NISHIMURA & ASAHI

西村あさひ法律事務所

Thailand V. Vietnam's Personal Data Protection Law: What are the notable differences?

Asia / Data Protection Newsletter

August 17, 2023

Author:

E-mail Tomonobu Murata
E-mail Nguyen Tuan Anh
E-mail Nguyen Thi Thanh Ngoc
E-mail Chanakarn Boonyasith
E-mail Pitchabsorn Whangruammit
E-mail Natrada Ruangwuttitikul

Introduction

This newsletter provides a glimpse of key differences between Thai and Vietnamese personal data protection laws, with a focus on some topics that businesses handling personal data in both nations should understand. Given that personal data is precious treasure to business development in this digital era, these regulations represent the authorities' effort to protect Thai and Vietnamese data subjects against illicit collection, usage, or sharing of their personal data, as well as shape the good order of data processing in their jurisdictions.

In Thailand, the Personal Data Protection Act BE 2562 (2019) ("**Thai PDPA**") was originally scheduled to come into full effect on 27 May 2020. However, recognizing the lack of preparedness in both the public and private sectors for Thai PDPA compliance, the Government wisely issued a Royal Decree on 20 May 2020, technically postponing full enforcement until 31 May 2021. Due to unforeseen circumstances, including the third wave of the COVID-19 outbreak, Thai PDPA enforcement was further delayed through a Royal Decree on 7 May 2021, extending the postponement until 31 May 2022. At present, limited sub-legislation related to the Thai PDPA has been officially announced. As a whole, the Thai PDPA is very similar to the EU General Data Protection Regulations ("**GDPR**"); therefore, it might not be difficult for global businesses to understand and comply with the regulations.

In Vietnam, Decree No. 13/2023/ND-CP of the Government on Personal Data Protection (dated 17 April 2023) ("**Vietnam PDPD**") came into effect on 1 July 2023. The Vietnam PDPD symbolizes the Government's approach in unifying and fortifying the legal framework safeguarding personal information in Vietnam. The Vietnam PDPD has introduced unique regulations emphasizing supervision by the government, with some being more strict than the GDPR; therefore, it might be more difficult to understand and comply with the regulations.

By comparing the Thai PDPA and Vietnam PDPD, this newsletter aims to shed light on their differences by providing a regulatory comparison of some notable topics, primarily for business transactions pertaining to personal data within the jurisdictions of Thailand and Vietnam. This newsletter serves as preliminary guidance, offering a concise and straightforward narrative to facilitate a better understanding of the subject matter in the below points.

Summary and Key Takeaways

As the Thai PDPA came into effect prior to the Vietnam PDPD, there have been greater advancements in terms of the number of some sub-regulations and guidelines issued in Thailand. Both the Vietnam PDPD and Thai PDPA share a similar landscape concerning the absence of precedent cases and certain sub-regulations to bolster the fundamental tenets of personal data protection. The current state of affairs highlights the need for ongoing developments and regulatory measures to strengthen the frameworks governing data protection in both jurisdictions.

However, **there are quite a few differences when comparing the Thai PDPA and Vietnam PDPD. The most important difference is that, under the Vietnam PDPD, all businesses processing or internationally transferring personal data are required to record and assess the associated risks and submit verification of having done so (including, where necessary, the actual records) to the government.** Thailand has no such regulations. Rather, the Thai government has not included regulations on data protection impact assessment in enacting the Thai PDPA (however, the said concept is acknowledged and suggested to be implemented by the Personal Data Protection Committee (the "**PDPC**") before a data controller (defined below) collects, uses or discloses personal data from other sources, apart from the data subject directly). Also, **the Vietnam PDPD still utilizes a consent–oriented approach for processing personal data. The Thai PDPA, on the other hand, has introduced legitimate interest as one of the legal grounds for personal data processing, following the GDPR; the Vietnam PDPD, however, did not adopt this approach.** As such, businesses in Vietnam may have more problems processing personal data when it is practically difficult to obtain consent from data subjects.

