ECCIL
EUROCHAM LAOS

WHITE PAPER

Electronic Data Protection and Personal Data

WHITE PAPER

Electronic Data Protection and Personal Data

Its contents are the sole responsibility of the European Chamber of Commerce and Industry in Lao PDR and do not necessarily reflect the views of the European Union.

This paper is provided for information only and not for publication or general circulation.

EUROCHAM LAOS Building
Nokeokoumane street, Anou Village,
P.O. Box 11781 Chanthabouly District, 1000
Phone: +856 21 264 330
Email: contact@eccil.org
www.eccil.org

Electronic Data Protection and Personal Data

1. Institutional Environment

In Laos, the regulatory framework on data privacy focuses mainly on electronic data, which can be defined as data that is stored electronically. The Law on Electronic Data Protection (2017) designated the Ministry of Post and Telecommunications — which has since been renamed the Ministry of Technology and Communications (**MTC**) — to handle matters related to the protection of electronic data. As the main government body responsible for issues pertaining to electronic data privacy, the MTC is assisted by its departments, located in each of the 17 provinces of Laos. The MTC supervised the drafting of the laws, instructions, and decisions mentioned below. In addition, the MTC has published a series of guidelines for professionals and individuals on best practices relating to the use of software and hardware, social media platforms, and the protection of electronic data.

In analyzing and responding to digital threats, the MTC is assisted by the Lao Computer Emergency Response Team (**LaoCERT**), which was established in 2012. LaoCERT, which is under the direct supervision of the MTC, is the frontline agency that receives reports of security breaches from individuals and legal entities operating in Laos, as well as complaints of offenses committed online.

2. Legal Framework

Laos began developing a comprehensive legal framework on electronic communication ahead of some of its neighbors in the region, showing that the authorities take the matter seriously and understand the importance of ensuring that growth in online activity is accompanied by adequate regulation. Over the past decade, Laos has developed a legal framework to address issues pertaining to online activities generally, as well as the use, transfer and protection of electronic data. One of the first pieces of legislation to address online transactions, activities, and the transfer of information was the Law on Electronic Transactions (2012), which was published in the Official Gazette in 2013. Attempts to develop a legal framework on electronic data, cybercrime, and data privacy, were accelerated from 2015 with the enactment of the Law on Cyber Crime (2015).

Today, the legal framework concerning electronic data is primarily based on the following instruments:

- Law on Electronic Transactions (2012)
- Decree on the Management of Information on the Internet (2014)
- Law on Cyber Crime (2015)
- Decision on the Penalties of the Law on Cyber Crime (2017)
- Law on Electronic Data Protection (2017)
- Instructions on Computer Systems Security (2017)
- Instructions on the Implementation of the Law on Cyber Crime (2018)
- Instructions on the Implementation of the Law on Electronic Data Protection (2018) (the **EDP Instructions**)
- Law on Electronic Signature (2018)
- Instructions on the Use of Social Media (2020)

The Law on Electronic Data Protection, and the subsequent EDP Instructions issued in 2018, form the main regulatory framework for the protection of electronic data and electronic data privacy. The Law on Electronic Data Protection regulates only electronic data and does not intend to touch upon other types of data (i.e., non-electronic data on hard copy). One of the key benefits of this law is that it creates a specific framework for electronic data, compared to other models that either do not cover electronic data at all or apply generic frameworks to online activities.

3. Observations on Personal Data and the Law on Electronic Data Protection

The Law on Electronic Data Protection aims to protect all types of electronic data.[1] The law categorizes electronic data into two broad groups: general data and sensitive data (a literal translation would be "specific data"). General data is that which can be accessed, used, or disseminated without the consent of the information owner, whereas consent is required for sensitive data. "Information owner" is the closest concept under Lao law to a data subject under the EU General Data Protection Regulation (GDPR). [2] The Law on Electronic Data also imposes further restrictions on the administration of sensitive data. The law relies on the EDP Instructions for practical examples of data that is general data or sensitive data (see 4.4 and 4.5 below).

