide, update, terminate, delete his or her data;
3. Inform data administration authority and other relevant sectors to secure his or her electronic data when the data have been damaged or in risk;
4. Complaint to the relevant organizations when receiving non-benefit from electronic data protection;
5. Use other rights as specified in the law.

Article 28: Obligations of the Data Owner

Data owners have the following obligations:

1. Inspect the content of electronic data before using or disclosing and must be responsible to the law and content of electronic data that created or responsible by data owner;
2. Ensure the correctness, clearness, and completeness of electronic data that provides to data administration authority;
3. Report the abnormal of electronic data to the data administration authority;
4. Report the illegal activation that relating to electronic data to the relevant organizations;
5. Comply with other obligations as specified in the law.

Chapter 6

Rights and Obligations of the Data Administration Authority

Article 29 Rights of the Data Administration Authority

Data Administration Authority has the following rights:

1. Intercept the creating, accessing, sending, receiving, using or disclosing electronic data that effect on the stability of the nation, peace and orderliness of the society;
2. Suspend the service of data owner who violates the agreement or has behavior that causing the damage to data administration authority, peace or orderliness of the society;
3. Delete the electronic data that relating to the stability of the nation, peace and orderliness of the society or the information that slander other persons as proposed by the officer or relevant person;
4. Create the inspection, monitoring and observation units for the security of data system;
5. Eradicate sources of dangerous program, virus, and others;
6. Comply with other rights as specified in the law.

Article 30 Obligations of data administration authority

Data administration authority has the following obligations:

1. Secure specific data of the owner, for the official data shall have the maintenance and administration system in accordance with the level of data security as specified in the Article 22 of this law;
2. Accessing, using, disclosing, providing, updating, terminating, editing, deleting the electronic from the request of data owner;
3. Responsible for the data that have been damaged;
4. Provide information to relevant officers for finding the offender;
5. Administrate the maintenance system and equipment of electronic data;
6. Ensure the accessing, using, disclosing, sending and transferring electronic data without effecting the stability of the nation and the orderliness of the society;
7. Create and update database system, database backup system, secured system, automatic data searching system, data restoring system and others to be ready;
8. Coordinate with Posts and Telecommunication Sectors regarding to secure form attacking data;
9. Ensure the measures regarding to the resolution of technical problems;
10. Research and use information technology to approach the social demand;
11. Comply with other obligations as specified in the law.

Article 7

Prohibition

Article 31 General Prohibition

Individual, legal entities or organizations are prohibited to act as follow:

1. Accessing, collecting, using, disclosing, destroying, blocking, editing, falsifying, providing electronic data that is the confidential of the state, individual, legal entities or organizations without permission;
2. Sending or transferring electronic data without permission from data owner;
3. Sending electronic data without sources, dangerous program, virus;
4. Creating the falsification of electronic data or dangerous data which causing the damage to others;
5. Use the gap or weakness of data system to access, collect, use and disclose the electronic data; and
6. Other acts that violate the law.

Article 32 Prohibition for the Data Owner

Data owners are prohibited to act as follow:

1. Interrupt in sending, interfering, destroying, deleting, editing and falsifying electronic data;
2. Attacking or other acts that cause the data security system is unable to operate;
3. Sending electronic data without sources, dangerous program, virus;
4. Creating the falsification of electronic data or dangerous data which causing the damage to individual, legal entities or other organizations;;
5. Use the gap or weakness of data system to access, collect, use and disclose the electronic data; and
6. Other acts that violate the law.

Article 33 Prohibition for the Data Administration Authority

Data administration authority are prohibited to act as follow:

1. Accessing, collecting, using, disclosing, or disseminating electronic data of the state, individual, legal entities or organizations without permission;
2. Accessing, collecting, using, disclosing, providing, editing, destroying electronic data without permission;
3. Collecting, using, disclosing electronic data that relating to race, ethnic, political attitude, religion belief, sexual behavior, criminal record, health or other data that effect on the stability of the nation, peace and orderliness of the society; and
4. Other acts that violate the law.

Chapter 8

Dispute Settlement

Article 34 Form of the Dispute Settlement

Dispute settlement can be conducted by one of the following forms:

1. Compromise settlement;
2. Administrative Settlement;
3. Settlement by Economic Dispute Settlement Organization;
4. File a complaint to People's courts;
5. Settlement with internationally features.

Article 35 Compromise Settlement

In case of causing any disputes regarding to electronic data the litigants can discuss and compromise together for the benefits of each parties.