When it comes to extraterritorial applicability, the criteria for determinations are different, with the Vietnam PDPD providing an unclear and broader scope compared to the Thai PDPA. Furthermore, the concept of overseas transfer of personal data differs as well. The Vietnam PDPD tends to use the threshold of cyberspace, electronic devices, equipment, or other means for cross-border data transfers, while the Thai PDPA broadly covers the transfer of personal data to overseas. Additionally, the concept of appointing a Data Protection Officer ("**DPO**") also differs in that the Vietnam PDPD mandates the appointment of a DPO only for sensitive personal data, whereas the Thai PDPA extends the requirement to data controllers or data processors who are public authorities or entities with a large amount of personal data requiring regular monitoring as well, not solely based on sensitive personal data.

In detail

1. Extraterritorial scope of application

The Thai PDPA and the Vietnam PDPD both set forth extraterritorial applicability; however, the criteria for determining this applicability are different. It seems that the Vietnam PDPD provides a broader scope of extraterritorial applicability than that of the Thai PDPA.

In Thailand, the Thai PDPA may apply to any entities located outside Thailand if they collect, use or disclose personal data of a data subject who is located in Thailand, for (i) offering of goods or services to data subjects located in Thailand, irrespective of whether or not a payment has been made by the data subject; or (ii) monitoring of a data subject's behaviour which takes place within Thailand.

In Vietnam, similar to the Thai PDPA, the Vietnam PDPD has an extraterritorial scope of application that may capture a wide range of offshore subjects, including foreign agencies, organizations, and individuals, without

having any presence in Vietnam, (i) directly participating in or (ii) related to personal data processing activities in Vietnam. The Vietnam PDPD is silent on how to determine these two criteria, as a result, the determination of such criteria is subject to interpretation of the regulatory authority in Vietnam.

We think that although both the Thai PDPA and the Vietnam PDPD provide extraterritorial application scopes, the criteria under the Thai PDPA seems to be straightforward while those under the Vietnam PDPD seem vague. This vagueness results in a possibility that the governing scope of the Vietnam PDPD could be much broader than that of the Thai PDPA.

2. Definition of "Personal Data"

It is important for an individual or entity engaging in data processing to confirm that they have the correct understanding of how to identify whether they collect, use or disclose "**personal information/data**". This is the first step in understanding whether the Thai PDPA or Vietnam PDPD apply to their particular activities.

For the **Thai PDPA**, “personal information/data” means **any information relating to a natural person, which enables the identification of such person, whether directly or indirectly**, but does not include the information of a deceased person.[1]

Comparable to the Thai PDPA, **the Vietnam PDPD** defines "personal data" as **electronic information in the form of symbols, letters, numbers, images, sounds, or equivalences that are associated with a specific individual or help identify a specific individual**.[2] Article 2.2 of the Vietnam PDPD further stipulates that information that helps identify a specific individual means information derived from an individual's activities that, when combined with other data and stored information, can identify a particular person. This definition covers personal data of any individual without any exclusion. Therefore, the personal data of a deceased person is included and protected under the Vietnam PDPD.

Per the above, we think that the definition of personal information/data in both Thai PDPA and Vietnam PDPD are generally similar in terms of aiming for identification of the individual. However, unlike the Thai PDPA, the Vietnam PDPD provides a broader scope of personal data covering that of even deceased persons.

3. Covered Actors

The Thai PDPA governs the main actors namely, data subjects, data controllers and data processors. A “data controller” is a person who determines or decides whether it will collect, use or disclose personal information/data, while a “data processor” is a person who collects, uses or discloses personal data pursuant to orders given by or on behalf of the data controller.[3]

1 Thai PDPA, Section 6.

2 Vietnam PDPD, Article 2.1.

3 Thai PDPA, Section 6.

Data controllers are obligated to collect, use and disclose personal data lawfully, which includes relying on consent or legal exceptions[4], ensuring purpose limitation,[5] ensuring data minimization,[6] conducting privacy information notifications,[7] complying with the cross-border data transfer requirements,[8] conducting data processing record/documentation,[9] DPO appointment,[10] providing appropriate 'security measures', preventing recipients of personal information from using or disclosing it unlawfully, putting in place an examination system for erasure or destruction of personal information, and conducting data breach notifications,[11] as well as to uphold data subject's rights recognized under the Thai PDPA.