In addition, a third category can be referred to as "prohibited data," which is data that cannot be administrated electronically. Unlike the other two groups, prohibited data is specifically defined as information on race; ethnicity; political opinion; religious beliefs; sexual behavior; criminal records; health, or any information that may affect the stability of the nation, public order, and the orderliness of society. Data administrators [3] are prohibited from electronically administrating this type of data (Article 33, Section 3).

While the definitions of general, sensitive, and prohibited data are not very precise (see further below), personal data will fall into one of the three categories, depending on its nature.

The Law on Electronic Data Protection does not include specific provisions about individual privacy or the protection of personal data pertaining to individuals. Rather, the law defines "personal data" broadly as the electronic data of individuals, legal entities and organizations. [4]

In the Law on Electronic Data Protection, administration of data is defined as the management and arrangement of data, which includes the collection, copying, submission, receipt, storage, and destruction of electronic data. The concept is broadly similar to the idea of data processing under the GDPR.

Laos' legislators have made efforts to provide rights and obligations for different categories of stakeholders and have sought to tailor these rights and obligations to each stakeholder depending on their level of involvement in the processing of electronic data, as is also the case under the GDPR. Howev-

[1] Article 2 of the Law on Electronic Data Protection: "Electronic data means a message made of number, letter, animated image, non-animated image, voice, video, etc. which is stored in its electronic form."

[2] Article 3, Section 10 of the Law on Electronic Data Protection: "individual, legal entity, and organization who/which is the owner of the electronic data."

[3] Article 3, Section 14 of the Law on Electronic Data Protection, Data Administrator means: "individual, legal entity, and organization, which as the duty to administrate electronic data, such as: a Ministry, an Internet Data Center, a Telecommunications Service Provider, an Internet Service Provider, a Bank."

[4] Article 3, Section 12, of the Law on Electronic Data Protection: "Personal Data means Electronic data of individual, legal entity, organization"

a result, individuals and legal entities may find it challenging to use electronic data for the purpose of business activities without infringing the law. This may continue to deter local and foreign investors from developing business practices that heavily rely on electronic data.

4. Comments on the Law on Electronic Data Protection

4.1. The definition of "information owner" is not sufficiently restrictive.

According to the Law on Electronic Data Protection, an information owner can be an "individual, legal entity, or organization who/which is the owner of the electronic data" (Article 3, Section 10). This definition is not satisfactory as it might capture a broader range of individuals than intended by the policymakers. This is because the term is not defined by reference to the person who can be identified by the data, but, rather, by reference to the person who "owns" the data.

To illustrate this problem, we might consider the example of a hotel operator who collects the personal information of a customer. Based on a strict interpretation of the law, the hotel operator could be an information owner since they are in possession of the information. This could create confusion as to which party benefits from the protections afforded to an information owner.

The legislators likely did not intend for the term "information owner" to be given such a broad interpretation. For this reason, the current definition must be clarified so that there is a clear distinction between an entity that collects and stores data (the hotel operator in the above example) and an individual who can be identified by that data (the customer in the above example).

4.2. The definition of "data administrator" is unclear and not sufficiently restrictive.

As noted above, the Law on Electronic Data Protection refers to data administrators, the closest concept under Lao law to data processors under the GDPR. The law defines a data administrator as "an individual, legal entity, and 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, a Bank" (Article 3, Section 14). The law places a range of obligations on data administrators. As such, it is important to be able to identify the entities that fall within this definition.

Under this definition, a data administrator is someone who has a "duty" to administrate electronic data. This term is not particularly clear, and it does not limit the definition to entities that administrate data on behalf of another party.

The use of "such as" suggests that the list of examples provided is not exhaustive. The legislators likely intended to clarify the definition by providing examples in the law. However, the examples fail to provide clarity as the entities listed are intrinsically different from one to another and, in some cases, are not best understood as data administrators. To take one example, government ministries, which are included on the list, regularly process "prohibited data" which they would not be allowed to administrate electronically if they were data administrators.

