A STUDY OF THE NECESSITY OF AND APPROACHES TO THE PREPARATION OF PERSONAL DATA PROTECTION GUIDELINES*

*Khemmapat Trisadikoon***

1. INTRODUCTION

Thailand's Personal Data Protection Act, B.E. 2562 (2019) was enacted to protect the personal data of a data subject (defined as a natural person or juristic person about whom a controller holds personal data and who can be identified, directly or indirectly, by reference to that personal data) by setting out rules, and mechanisms, along with regulatory measures regarding the collection, storage, use, or disclosure of personal data, collectively known as "personal data processing."

However, that Act does not provide rules or procedures in detail. As a result, a guideline must be developed as an important instrument to assist in the reasonable implementation of the law or the principles set out in legislation in practice, particularly for agencies with specific missions or services.

Therefore, the Office of the Permanent Secretary, Ministry of Digital Economy and Society, serving as the Office of the Personal Data Protection Commission,[1] has assigned the Thailand Development Research Institute (TDRI) as a research team to study and draft personal data protection guidelines for relevant entrepreneurs and for the benefit of effective enforcement in accordance with the personal data protection law under the "Personal Data Protection Guideline for Personal Data Controllers and Data Processors according to the Data Protection Act, B.E. 2562" program, and to prepare relevant policy recommendations to address the issues not applied under the guidelines. Although the draft guidelines do not have a legal status that must be strictly followed, the draft guidelines, which lay out guidelines for relevant parties to implement, must be considered and reviewed by the Personal Data Protection Committee, which will be established later, before further promulgation.

* *The article is a part of the "Project on Preparing Personal Data Protection Guidelines on Data Controllers and Processors under the Personal Data Protection Act, B.E. 2562 (2019)," which was completed in December 2021. The project was funded by the Permanent Secretary of the Ministry of Digital Economy and Society.*

** *Khemmapat Trisadikoon is Researcher, Law for Development, Thailand Development Research Institute.*

[1] *Personal Data Protection Act, B.E. 2562 (2019), Section 93. During the period when the Office of the Personal Data Protection Committee has not yet been duly set up, the Office of the Permanent Secretary of the Ministry of Digital Economy and Society shall perform the duties in accordance with this Act, and the Minister shall appoint a Deputy Permanent Secretary of the Ministry of Digital Economy and Society to perform the Secretary-General's duties.*

2.GUIDELINES FOR PERSONAL DATA PROTECTION ACCORDING TO THE LAW IN THAILAND

The Act determines personal data protection measures that provide personal data subjects with the power to decide on their personal data. This includes establishing methods for exercising their rights over personal data under control of the data controller or the data processor.

Under the provisions of the Act, the guidelines for personal data protection are divided into five fields as follows:

2.1 Scope of law enforcement

The scope of law enforcement is a critical topic that raises the question "in what matters and to what territories can the law be applied." The scope of enforcement of the Act can be divided into two characteristics: material scope and territorial scope.

(a) Material scope

The Act provides seven exceptions[2] to the processing of personal data for certain activities as follows: (1) personal data processing for personal gain or household activity; (2) personal data processing for the purpose of maintaining state security or public safety; (3) personal data processing in the case of mass media, fine arts, or literature; (4) personal data processing in compliance with the relevant legislative duties and powers; (5) personal data processing in court proceedings, criminal justice procedures, legal execution, and deposit of property; (6) personal data processing in the case of credit bureau business; and (7) personal data processing exempted by royal decree. The Act shall not apply to the processing of personal data under the aforementioned clauses. However, such personal data must still be protected by the personal data controller, who must provide security in accordance with the standard.[3] Furthermore, it may be necessary to comply with other methods that are specifically required by law. For example, the personal data protection procedure in judicial proceedings might employ the methods prescribed in procedural laws.

(b) Territorial scope

With regard to territorial scope, the Act supports extraterritoriality where it can be applied to the personal data processing of a personal data subject of Thai nationality, whether or not the processing takes place in Thailand. However, a personal data controller or processor based outside of Thailand shall be held accountable only if the processing is done for the purpose of offering goods or services, or monitoring of the personal data subject's behavior where the behavior takes place within Thailand.[4]

2.2 Rights of the personal data subject

The objective of the personal data subject's rights under the Act is to ensure the legal authority