The Vietnam PDPD governs the actors, including data subjects, data controllers, data processors, data processor-controllers and third parties. In comparison, while the concepts of data controller and data processor and their main obligations under the Vietnam PDPD are generally the same as those prescribed under the Thai PDPA,[12] the Vietnam PDPD introduces the "data processor-controller" as an unique actor mixing elements of the data controller and data processor concepts, who simultaneously decides the purposes and means of data processing and directly processes personal data. This actor must comply with the obligations and requirements imposed on both data controllers and data processors.

4. Legal bases for processing personal data

The Vietnam PDPD provides a number of legal bases for the processing of personal data. Generally, entities must obtain the data subject's valid consent for the processing of their personal data.[13] In addition, the Vietnam PDPD provides certain cases where entities may process personal data without consent, in particular:[14]

- In the event of an emergency, the relevant personal data must be immediately processed to protect the life and health of the data subject or others;

- The disclosure of personal data in accordance with the law;

- The processing of data by competent state agencies in the event of an emergency on national defense, national security, social order and safety, major disasters, or dangerous epidemics; when there is a risk of threatening security and national defense but not to the extent of declaring a state of emergency; to prevent and combat riots and terrorism, and to prevent and combat crimes and violations of the law in accordance with the law;

---

4 Thai PDPA, Section 19.

5 Thai PDPA, Section 21.

6 Thai PDPA, Section 22.

7 Thai PDPA, Section 23.

8 Thai PDPA, Section 28 and Section 29.

9 Thai PDPA, Section 39.

10 Thai PDPA, Section 41.

11 Thai PDPA, Section 37.

12 Vietnam PDPD, Articles 2.9 and 2.10.

13 Vietnam PDPD, Article 11.

14 Vietnam PDPD, Articles 17 and 18.

- To fulfill the contractual obligations of the data subject with relevant agencies, organizations and individuals in accordance with the law;

- To serve the activities of state agencies as prescribed by specialized laws; and

- Competent agencies and organizations may record audio and/or video and process personal data obtained from such audio and/or video recording activities in public places for the purpose of protecting national security, social order and safety, organizations, legitimate rights and interests of organizations and individuals in accordance with the law. When recording audio and/or video, competent agencies and organizations are responsible for notifying the subject of such recording so that the data subject understands that they are being recorded, unless otherwise prescribed by the law.

For the Thai PDPA, the general principles concerning the collection of personal data, similar to the Vietnam PDPD, are based around **whether to obtain the consent or rely on exemptions**. That said, the entities shall not be able to collect, use and disclose personal data unless the data subject grants his/her consent before or at least at the time of such collection[15] in a manner provided for in Section 19 of the Thai PDPA (i.e., *conditions for consent)*; except where the Thai PDPA or other applicable laws allow him/her to do so without the data subject's consent, under certain **exceptions**.

The exemptions that allow the collection, use and disclosure of personal data (that is not considered as sensitive information) without consent are for preparation of scientific, historical or statistic research,[16] vital interest,[17] contract,[18] public task,[19] legitimate interest,[20] and legal obligation.[21] *Nevertheless,* exemptions of the consent required for collection, use or disclosure of sensitive personal information are more limited and different from general personal data under Section 24 of the Thai PDPA.

Both the Vietnam PDPD and the Thai PDPA share some similarities in terms of legal basis for data processing, **however Vietnam does not allow data processing based upon legitimate interest as Thailand does.** Furthermore, unlike the Thai PDPA that leaves vital interests broad, the Vietnam PDPD defines and limits the vital interest of an individual to his or her health and life only.

On this point, in light of the case study recently published on the Ministry of the Digital Economy and Society's website, the Thai PDPA appears to take a similar approach to the GDPR on how to select legal bases in processing personal data (i.e., it cannot be easily changed); therefore, businesses should be more careful to rely on consent, taking into account a possibility of consent withdrawal.