The examples provided in the law imply that data administrators are entities that manage a high volume of sensitive information. Questions remain as to whether insurance companies and hospitals, among others, would also be considered data administrators.

Apart from these examples, and the definition provided, there is no official guidance on identifying data administrators. As a result, the issue appears to be subject to the interpretation of the relevant authority. The vague definition weakens legal certainty around the identity of the data administrator.

4.3. The Law on Electronic Data Protection fails to provide a legal status to other stakeholders.

Under the Law on Electronic Data Protection, there is uncertainty around the legal rights and obligations of persons who fall outside of the scope of information owners or data administrators.

In the example in section 4.1 (above), we noted that a hotel operator may fall within the scope of the definition of information owner. There is also uncertainty about whether a hotel operator would fall within the definition of data administrator. This could lead to a scenario where the hotel operator possesses the rights of an information owner but not the obligations of a data administrator. The hotel operator would be exempted from complying with the provisions regulating the collection, use, transfer, and dissemination of electronic data. The hotel operator may also be exempted from restrictions on the administration of sensitive data and prohibited data. Without a clearer definition and the recognition of the variety of stakeholders involved in the administration of data (such as the categories of "controller" and "processor" under the GDPR), the protection of electronic data cannot be ensured as there may be stakeholders who are not captured by the legal obligations.

4.4. The law fails to provide a satisfactory definition of general data and personal data, thereby casting doubt on the categorization of personal data.

The Law on Electronic Data Protection provides that general data is information relating to "individual, legal entity, organization, which can be accessed, used and disseminated, however, its source should be correctly indicated" (Article 9). A list of examples is provided in the EDP Instructions: "name, address, phone number, e-mail address, information on organizations, general statistics, academic articles, etc." (Section 2).

The Law on Electronic Data Protection provides that "personal data is data of individual, legal entity, and organization" (Article 3, Section 12). Depending on its nature, personal data may fall under the scope of the definition of general data, sensitive data, or prohibited data.

As a result, apart from the examples provided in the EDP Instructions, it is difficult to identify what types of personal data might be deemed to be general data. The relevant authority must be consulted for guidance on data that is not expressly cited in the EDP Instructions. Legal certainty is bound to be weakened if reliance is placed on the discretionary decisions of such an authority.

4.5. The law fails to provide a satisfactory definition of sensitive data.

The Law on Electronic Data Protection provides that sensitive data is information "that individuals, legal entities, and organizations cannot access, use, or disseminate if [they] have not received consent from the Information Owner, or the relevant organization" (Article 10). A list of examples is provided in the EDP Instructions: "information on customers, financial information, CV, history of medical treatment, race, religion, project plan, budget plan, official servant secret, etc." (Section 3). Like general data, the law's definition of sensitive data does not refer to the qualities or characteristics of the data. As a result, apart from the examples provided in the EDP Instructions, it is difficult to identify data that might be deemed sensitive data.

Consequently, the relevant authority must be consulted for guidance on data that is not expressly cited in the examples in the EDP Instructions. In this case, legal certainty is important as sensitive data requires express consent from the information owner prior to being administrated by a data administrator. Accordingly, it is necessary for this issue to be clarified so that the relevant entities can take the appropriate steps prior to collecting this type of data.

4.6. There is a lack of clarity as to whether consent is required for the collection and transfer of general data.

General data can be "accessed, used, and disseminated" without the consent of the information owner. Access is defined in the EDP Instructions as "accessing general or sensitive data in order to use and disseminate [the data]" in accordance with the reason for which access was requested (Section 11). Use and dissemination refer to "taking out information" and sharing it with third parties, provided the purpose for which the information is shared accords with the purpose for which it was accessed, such as for marketing purpose (Section 9 of the EDP Instructions).

The Law on Electronic Data Protection provides that "the collection of information must receive the consent of the Information Owner" (Article 12). The collection of information is defined under the EDP Instructions as "the compiling of information in a database…for the convenience of access, monitoring, and use…" (Section 5).