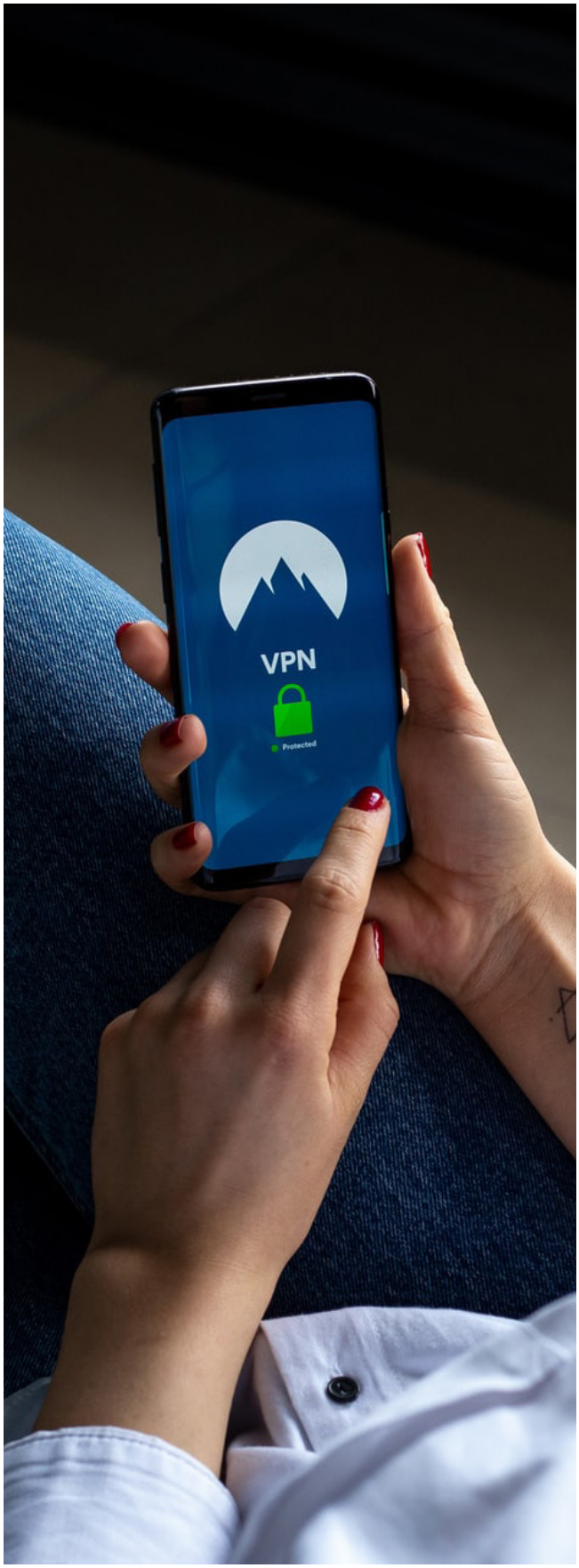
[2] *Personal Data Protection Act, B.E. 2562 (2019), Section 4.*

[3] *Ibid., Section 4.*

[4] *Ibid., Section 5.*

of the personal data subject to exercise the subject's right over one's own personal data by assigning duties to the personal data controller that allow the personal data subject to exercise his, her or its (hereafter "its" is used for convenience when referring to singular subjects) rights with ease. The law also provides the methods that encourage the personal data subject to fully exercise its right to regulate decision-making regarding personal data through data subject access requests. The personal data subject has eight rights that are currently recognized by law (Table 1), although the personal data controller may deny the exercise of such rights if there are adequate legal grounds.[5]

Nevertheless, compared with the international guidelines for exercising personal data subject rights, the Act does not endorse the right of personal data subjects to exercise their legal rights free of charge,[6] which may affect the exercise of legal rights in practice.



[5] *However, the rights of data subjects under the Act differ from certain rights guaranteed in the General Data Protection Regulation (GDPR), such as rights related to automated decision-making, including profiling under Article 22 of the GDPR.*

[6] *GDPR, Article 12.*

Table 1: Right of personal data subject under the Personal Data Protection Act, B.E. 2562

Right	Description
Right to be informed	The data subject has the right to know details about the data controller's use of personal data or events about that personal data. The data controller shall notify the data subject prior to or while the personal data is being processed so that the data subject can make informed decisions on matters that may affect its privacy rights. This right, therefore, calls for the controller to provide notification by means of clear and easy-to-understand communication.
Right to access	The data subject has the right to access its personal data collected by the data controller to check and recognize the relevant details, and can obtain a copy of the personal data that the personal data controller has collected.
Right to object	If the data subject does not agree to the processing of its personal data, the data subject may request the data controller to separate the data subject's wishes from other data sets and stop processing such data sets. After the data subject requests to exercise its rights, the data controller will not be able to continue collecting, using, or disclosing that personal data.
Right to withdraw consent	The right to express one's wishes to the data controller where data processing is based on consent is a legitimate ground for the processing of personal data. The data subject can express its wish to withdraw its consent at any time. After the consent is withdrawn, the data controller will not be able to process the personal data.
Right to data portability	If the processing of personal data is carried out by a technological system (not a paper file format), the data subject can request the data controller to provide or proceed to send the information to another data controller to the extent that the data controller can do so within the framework of the limitations or ability of the data controller to collect, use, disclose or transmit personal data.
Right to restriction of processing	The data controller shall limit or temporarily stop the processing of the data subject's data (different from the right to object, which is a permanent cessation of data processing).
Right to rectification	The data subject can submit a request to exercise the right to correct the data. This includes requesting the removal of old data and adding new data, so that the processing will be complete and involve accurate use of current data, and not cause any misunderstanding, and is beneficial to the data subject in order that the data subject would receive appropriate services.
Right to erasure and right to be forgotten	The data subject may request the data controller to delete or destroy its personal data. This includes using whatever means that make the information no longer personally identifiable. In addition, if such information is no longer necessary for its purpose, without any other legal basis, it is grounds for legally processing that data. The data controller should also have to delete personal data.

Source: Somkiat Tangkitvanich and others, 2021.

2.3 Relationships between parties involved in the processing of personal data

The Act establishes the relationship between the parties involved in the processing of personal data by dividing the relationship into two parts: (a) the relationship between the personal data subject and the personal data controller; and (b) the relationship between the personal data controller and the personal data processor.