15 Thai PDPA, Section 23.

16 Thai PDPA, Sections 24(1) and 27.

17 Thai PDPA, Sections 24(2) and 27.

18 Thai PDPA, Sections 24(3) and 27.

19 Thai PDPA, Sections 24(4) and 27.

20 Thai PDPA, Sections 24(5) and 27.

21 Thai PDPA, Sections 24(6) and 27.

5. Processing of "Sensitive Personal Data"

The Vietnam PDPD mandates certain measures to be taken to protect sensitive personal data (i.e., any personal data associated with a particular individual's privacy which, upon being violated, will directly affect the individual's legitimate rights and interests, such as political and religious opinions; health condition and information on private life stated in health records, excluding information on blood type; information about racial or ethnic origin; information about genetic data related to an individual's inherited or acquired genetic characteristics; information about an individual's own biometric or biological characteristics; information about an individual's sex life or sexual orientation). It is practically notable that financial data including bank account data is included in the definition of the sensitive personal data. The GDPR and the Thai PDPA do not treat such data as sensitive personal data. Other than the similar measures compelled for the protection of basic data, the entities involved in the processing of sensitive data must designate a data protection department (DPD) and a DPO, and further provide the contact information of their DPD and DPO to the Department of Cyber Security and Hi-tech Crime Prevention under the Ministry of Public Security (commonly referred to as "**A05**"). In addition, the concerned entities must further notify the data subjects of their sensitive data being processed, except for a number of cases where such notification is not required as prescribed in the Vietnam PDPD; for example, in cases where the personal data is processed by the competent authority to support such authority's operation.[22]

The Thai PDPA also mandates certain measures for sensitive personal data (i.e., racial, ethnic origin, political opinions, cults, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data[23] or any data which may affect the data subject in the same manner as prescribed by the Personal Data Protection Committee ("**PDPC**")), like the Vietnam PDPD. In addition, the data controller and the data processor shall have an obligation to establish a DPO (in particular, where, amongst others, the core activity of the data controller or the data processor is the collection, use, or disclosure of the sensitive personal data[24]) and to provide the information of the DPO, contact address, and contact channels to the data subject and the Office of the PDPC. The data subject shall be able to contact the DPO regarding the collection, use, or disclosure of the Personal Data and the exercise of rights of the data subject under the Thai PDPA.[25] Generally, the Thai PDPA requires a higher level of consent for sensitive personal information, where sensitive personal information must not be collected **unless explicit consent is obtained from the data subject**.[26] Nevertheless, there is no sub-legislation or clear guidance from the relevant authority as to what should be considered as '**explicit consent**'.

Referring to the exemptions in cases involving sensitive personal information, they are more limited and different from exemptions in cases involving general personal information. A summary of exemptions where 'explicit consent' does not need to be required for collecting, using or disclosing sensitive data can be summarized as follows:

- Where it is to prevent or suppress a danger to the life, body or health of a person, where the data subject is incapable of giving consent for whatever reason;

---

22 Vietnam PDPD, Article 28.

23 Thai PDPA, Section 26, paragraph two: 'biometric data' means the Personal Data arising from the use of technics or technology related to the physical or behavioral dominance of an individual, which can be used to identify such individual apart from other individuals, such as the facial recognition data, iris recognition data or fingerprint recognition data.

24 Thai PDPA, Section 41(3) Paragraph 1.

25 Thai PDPA, Section 41 Paragraph 5.

26 Thai PDPA, Section 26.

- Where it is carried out in the course of legitimate activities with appropriate safeguards put in place by the foundations, associations or any other not-for-profit bodies with political, religious, philosophical or trade union purposes, for their members, former members of the bodies or persons having regular contact with such foundations, associations or not-for-profit bodies in connection with their purposes without disclosing the personal data outside of such foundations, associations or not-for-profit bodies;
- Where it is information that is disclosed to the public with the explicit consent of the data subject;
- Where it is necessary for the establishment, compliance, exercise or defense of legal claims; and
- Where it is necessary for compliance with a law to achieve purposes in respect of specific matters described in the Thai PDPA.

The Thai PDPA and Vietnam PDPD have similar requirements upon data controllers for appointing a DPO upon the processing of sensitive personal data, and additional requirements regarding provision of DPO contact information to the competent authorities. Other than the above requirements, the Vietnam PDPD only requires additional information on the sensitivity nature of the data to be processed without any further treatment requirements. The Thai DPDA imposes stricter conditions for valid consent and limits the consent exemptions regarding the sensitive personal data to be processed.