Accordingly, while the consent of the relevant information owner is not required to access, use, and disseminate general data, consent is required to collect the data. Ultimately, in most cases the consent of the information owner will be required, as the collection of data will be, in practice, a prerequisite for access, use, and dissemination.

Similarly, the Law on Electronic Data Protection provides that data (the type is not specified) can only be transferred with the consent of the information owner, and if it can be guaranteed that the data will be adequately protected by the party receiving it (Article 17). It is unclear how the transfer of data, which requires consent, differs from dissemination, which can be carried out without consent.

Overall, the manner in which general data may be used by third parties appears to be limited.

4.7. Some data belongs to more than one category.

While the Law on Electronic Data contains three categories of data, some data would appear to belong to more than one category.

As noted above, sensitive data includes "information on customers, financial information, CV, history of medical treatment, race, religion, project plan, budget plan, official servant secret, etc." (Section 3 of the EDP Instructions).

Under the Law on Electronic Data Protection, prohibited data includes information pertaining to "race, ethnicity, political opinion, religious beliefs, sexual behavior, criminal records, health information, or any information that may affect the stability of the nation, the public order, and social orderliness of the society" (Article 33, Section 3).

The term "race" is explicitly mentioned in the definitions of both sensitive data and prohibited data. In addition, it is unclear what the difference is between "religion" (in the definition of sensitive data) and "religious beliefs" (in the definition of prohibited data).

Moreover, while "history of medical treatment" is listed as sensitive data in the EDP Instructions, "health information" is listed as prohibited data in the Law on Electronic Data Protection. Clarity on this point is important as health information is regularly administrated by business operators across many sectors. There is a risk of overregulation that could have severe implications in practice.

4.8. The definition of prohibited data is overly broad and could inhibit private sector operators from effectively using data for their internal operations and developing business activities that rely on electronic data.

As noted above, the Law on Electronic Data Protection provides that certain types of data cannot be administrated, even with the consent of the information owner. This includes data pertaining to:

- race;
- ethnicity;
- political opinion;
- religious beliefs;
- sexual behavior;
- criminal records;
- health information; or
- any information that may affect the stability of the nation, the public order, and social orderliness of the society.

The inclusion of health information in the list of prohibited data is unfortunate as it deprives many businesses that may be deemed to be a data administrator, or businesses relying on the services of a data administrator, from handling human resources effectively. Future electronic or mobile applications dedicated to health (e.g., telehealth) that rely on the electronic transfer of health information are likely to violate the law. Similarly, a company's records for any employees with a disability cannot be registered digitally, thereby complicating the company's hiring process and diversity. This would severely inhibit private sector employers handling employee records, which nowadays is usually done electronically.

On a similar note, companies often rely on electronic data when inquiring about the criminal records of new employees.

4.9. Lao government ministries are defined as data administrators, creating uncertainty over whether they can administrate citizens' data.

While the definition of "data administrator" is vague and imprecise, the Law on Electronic Data Protection explicitly states that ministries are data administrators. Accordingly, they are prohibited from electronically administrating prohibited data (see 4.8 above).

To take an example, on a plain reading, these provisions would make it unlawful for the Ministry of Public Security to electronically collect and store criminal records. Likewise, all other forms of prohibited data listed above could not be administrated electronically by a Lao government ministry.

5. Key Recommendations

5.1. The definitions of "personal data," "information owner" and "data administrator" should be amended and the rights and obligations of each should be clearly specified.

The Law on Electronic Data Protection would benefit from modeling its provisions on the GDPR, which has already been deemed a global blueprint for legislation in this area.

Personal Data and Information Owner

The definition of "personal data" is not satisfactory, as it does not refer to the qualities or characteristics of the data. Moreover, in order to create specific and comprehensive protection of data pertaining to individuals, the definition of "personal data" should not refer generally to data pertaining to individuals, legal entities, and organizations. Following the GDPR, personal data should be defined as any information that enables the identification of an individual.