(a) The relationship between the personal data subject and the personal data controller

The relationship between the personal data subject and the personal data controller under the Act is in the form of rights that the personal data subject has toward the personal data controller and duties that the personal data controller owes to the personal data subject, which can be classified into three groups:

(1) The first group: the duties of the personal data controller in relation to the processing of personal data in seven matters as follows:

- Collecting data to the extent necessary;[7]
- Informing the subject about the details regarding personal data processing;[8]
- Processing personal data based on legal grounds;[9]
- Requesting consent for the processing of personal data in the absence of other legal bases or grounds;[10]
- Maintaining records of processing activities;[11]
- Complying with the conditions of personal data collection from third parties;[12]
- Complying with the conditions of personal data transfer to foreign countries.[13]

(2) The second group: the duties relating to the exercise of rights by the personal data subject, that the personal data controller is obligated to assist and facilitate when the data subject requires the exercise of its legal rights.[14]

(3) The third group: the specific legal duties of the personal data controller.

- Maintaining the security of personal data;[15]
- Complying with requirements regarding the transfer of personal data to third parties;[16]
- Establishing a system for examining and editing personal data;[17]
- Appointing a data protection officer;[18]
- Reporting a personal data breach when it occurs.[19]

7 *Personal Data Protection Act, B.E. 2562 (2019), Section 22.*
8 *Ibid., Section 23.*
9 *Ibid., Section 24.*
10 *Ibid., Sections 19 and 24.*
11 *Ibid., Section 39.*
12 *Ibid., Section 25.*
13 *Ibid., Sections 28 and 29.*
14 *See Act's Sections 19, 23 and 30–36.*
15 *Personal Data Protection Act, B.E. 2562 (2019), Section 37 (1).*
16 *Ibid., Section 37 (2).*
17 *Ibid., Sections 35 and 37 (3).*
18 *Ibid., Section 41.*
19 *Ibid., Section 37 (4).*

(b) The relationship between the personal data controller and the personal data processor

In practice, the personal data controller may not always process personal data on his or her own and therefore may assign the processing work to other persons, business organizations, or government agencies, as the case may be. By law, personal data processors do not have a direct contractual or legal connection with the personal data subject. As a result, the personal data controller is required by law to supervise and control the work of the ersonal data processor. The duties of the personal data processor include: following the orders of the personal data controller in the processing of personal data; providing security measures for personal data; and maintaining records of personal data processing activities as assigned.[20]

2.4 Rules on the processing of personal data

The Act prescribes rules for personal data processing throughout the data life cycle, including data collection, usage, disclosure, and erasure or destruction of personal data, starting from evaluating the legal basis or grounds for processing personal data so that it is in accordance with personal data processing activities.[21]

2.5 Penalties and Powers of the Personal Data Protection Authority

Another important aspect of this Act is the penalties and powers of the Personal Data Protection Authority. The penalties for violations are classified into criminal,[22] administrative,[23] and civil.[24] The law also authorizes the Personal Data Protection Committee and the Office of the Personal Data Protection Commission to supervise compliance with the law.

3. APPROACHES TO THE PREPARATION OF FOREIGN PERSONAL DATA PROTECTION GUIDELINES

The drafting of the personal data protection guidelines is new to Thailand. By establishing a good and clear framework which is also consistent with international standards will help encourage the related parties to apply such guidelines effectively. The research team therefore divided a study of foreign guidelines into two aspects: (a) a study of the global legal system of personal data protection; and (b) foreign best practices of personal data protection that are consistent with Thailand's law.

Currently, the world's legal system for personal data protection can be divided into three systems: (a) open model system, as used in the United States; (b) conditional model system, as used

---

[20] *See Personal Data Protection Act, B.E. 2562 (2019), Section 40.*

[21] *Ibid., Part 2, Personal Data Collection; and Part 3, Use or Disclosure of Personal Data.*

[22] *Personal Data Protection Act, B.E. 2562 (2019), Sections 79–81.*

[23] *Ibid., Sections 82–90.*

[24] *Ibid., Sections 77–78.*

Table 2: Data protection law models

Model	Cross-border data flows	Domestic data processing
Open Model	• Self-certification • Self-assessment schemes • Ex-post accountability • Trade agreements and plurilateral arrangements as the only means to regulate data transfers	• Lack of comprehensive data protection framework • Lack of informed consent • Limited sectoral regulations • Privacy as a consumer right
Conditional Model	Conditions to be fulfilled ex-ante, including the adequacy of the recipient country, binding corporate rules, standard contract clauses, data subject consent, codes of conduct and others	• Broad data subject rights • Data subject consent • Right to access, modify and delete personal data • Establishment of data protection authorities or agencies • Privacy as a fundamental human right
Control Model	• Strict conditions including bans to transfer data across borders • Local processing requirements: ad hoc government authorization for data transfer • Infrastructure requirements • Ex-ante security assessments	• Extensive exceptions for government access to personal data • Privacy vs. security and social order

Source: Martina Francesca Ferracane and Erik van der Marel, 2021.

in the European Union and the United Kingdom; and (c) control model system, as used in China and Russia. Each system has different methods for achieving personal data protection, both in terms of cross-border personal data flow and domestic processing of personal data, as shown in Table 2.