6. Data Protection Officer (DPO)

In compliance with **the Thai PDPA**, the concept of a **DPO** has been introduced.[27] Data controllers and data processors are mandated to designate a DPO in the following scenarios:

- Where the data controller or data processor is a public authority as prescribed and announced by the PDPC;

- Where the activities of the data controller or data processor in the collection, use or disclosure of the personal data require regular monitoring of the personal data or the system, by the reason of having a large amount of personal data as prescribed and announced by the PDPC; or

- Where the core activity of the data controller or data processor is the collection, use or disclosure of sensitive personal data.[28]

Though, like the Thai PDPA, the concept of DPO is introduced in the **Vietnam PDPD**, there is a notable difference in the events determining whether a DPO is required under the two regulations. Under the Vietnam PDPD, the appointment of a DPO only is required when processing any sensitive personal data.[29] Comparing the manner in which events of processing sensitive personal data are defined, it seems that the Vietnam PDPD covers a broader scope of application than the Thai PDPA by requiring the appointment of a DPO in any processing of sensitive data. Alternatively, the Thai PDPA only requires a DPO be appointed in cases where the processing of the sensitive data is the core activity.

7. Data Processing Impact Assessment

Under the Thai PDPA, a data controller is not required to conduct a Data Processing Impact Assessment ("**DPIA**"; it is merely suggested to do so before collection, use or disclosure of personal data from other sources,

27 Thai PDPA, Section 41.

28 Thai PDPA, Section 26.

29 Vietnam PDPD, Article 28.2.

apart from the data subject directly, as per the guidance issued by the PDPC) but is required to *at least* record and maintain the following information and make it available for data subjects or the PDPC Office to check on (in either in written or electronic form):[30]

- the collected personal data;
- the purpose of the collection of the personal data in each category;
- details of the data controller;
- the retention period of the personal data;
- rights and methods for access to the personal data, including the conditions regarding the person having the right to access the personal data and the conditions to access such personal data;
- the use or disclosure under Section 27 paragraph three of the Thai PDPA;
- the rejection of request or objection; and
- explanation of the appropriate security measures.

In the context of the Thai PDPA, a Thai Company classified as a 'small organization' based on criteria established by the PDPC will be exempted from recording the majority of information outlined in Section 39 of the Thai PDPA, as mentioned earlier (excluding information related to denial of data subject's requests, which is still required to be recorded under the Thai PDPA).

Under the Vietnam PDPD, from the commencement of data processing, the data controller, data processor, or third party is required to conduct a DPIA and record a number of types of information in a DPIA dossier (similar to those recorded as required under the Thai PDPA) as below:

- Contact information and details of the data controller/processor/third party;
- Name and contact details of the organization or employee assigned to protect the personal data of the data controller;
- Purposes of processing data;
- Types of personal data to be processed;
- Organizations or individuals receiving data, including the organization or individual that is located outside the territory of Vietnam;
- Cases of overseas transfer of personal data;
- Duration of processing of personal data; estimated duration of deletion or destruction of personal data (if any);
- Description of measures for personal data protection;
- Assessment of impact of personal data processing; undesirable consequences and damage that may occur, measures for mitigating or removing such consequences and damage.

The data controller/processor must record the foregoing information in a DPIA dossier and submit such dossier to the A05 within 60 days from the commencement date of data processing.[31] The dossier must always be up-to-date and available for the check and inspection of A05.[32] Unlike the Thai PDPA, the Vietnam PDPD provides no exceptions for the information record obligation of the data controller.

30 Thai PDPA, Section 39.

31 Vietnam PDPD, Clauses 1, 3 of Article 24.

32 Vietnam PDPD, Clause 24.6 of Article 24.

8. Cross-Border Data Transfers

In the concept of the Thai PDPA, in the case where the data controller sends or transfers personal data to a foreign country, the destination country or international organisation receiving such data shall have **an adequate protection standard** and **such transfer shall be carried out in accordance with the rules prescribed by the PDPC.**[33]

Within this conceptual framework, the scenario arises where the Thai company engages in the sharing of personal data with its headquarters, subsidiaries, affiliates, and similar entities in foreign jurisdictions. Consequently, **the permissibility of cross-border data transfers hinges upon adherence to both an adequate protection standard and the pertinent laws.** Nevertheless, it is worth noting that the absence of explicit guidance from the relevant authority leaves the notion of an "*adequate protection standard*" within the realm of uncertainty, necessitating caution and ongoing vigilance.