Similarly, the definition of "information owner" should not refer generally to individuals, legal entities and organizations. Rather, an information owner should be the individual who can be identified by the personal data, following the definition of "data subject" under the GDPR. The definition should not refer to ownership of the information, as this could create legal uncertainty and may trivialize the protections that the law creates.

Data Administrator

The Law on Electronic Data Protection should further clarify the definition of "data administrator" by targeting individuals, legal entities, and organizations that administrate data for or on behalf of another individual or legal entity.

As discussed above, under the current law it is unclear what rights or obligations, if any, are placed upon individuals, legal entities, or organizations that do not fall within the definition of "information owner" or "data administrator."

Under the Law on Electronic Data Protection, "data administrator" is 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, a Bank" (Article 3, Section 14). According to the Law on Electronic Data Protection, "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."

A plain reading of these provisions would suggest that only a limited number of entities are considered to be data administrators. The law would appear to only capture entities that administrate a large volume of potentially sensitive data, as reflected in the entities expressly listed (Ministry, internet data centers, banks, etc.). Furthermore, we note that a data administrator is defined as an entity that has a "duty to administrate electronic data", which is significantly narrower than the concept of data controller under the GDPR, which captures entities that "determines the purposes and means of the processing of personal data". In this respect, the concept of data administrator under the Law on Electronic Data Protection may be closer to the concept of data processor under the GDPR, to the extent that it is concerned with the entity that actively administrates (or processes) the data, although it is not an exact equivalent as a data administrator does not administrate data on behalf of another party.

In various respects, it is unclear how the Law would be interpreted and applied in practice, and it is possible that it could be given a broader interpretation. As drafted, we believe that the Law on Electronic Data Protection is missing a "chain link" in its failure to distinguish between entities that process, treat and use electronic data.

The Law on Electronic Data Protection would benefit from the introduction of a further category modeled on the concept of "controller" under the GDPR. This would be an individual, legal entity, and organization that determines the purposes and means of the administration of electronic data. The introduction of this additional category would ensure that stakeholders who are involved in data processing are placed under legal obligations, even if they do not fall within the definition of Data Administrator. This would not prevent an individual, legal entity, or organization from being both a Data Administrator and a Controller, and there could be common obligations that apply to both entities (e.g., obtaining consent prior to collecting data from the Information Owner), it would also be possible to devise different rights and duties for these two entities.

Recommended Definitions

We recommend that Laos adopt the definitions provided in Article 4 of the GDPR, which are the benchmark for countries embracing data protections laws.

"Personal data" and "information owner" could be defined in a single provision as follows:

> ***"Personal data"*** *means any information relating to an identified or identifiable natural person ("Information Owner"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.*

In addition, in order to ensure that the law is in line with common practice wherein some types of personal data are widely communicated without requiring consent, the amended definition may provide that personal data does not include "data which specifies only the name, title, work place, or business address," as is the case under Singapore's data protection law.

"Data administrator" should be defined as follows:

> ***"Data Administrator"*** *means a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.*

Finally, an additional category of "controller" should be introduced and defined as follows:

> ***"Controller"*** *means the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.*

5.2. The Law on Electronic Data Protection should specifically protect "personal data" and provide satisfactory definitions of "general data" and "sensitive data."

In order to better protect information pertaining to individuals, there should be a chapter in the Law on Electronic Data Protection dedicated to personal data. Under this chapter, "personal data" would refer to the definition set out in section 5.1 above, and personal data could be collected, accessed, used, disseminated and transferred with the consent of the information owner.

Following the GDPR, a category of "sensitive personal data" could also be created (see GDPR Article 9 for reference). Such data may only be administrated with the consent of the information owner for legitimate use in specific circumstances. For instance, an employee may authorize the processing of their health data by their employer for a purpose related to their employment (e.g., sick leave, medical checkup, insurance benefits, social security). Likewise, a prospective employee could authorize the processing of other sensitive data (e.g., criminal records) as may be required for the hiring process. Notably, such data is also required by the local authorities for the processing of a business license.