Within the abovementioned framework, each approach to personal data protection differs systematically, the research team therefore chose countries that employ the open model system and the conditional model system in order to be consistent with the context of Thailand, which is influenced by the previously mentioned General Data Protection Regulation, or GDPR,[25] an essential basis in the enactment of the Personal Data Protection Act, B.E. 2562 (2019). The researchers also relied on four other factors when selecting countries to study. The factors are as follows: (a) geographical diversity; (b) regulatory diversity; (c) law enforcement experience; and (d) the impact of enforcement. After consideration, the researchers chose to study the personal data protection guidelines of the European Union, Japan, Singapore, the United Kingdom, and the United States. The details of the study are as follows.

[25] *In the draft of the Personal Data Protection Act, B.E. 2562 (2019), the note does not mention that the law is modeled after the European Union's GDPR, but considered in the Minutes of the National Legislative Assembly; it can be seen that the GDPR had a great influence on the drafting of the Act (see National Legislative Assembly, Minutes of the 18/2019 National Legislative Assembly (27 February 2019), 98).*

3.1 National personal data protection legal system of each country

In considering the personal data protection laws of the five countries chosen for the study, the research team found that each country's national personal data protection legal system differs in detail and form of law enforcement. In the European Union, Japan, Singapore, and the United Kingdom, the personal data protection legal system is centralized by stating that their personal data protection law is a general law, thus allowing the law to be applied to any matter or activity that belongs either to either government agencies or private businesses. However, there may be cases where specific regulations may be enacted to provide additional details from the Act, such as the enactment of law for administrative and independent administrative agencies in Japan.

The United States legal system differs from that of other countries because the "Patchwork System"[26] lacks a central law and instead relies on the enforcement of multiple federal and state laws that are distributed among the business regulations in each industry. The Federal Trade Commission Act, for example, regulates the trade and commerce industry, as do state-level personal data protection laws, such as the California Consumer Privacy Act, which regulates the processing of personal data under the law. However, there are loopholes in the supervision because some industries may lack an applicable personal data protection law. Furthermore, many regulations applied to protect personal data have the objective of protecting consumers rather than personal data.

3.2 Consistency between personal data protection laws and the GDPR

A review of the laws of the five sample countries showed that they were all influenced by the GDPR of the European Union. After the promulgation of the GDPR, all five countries were required to amend their laws related to personal data protection to be consistent with the standards set forth by the GDPR. The amendments were made to build confidence with the European Union, which has a larger economy than that of other countries, by establishing a personal data protection policy that is consistent with the European Union and supporting the security of cross-border personal data transfers. One of the evident examples is the case of the United Kingdom, where the Data Protection Act 2018 was enacted in lieu of the former Personal Data Protection Act with the purpose of adapting GDPR criteria into the national legal system since the United Kingdom was also part of the European Union at that time. Other countries have likewise made efforts to align their legal structures and principles with the GDPR.

3.3 Forms of personal data protection guidelines

The study of the forms of the personal data protection guidelines of the five sample countries

[26] *See Heck, Z. S. 2018. "A Litigator's Primer on European Union and American Privacy Laws and Regulations." Litigation 44(2): 59–61. https://www.jstor.org/stable/26402126.*

revealed that they can be classified into three forms: (a) general/concept guidelines; (b) sector-specific guidelines; and (c) topic-specific/activity-based guidelines. The details of each form are shown as follows:

(a) General/concept guidelines of personal data protection

General/concept guidelines of personal data protection collect explanations or advise on issues that are not explicitly stated by the law or secondary laws. The guidelines may also describe specific principles and concepts relevant to personal data protection laws, such as giving key definitions to the term "personal data" or "person" under the personal data protection law, for example. Another significant scope of content is the determination of legal compliance methods under different circumstances, such as consent request method, notification of personal data collection, selection of personal data processing basis, and actions in the event of a personal data breach, and so on. The details are shown in Table 3.

(b) Sector-specific guidelines of personal data protection

The study found that Japan, Singapore and the United States are examples of countries that have developed sector-specific guidelines of personal data protection for business operators in related industries in order to comply with applicable personal data protection laws. Major industries that have established guidelines on personal data protection are public health, telecommunications, education, finance, banking, and credit. The details are shown in Table 4.

(c) Topic-specific/activity-based guidelines of personal data protection

Another form that has been developed is the topic-specific/activity-based guidelines, which take into account the context of personal data use in relation to the processing of personal data in a specific event or matter. For example, the European Union established guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 pandemic, which consider the context of personal data use for medical research as well as the use of location data and tracing tools in accordance with the situation in order to provide personal data protection that is consistent with the effectiveness of epidemic prevention.[27] The research team found that the topic-specific/activity-based guidelines were created to address recently emerged issues or newly developed innovations, thus requiring interpretation or guidance for the processing of personal data in such contexts. The details are shown in Table 5.

However, aside from the three forms as presented above, the study also found that the websites of some sample countries' data protection authorities accommodate users by displaying the guidelines'

[27] *EDPB, 2020, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 3–4, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, accessed April 4,2022.*

Table 3: Comparison of key issues that appear in the general guideline, by country/area

Key issues	European Union	United Kingdom	Singapore	Japan
Data controller and data processor	✓	✓		
Lawful basis	✓	✓		✓
Data subject rights		✓		
Transparency	✓	✓	✓	✓
Data transfer	✓	✓	✓	✓
Consent	✓	✓	✓	✓
Sensitive data or special categories		✓		?
Data protection officer	✓	✓	✓	
Anonymized information		✓	✓	✓
Data breach notification	✓	✓	✓	✓
Data protection impact assessment	✓	✓		
Fines	✓			

Source: Somkiat Tangkitvanich and others, 2021.