Article 36 Administrative Settlement

In case if the dispute have been disagreed or cannot be mediated, the litigants can propose to the Administration of Electronic Data Protection for the resolution.

Article 37 Settlement by the Economic Dispute Settlement Organization

In case of causing any economic disputes regarding to Electronic Data Protection, the litigants can propose to the Economic Dispute Settlement Organization as specified in the Law on Economic Dispute Settlement.

Article 38 File a Complaint to People's Courts

In case of causing any disputes regarding to Electronic Data Protection, the litigants can file a complaint to People's Courts for judgment.

Article 39 Settlement with Internationally Features

In case of causing any disputes regarding to Electronic Data Protection with international features, shall comply with the relevant laws of Lao PDR, international treaties and agreements that the Lao PDR is a party.

Chapter 9

The Administration of Electronic Data Protection

Article 40 Administration Organization of Electronic Data Protection

The government is an administration center of Electronic Data Protection and unity throughout the country which the Ministry of Posts and Telecommunication is a key person in responsible and coordination with line ministries, Government Organizations equivalence to the ministry, Local Authorities, and other relevant sectors are implemented.

The Electronic Data Protection Administration Organizations comprise of:

1. Ministry of Posts and Telecommunication;
2. Provincial, and Capital Department of Posts and Telecommunication;
3. Posts and Telecommunication Office of District, Municipality, City.

Article 41 Rights and Duties of Ministry of Posts and Telecommunication

Regarding to the administration of Electronic Data Protection, the Ministry of Posts and Telecommunication has the following rights and duties:

1. Research, create policy, strategy plan, laws and regulations regarding to the Electronic Data Protection in order to propose to the government for consideration;
2. Develop policy, strategy plan, and laws to be a plan, scheme and project that relating to Electronic Data Protection and implement;
3. Advertise, disseminate, and educate laws and regulations that relating to Electronic Data Protection throughout the country;
4. Guide, administrate, monitor, and inspect the administration; implementation of Laws and regulations that relating to Electronic Data Protection;

5. Research, create, and use the technical standard of data security;
6. Administrate certification system of national electronic security code;
7. Inspect the gap regarding to data security system;
8. Create, upgrade, and develop human resource regarding to Electronic Data Protection;
9. Consider and solve the proposals that relating to electronic data;
10. Coordinate with line ministries that relating to electronic data protection;
11. Relate and coordinate with foreign countries, regional and international regarding to Electronic Data Protection;
12. Regularly summarize and report Electronic Data Protection activities to the government;
13. Apply other rights and duties as specified in the law.

Article 42 Rights and Duties of Provincial, Capital Department of Posts and Telecommunication

Regarding to the administration of the Electronic Data Protection, Provincial, Capital Department of Posts and Telecommunication have the following rights and duties:

1. Advertise, disseminate, educate, and develop policy, strategic plan, laws and regulations that relating to the Electronic Data Protection throughout the country;
2. Implement policy, strategy plan, laws, regulations, plans, schemes, project that relating to Electronic Data Protection;
3. Guide, administrate, monitor, and inspect the administration; implementation of Laws and regulations that relating to Electronic Data Protection;
4. Propose plan, upgrade, and develop human resource regarding to the Electronic Data Protection to the Ministry of Posts and Telecommunication;
5. Consider and solve the proposals that relating to electronic data;
6. Coordinate with relevant Departments that relating to electronic data protection;
7. Relate and coordinate with foreign countries, regional and international regarding to Electronic Data Protection as assigned by the supervisor;;
8. Regularly summarize and report the Electronic Data Protection activities to the Ministry of Posts and Telecommunication, and Provincial, Capital Authorities;
9. Apply other rights and duties as specified in the law.

Article 43 Rights and Duties of the Posts and Telecommunication Office of District, Municipality and City

Regarding to the administration of Electronic Data Protection, the Posts and Telecommunication Office of District, Municipality and City have the following rights and duties:

1. Advertise, disseminate, educate, and implement the policy, strategic plan, laws, regulations, plans, scheme, and project that relating to Electronic Data Protection throughout the country;
2. Monitor and inspect the administration; implementation of Laws and regulations that relating to the use of Electronic Data;
3. Propose plan, upgrade, and develop human resource regarding to the Electronic Data Protection to the supervisor;
4. Submit the proposals that relating to Electronic Data Protection, and other proposals to the Provincial, Capital Department of Posts and Telecommunication for consideration;

5. Collect the statistic of Electronic Data Protection;
6. Coordinate with other offices that relating to Electronic Data Protection;
7. Regularly summarize and report Electronic Data Protection activities to the Department of Posts and Telecommunication, and District, Municipality, and City Authorities;
8. Apply other rights and duties as specified in the law.