Use of sensitive data could be also authorized for a variety of purposes, including:

- Legitimate business activity (e.g., insurance company);
- Medical analysis (e.g., for hospital, health care professional);
- When the information is made public by the information owner; etc.

Further conditions may be imposed on the data administrator and controller, such as requiring requests for the use of information to be precise, requiring informed consent, or establishing other technical requirements.

As the term "information owner" will be redefined to mean a natural person, and as the data of that natural person will be protected under the new category of "personal data/sensitive personal data", it might not be necessary to retain the separate category of "general data". If it is decided that category should be retained, it would need to be redefined to capture data that relates to information owners but which falls outside the scope of "personal data" (e.g., academic articles). Similarly, the role of the existing category of "sensitive data" will need to be considered if the new category of "sensitive personal data" is introduced.

5.3. The list of prohibited data should be removed or revised to allow more flexibility on the use of such data.

One option would be to remove the category of "prohibited data" entirely. The category of "sensitive data," or the proposed category of "sensitive personal data," would ensure a sufficient level of protection for sensitive information while still allowing it to be administrated in certain circumstances. This is vital in contexts where sensitive data must be processed, such as employment, health or public administration, as explained above.

If the category of prohibited data is retained, it should be revised given that ministries are deemed to be data administrators. For instance, it is doubtful that the Ministry of Public Security could transfer the criminal records that it stores electronically into nondigital forms of storage. Likewise, during the census, most of the types of data listed as prohibited data are collected by different ministries or governmental agencies and administrated electronically. Amending this list would ensure that the legal framework is aligned with the way such data is actually used by government agencies and business operators.

5.4. The legal requirement for private and public entities to appoint a data protection officer and ensure that data is correctly protected should be elaborated upon.

The Law on Electronic Data Protection introduces the concept of appointing an officer to be in charge of the protection of sensitive information (Article 23, Section 1). This provision should be elaborated upon to require the appointment of an independent data protection officer, like an independent financial auditor, who reports to the management level on issues pertaining to protection of personal data. As with the GDPR, this data protection officer would be registered with the authorities (e.g., LaoCERT), and would ensure that the legal requirements are consistently met. This officer would be the point of contact for the authorities in Laos that oversee data protection issues. LaoCERT could liaise and coordinate with the private sector via these data protection officers whenever a problem arises.

The mandatory appointment of a specific officer committed to the protection of personal data would cover entities that are data administrators, as well as other operators (e.g., insurance companies) and entities whose business relies on the administration of large volumes of electronic data (e.g., e-commerce or fintech companies), which may be either data administrators or controllers. The obligation should cover all high-risk entities and entities that administrate data in need of special protection (sensitive or prohibited data). In addition, it should cover entities that administrate large volumes of personal data. Entities that do not appoint a data protection officer should not be permitted to administrate personal data.

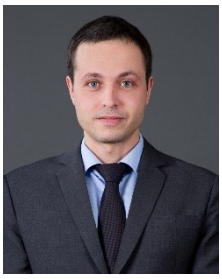
5.5. There is a lack of transparency relating to data breaches because notification of data breaches is not mandatory in Laos.

The Law on Electronic Data Protection only suggests that data administrators may work together with the LaoCERT to find a solution to a data breach or if their system is compromised (Article 26). Similarly, the EDP Instructions only suggest that a data administrator should seek guidance and is only required to contact the authorities to seek technical assistance and advice to prevent a data breach from "getting bigger" (Section 18).

In order to ensure transparency and the protection of data, the legal framework should make it mandatory for data administrators to report a data breach. This notification requirement may be triggered when a certain type of data (e.g., sensitive data) or a certain amount of data is breached.

Authors

Daniel Ferguson
daniel.f@tilleke.com



Dino Santaniello
dino.s@tilleke.com

Naiyane Xaechao
naiyane.x@tilleke.com

Tilleke & Gibbins

EUROCHAM LAOS Building
Nokeokoumane street, Anou Village,
P.O. Box 11781 Chanthabouly District, 1000
Phone: +856 21 264 330
Email: contact@eccil.org
www.eccil.org