Table 4: Comparison of industry guidelines, by country

Industry	Countries		
	Japan	Singapore	United States
Education		✓	✓
Medical and public health	✓	✓	✓
Finance and credit	✓		✓
Telecommunications	✓	✓	✓
Commerce			✓
Transport (CCTV)		✓	
Real estate		✓	
Property management		✓	
Social work		✓	
Insurance		✓	
Labor	✓		

Source: Somkiat Tangkitvanich and others, 2021.

content in an easily accessible format and connecting the information within the website to facilitate research or study of the personal data law in each issue. Furthermore, in some countries, specific contents have been created to assist specific groups of users. In the United Kingdom, for example, the Personal Data Protection Agency's website has specific guidelines or documents relating to small and medium-sized enterprises (SMEs), as well as a self-assessment checklist for people with legal duties to assess the risk in legal compliance or to check their preparedness in following legal rules and conditions, and so on.

In conclusion, a comparative study of foreign personal data protection guidelines found that the five sample countries have different personal data protection laws where they may be enacted as a general data protection laws and sector-specific

Table 5: Overview of topic-specific/activity-based guidelines, by country

Activities	Countries/ areas	Name
COVID-19	Singapore	• Advisories on Collection of Personal Data for COVID-19 Contact Tracing and Use of Safe Entry
	United Kingdom	• Data Protection and Coronavirus Information Hub
	European Union	• Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak • Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak
Online activities	Singapore	• Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Chapter 6: Online Activities
	European Union	• Guidelines 08/2020 on the targeting of social media users • Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects
	United States	**Commerce** • App Developers: Start with Security • Careful Connections: Keeping the Internet of Things Secure • Marketing Your Mobile App: Get It Right from the Start **Education** • Protecting Student Privacy While Using Online Educational Services: Requirement and Best Practices
Photography, video and audio recordings	Singapore	• Advisory Guidelines on the Personal Data Protection Act for Selected Topics – Chapter 4: Photography, Video and Audio Recordings
	European Union	• Guidelines 3/2019 on processing of personal data through video devices

Source: Somkiat Tangkitvanich and others, 2021.

personal data protection laws. These factors affect the nature of guidelines for which a personal data protection guideline may be formulated for specific industries only. In addition, when considering the form of personal data protection guidelines, there are three forms of guidelines: (a) general/concept guidelines; (b) sector-specific guidelines; and (c) topic-specific/activity-based guidelines.

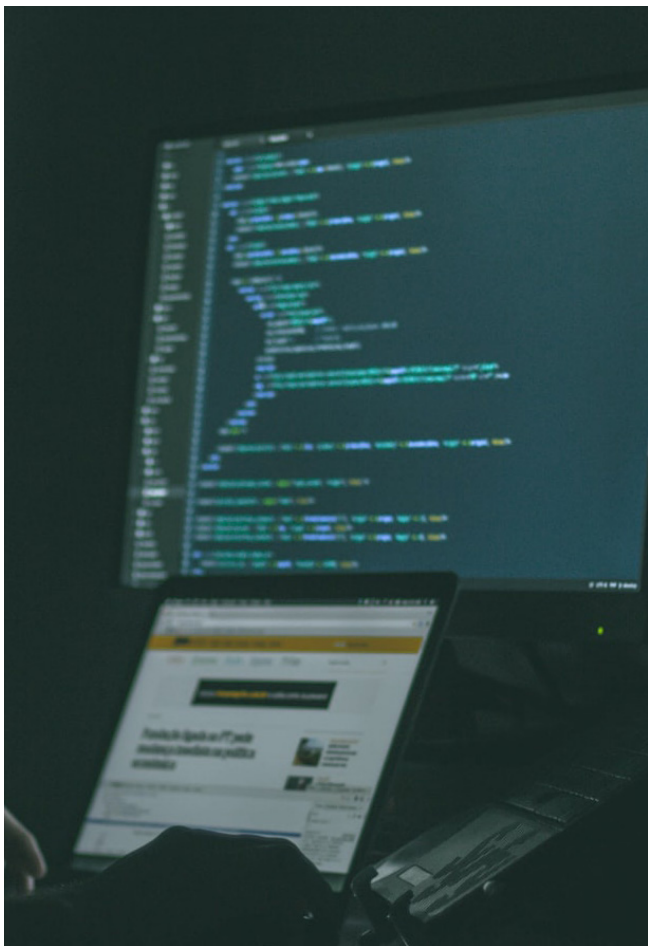
Table 6: Summary of comparison of personal data protection guidelines of sample countries/areas*

Key issues	EU	Japan	Singapore	UK	US
1. Data protection law models					
• Open model					✓
• Conditional model	✓	✓	✓	✓	
2. Status of personal data protection laws					
• Data protection governed by personal data protection law	✓	✓	✓	✓	
• Data protection governed by sectoral law					✓
3. Consistency between personal data protection laws and the GDPR	✓	✓	In the process of improvement	✓	In the process of improvement
4. Types of personal data protection guidelines					
• General guideline/concept guideline	✓	✓	✓	✓	✓
• Sector-specific guideline	-	✓	✓	-	✓
• Topic-specific guideline	✓	✓	✓	✓	✓
• Guideline of SMEs	-	-	-	✓	-
• Checklist / Self-assessment for Complying with Personal Data Protection Law	-	-	-	✓	✓

** Information as of December 14, 2021.*
Source: Modification of information, based on Somkiat Tangkitvanich and others, 2021.