Article 44 Rights and Duties of other Sectors, Local Authorities and Components

Regarding to the administration of Electronic Data Protection; rights and duties of other sectors, local authorities, and components are to collaborate and coordinate with Posts and Telecommunication Sector in accordance with its scopes.

Chapter 10

Electronic Data Protection Inspection

Article 45 Organization of Electronic Data Protection Inspection

Organization of electronic data protection inspection comprises of:

1. Internal inspection organization;
2. External inspection organization.

Internal inspection organization is an administration organization of the Electronic Data Protection as specify in Article 40 of this law.

External inspection organization comprises of the National Assembly, the Provincial People's Assembly, State Audition Organization, State Inspection Organization, Lao National Front for Development, and Mass Organization.

Article 46 Inspection Content

The inspection of electronic data protection has the following contents:

1. The implementation of policy, strategy plan, law and regulation regarding to electronic data protection;
2. The organization and activation of electronic data protection sectors;
3. The responsibilities, behavior and working methodologies of Electronic Data Protection officers;
4. The activation of data owner;
5. The activation of data administration authority;
6. The implementation of international treaties and agreements that Lao PDR is a party.

Article 47 Forms of Inspection

There are three forms of electronic data protection Inspection;

1. Regular inspection;
2. Inspection with advance notice;

3. Immediate inspection.

Regular inspection is an inspection with exact time and plan.

Inspection with advance notice is a non-planned inspection with advance notification to the inspected person.

Immediate inspection is an urgent inspection without advance notification.

In conducting the inspection shall strictly comply with the law.

Chapter 11

Policies toward Persons with Outstanding Achievements and Measures against Violators

Article 48 Policies toward Persons with Outstanding Achievements

Individual, legal entities or organizations with outstanding achievement in implementing this law will receive reward or other policies in accordance with the law.

Article 49 Measures against Violator

Individual, legal entities or organizations that violate this law or other relevant laws will be educated, warned, disciplined, fined or penalized depending on the degree of violation.

Article 50 Re-educational Measures

Individual, legal entities or organizations that violate this law mainly are the prohibitions that specify in this law in minor manner will be re-educated or warned.

Article 51 Disciplinary Measures

Government officials, military, police that violate this law, mainly are the prohibitions that specify in this law which is not considered as criminal offence will be disciplined as specify in the relevant laws.

Article 52 Fining Measures

Individual, legal entities or organizations that violate this law mainly are the prohibitions that specify in Article 31, 32, and 33 which are not considered as criminal offence will be fined 15.000.000 Kip.

Article 53 Civil Measures

Individual, legal entities or organizations violate this law that causing the damage to other persons shall pay the compensation of the damage that has been occurred.

Article 54 Penal Measures

Individual who violates this law which is considered as criminal offence will be penalized as specified

in Criminal Law and other laws that specified criminal penalties depending on the degree of violation.

Chapter 12

Final Provision

Article 55 Implementation

The government of Lao People's Democratic Republic is implemented this law.

Article 56 Effectiveness

This law enters into force from the date of the issuance of the promulgating decree the President of the Lao People's Democratic Republic and fifteen days after this law is published in the Official Gazette.

Other regulations and provisions which contradict to this law are cancelled.

The President of the National Assembly

(Signature and Sealed)

Pany Yathotou

Download Lao:Law on Electronic Data Protection 25/NA, Date 12 May 2017 (/images/download/Announcement_Lao_2017111515112644.pdf)

List Measures Related to Legal Documents

Name (/index.php?r=site%2Fdisplaylegal&id=289&sort=name)	Description (/index.php?r=site%2Fdisplaylegal&id=289&sort=description)	Status (/index.php?r=site%2Fdisplaylegal&id=289&sort=status)
No results found.		

About Us (/index.php?r=site/content&id=31)| **Terms and Conditions** (/index.php?r=site/content&id=27)|
FAQs (/index.php?r=site/content&id=28)| **Links** (/index.php?r=site/content&id=29)| **Site Map**
(/index.php?r=site/content&id=30)| **Contact Us** (/index.php?r=site/contact)

Copyright ©2021, Foreign Trade Policy Department, Ministry of Industry and Commerce, Lao PDR.