Amidst the lingering *ambiguity* surrounding the precise parameters of this qualifying standard, the data controller under the Thai PDPA retains the capacity to transfer personal information, even in cases where the data protection standards may fall short, provided certain exemptions are met (as explicitly stipulated in Section 28, paragraph one of the Thai PDPA). These exemptions encompass:

- compliance with the law;
- consent has been obtained (and the data subject has been informed of the inadequate personal data protection standards of the destination country);
- necessity for the performance of a contract; compliance with a contract between the Data Controller, and other persons or juristic persons for the interests of the data subject;
- prevention or suppression of danger to the life, body, or health of the data subject or other individuals, when the data subject is incapable of giving the consent at such time; and
- the necessity for carrying out the activities in relation to substantial public interest.

Alternatively, under Section 29 of the Thai PDPA, a data controller may rely on other provisions under the Thai PDPA, namely (i) for the transfer within same affiliated business, a data controller may rely on rules certified by the PDPC Office (commonly and unofficially known as the Binding Corporate Rule); or (ii) in absence of the PDPC's decisions and certified rules, the data controller may provide 'appropriate safeguards' and 'legal remedies' in accordance with the criteria prescribed by the PDPC. Furthermore, the draft sub-regulation, i.e., PDPC's Notification Re: Rules and Principles of Appropriate Personal Data Protection for International Transfer, has introduced the concept of a standard contractual clause, code of conduct and certification as appropriate safeguards. Nonetheless, the explicit obligations and conditions pertaining to the transfer of personal data needs further clarification and enhancement.

It is worth noting that the aforementioned draft underwent a process of public hearings in October 2021. However, as of now, there has been no official announcement regarding its enforcement.

In the current landscape of Thailand, while the absence of specific guidance on the adequate protection standard persists, **a prudent approach would entail seeking the data subject's consent or relying on the exemptions as listed above for the transfer and disclosure of their personal information to other subsidiaries or affiliated entities situated in foreign jurisdictions.**

---

[33] Thai PDPA, Section 28.

However, the Vietnam PDPD prescribes a concept of overseas transfer of personal data that is slightly different from the concept of "cross-border transfer of data" under the Thai PDPA. Overseas transfer of data is the act of using cyberspace, electronic devices, equipment, or other forms to transfer the personal data of a Vietnamese citizen to a location outside the territory of Vietnam or using a location outside the territory of Vietnam to process personal data of a Vietnamese citizen.[34]

The transferor of the personal data is obliged to compile a data transfer impact assessment dossier which comprises, without limitation, the following information: the consent of the data subject; description and explanation about objectives of the processing of a Vietnamese Citizen's personal data after the personal data is transferred abroad; assessment of the impact of personal data processing, undesirable consequences and damage that may occur, and measures for mitigating or removing such consequences and damage.[35] **The said dossier must be sent to the A05 within 60 days from the commencement date of data processing and must further be up-to-date and, at all times, available for the check and inspection of A05**.[36]

9. Data Breach Notification

Under the Vietnam PDPD, the data controller or the data processor-controller is mandated to notify the A05 within 72 hours from the occurrence of a data breach.[37] In case of a late notification, the concerned entity must further send to the A05 an explanation for such late notification. The data processor must notify the data controller as quickly as possible after noticing a violation of the regulations on personal data protection.[38] However, the Vietnam PDPD does not clearly require businesses to make such notification to data subjects (unlike the GDPR and the Thai PDPA), although such obligation might be interpreted to be triggered based upon the principle of "transparency" under the Vietnam PDPD (Article 3.2).