4. APPROACHES TO THE PREPARATION OF GUIDELINES ON PERSONAL DATA PROTECTION OF THAILAND

In order to effectively enforce the Personal Data Protection Act, B.E. 2562 (2019), personal data protection guidelines must be developed to help expand the unclear provisions in the Act, which also lacks a sufficiently clear legal practice guideline for compliance in each situation. As a result, planning for the drafting of guidelines is crucial in order to provide those involved with guidance on how to comply with the law. After analyzing examples of foreign guidelines with Thai personal data protection legal frameworks, the research team drafted a guideline which summarizes the guidelines and factors that must be considered in terms of form and scope of content as follows:



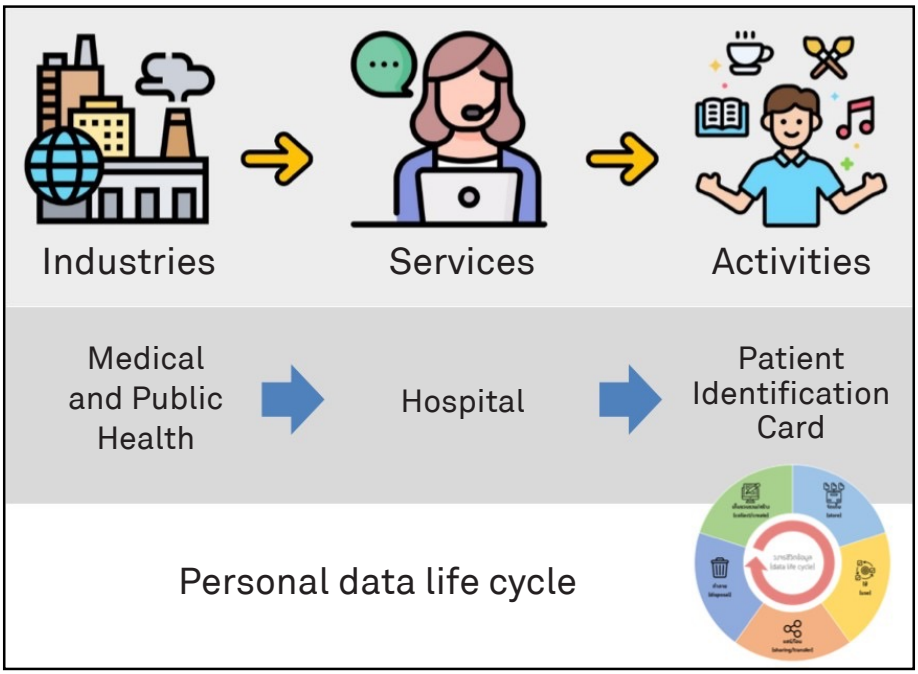
4.1 Forms of personal data protection guidelines

Considering that the enforcement of the personal data protection law has been delayed because of its complexity, the operators with legal duties are not yet ready to comply with the measures prescribed by the law[28] due to the lack of clear guidance for legal compliance; therefore, it is necessary to develop clear guidelines on personal data protection.

In a study on the drafting of guidelines concerning personal data protection for agencies with specific missions or services, the operation should conduct both an industry overview study and a detailed study of personal data processing activities within the organization by conducting detailed analyses at the industry level, services level, and personal data processing activities respectively. The personal data life cycle may be taken into account at the activity level. The details are shown in Figure 1.

[28] *For the first time, the Royal Decree Specifying Data Controllers that are Entities and Businesses not subject to the Personal Data Protection Act, B.E. 2562 (2019), and B.E. 2563, were announced on May 21, 2020; and for the second time, the Royal Decree Specifying Data Controllers that are Entities and Businesses not subject to the Personal Data Protection Act B.E. 2562 (2019) (second edition), B.E. 2564, was announced on May 8, 2021.*

Figure 1: Methodology to develop personal data protection guidelines for certain sectors



Source: Somkiat Tangkitvanich and others, 2021.

4.2 Determining the scope of content of the personal data protection guidelines

Aside from the form, the preparation of the guidelines should take into account the scope of content to be drafted under the guideline development program. The research team conducted the study by dividing the guideline drafts into seven areas: public health; education; real estate and property management; tourism; retail and e-commerce; transportation and logistics; and government agencies. The content is divided into four parts as follows:

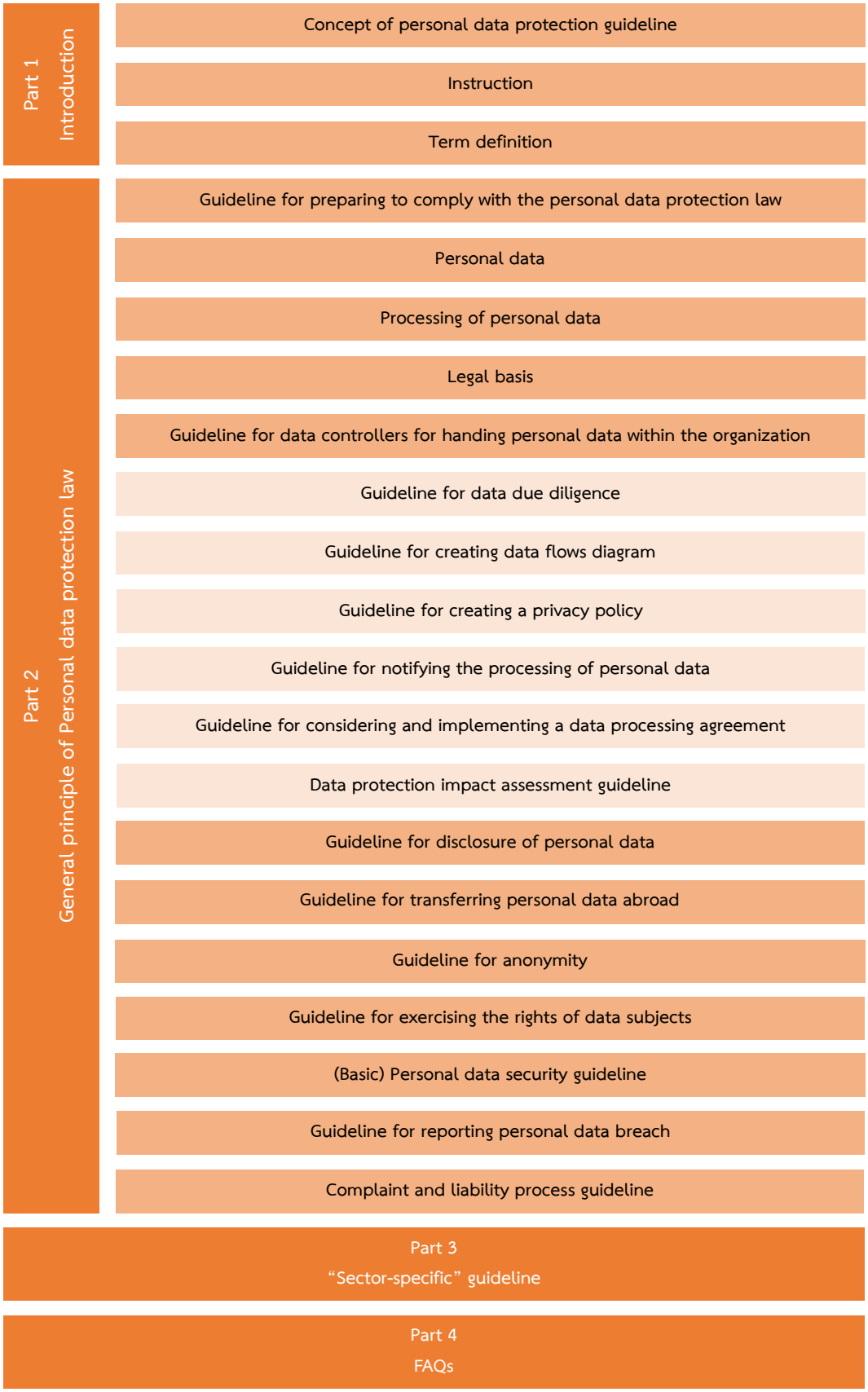
Part 1 Introduction and statement: this part describes the purpose, statements, instructions, and definitions of vocabulary used throughout this guideline;

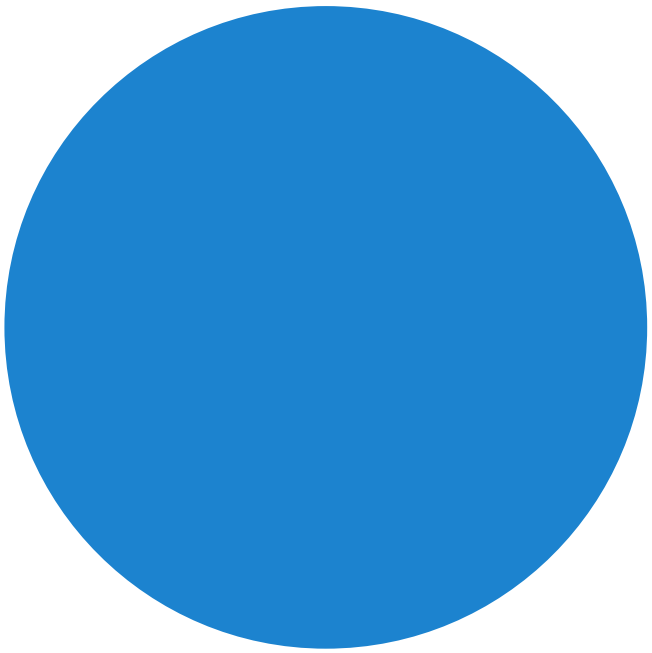
Part 2 General principles: this part explains the principles, procedures, and methods that the relevant parties are required to follow under the Act, such as guidelines for selecting a legal basis for the processing of personal data; guidelines for notifying the processing of personal data; guidelines for disclosure of personal data; guidelines for exercising the rights of personal data subjects; and guidelines for dealing with personal data leaks, among other guidelines;

Part 3 Guideline draft for specific personal data protection activities: this part provides examples of activities that require the processing of personal data and are essential to the agencies with missions or services in each area. The agencies can apply the guidelines from these sample activities to their own internal operations;

Part 4 Frequently Asked Questions (FAQs): this part includes issues and concerns that frequently occur in the context of each agency's operations in their mission or service.