There are some slight differences and additional inputs of provision between the Thai PDPA and the Vietnam PDPD. For the Thai PDPA, **the data controller alone** is required to notify the PDPC Office of any personal data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such personal data breach is unlikely to result in a risk to the rights and freedoms of the underlying individuals. **If the personal data breach is likely to result in a high risk to the rights and freedoms of such individual(s)**, the data controller is required to notify both the personal data breach and the remedial measures to the data subject without delay. The notification and the exemption to the notification is subject to the rules and procedures set forth by the PDPC.

10. Penalty

Non-compliance with **the Thai PDPA** is subject to **three categories of penalties**, which are **civil liabilities** accompanied by punitive damages, **administrative penalty** as fines reaching up to Baht five million (equivalent to approximately USD 142,000), as well as **criminal penalties**, including imprisonment for a maximum of one year, a fine of up to Baht one million (around USD 28,500), or both.

---

34 Vietnam PDPD, Article 2.14.

35 Vietnam PDPD, Clauses 1 and 2 of Article 25.

36 Vietnam PDPD, Article 25.3.

37 Vietnam PDPD, Article 23.1.

38 Vietnam PDPD, Article 23.2.

However, **in Vietnam,** specific penalties concerning personal data protection violations in Vietnam are not detailed in the Vietnam PDPD and will be specified in a different legal document which is currently under development. In particular, the Ministry of Public Security is working on a Decree on administrative penalties in the field of cybersecurity, which provides sanctions applicable to violations of relevant regulations on personal data protection under the Vietnam PDPD. Under the latest version of the said draft Decree available on public sources, the monetary sanctions imposed on organizations for violations of personal data protection regulations varies depending on the specific violation, among which, the highest level of fine is VND 1,000,000,000, or five percent of the revenue of such enterprise in the Vietnamese market.[39]

While there is yet to be a specific legal text on administrative penalties for violations in the field of personal data protection, some of the violations of the Vietnam PDPD may still be imposed with certain penalties available under existing regulations, including a fine level of up to VND 60 million (approx. USD 2.500).[40] In addition to administrative penalties, non-compliance with the Vietnam PDPD may be subject to either civil or criminal penalties, depending on the degree and character of such non-compliance.[41]

11. Regulatory Authority

In Thailand, the **PDPC**, acting as the regulatory authority, assumes the crucial role of formulating and promulgating sub-regulations under the Thai PDPA. Their expertise and dedication play a pivotal role in shaping a robust regulatory framework aimed at effectively safeguarding personal data. They hold the power and duty to determine operational measures for personal data protection, ensuring Thai PDPA compliance and promoting data protection. They also are responsible for issuing notifications, orders, and establishing rules and guidelines for the compliance of personal data controllers and processors.

The PDPC comprises **not just only government officials, but also well-selected experts** having distinguished knowledge, skills, and experience in various domains, such as personal data protection, consumer protection, information technology, communication, social science, law, health, finance, and other relevant fields. These experts are carefully chosen based on their extensive knowledge, skills, and experience to ensure effective implementation and protection of personal data.[42]

In Vietnam, A05 under the Ministry of Public Security serves as a specialized force to support the Government in the protection of personal data in Vietnam. The A05's primary responsibilities are quite similar to those of the PDPC, as previously stated. The striking difference between the PDPC and A05 comes in their respective compositions; while the PDPC in Thailand comprises experts in different sectors related to personal data, A05 is entirely made up of government officials. However, A05 will carry out its task and functions in collaboration with other relevant governmental bodies.[43]

With these similarities and differences identified through the comparison of the Thai PDPA and Vietnam PDPD, we aim to provide you with a comprehensive understanding of the concept of personal data protection in

39 The latest version of the draft Decree, Article 5.2 and Article 43.

40 Decree No. 98/2020/ND-CP and Decree No. 15/2020/ND-CP.

41 Vietnam PDPD, Articles 4, 9.10; Criminal Code, Article 288.

42 Thai PDPA, Section 8.

43 Vietnam PDPD, Articles 23, 24, 25 and 32, and Chapter III.

Thailand and Vietnam. Should you wish to obtain further details on the Thai PDPA and the Vietnam PDPD and their comparison, please contact us.

Public Relations Section, Nishimura & Asahi E-mail✉