Figure 2: Personal data protection guideline structure





In terms of implementing the four parts of the guidelines draft, the researchers prepared it by taking into account the benefits of the user in order to facilitate the search through the general principles section, the samples of specific personal data protection activities guideline section, and the frequently asked questions section; the user can also study any specific content in the guideline. Moreover, for the benefit of reference, the research team included an index in each paragraph, enabling the user to refer to the guidelines in each paragraph, a method similar to that used in the foreign personal data protection guidelines.

5. SUGGESTIONS

Under this guideline study project, the research team has made a recommendation which is divided into two parts: recommendations on the dissemination of personal data protection guidelines after approval; and other policy recommendations.

5.1 Recommendations on the promulgation of guidelines on personal data protection

As for the recommendations on the dissemination of personal data protection guidelines after approval, the research team's recommendations are divided into two parts: (a) recommendations on the promulgation of personal data protection guidelines; and (b) recommendations on the dissemination of personal data protection guidelines after publication.

(a) Recommendations on the promulgation of the approved personal data protection guidelines

The guidelines on personal data protection are important for compliance with the Personal Data Protection Act, B.E. 2562 (2019). The research team believes that the guidelines should be promulgated, keeping in mind the preparedness of the agencies and the relevant parties; however, the seven areas in the guideline draft proposed by the research team, which are education, public health, tourism, real estate and property management, transportation and logistics, retail and e-commerce, and government agencies, may differ in readiness. Therefore, the research team suggested that the guidelines for each area should be promulgated in the sequence specified in the roadmap. The areas can be classified into three groups as follows:

Group 1 is prepared to comply with the guidelines and their implementation has a significant impact on law enforcement. This group includes

retail and e-commerce, public health, education, and government agencies. This group is designed to benefit the most from the guidelines in terms of clarity of usage, interpretation, and readiness for legal compliance. If the guidelines could be promulgated prior to the enforcement of the law before the end of the first quarter of 2022, they would benefit users who are personal data controllers and personal data processors before the Personal Data Protection Act, B.E. 2562 (2019) comes into force.

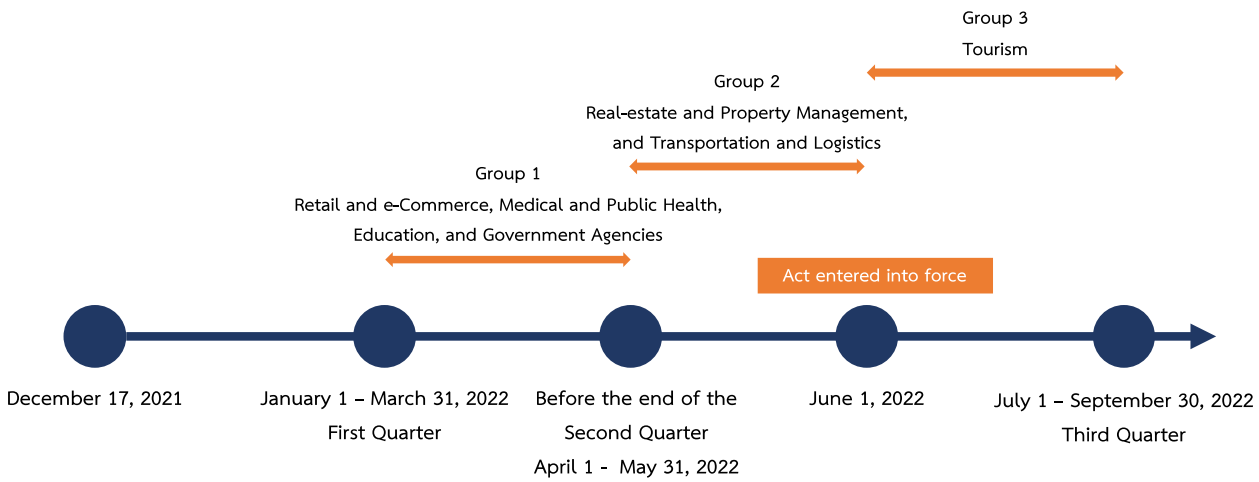
Group 2 is prepared to comply with the guidelines and their implementation has a less significant impact on the enforcement. This group includes real estate and property management, and transportation and logistics. Despite the fact that the guidelines have a significant impact on enforcement and readiness to comply with the Act, in terms of the number of users and the condition of the business, the entrepreneurs with missions or services in this group are mostly medium and large-scale business organizations (except in the case of real estate brokerages in the real estate and property management area); hence the guidelines for this group may be promulgated after the first group, which is during the second quarter before the Act comes into force.

Group 3, the tourism businesses, is less prepared to follow the guidelines and their implementation has a smaller impact on enforcement at this time. The businesses with tourism missions or services are currently experiencing difficulties and impacts caused by the COVID-19 pandemic. As a result, they are unprepared to adhere to the guidelines during this time period. Furthermore, entrepreneurs must concentrate on resolving the problems in the aftermath of the pandemic; thus, in terms of promulgation, this group should be the last, which may be after the Personal Data Protection Act, B.E. 2562 (2019) comes into effect after the postponement of enforcement in the third quarter. To keep the content up to date with the situation following the pandemic, the research team concluded that a meeting with the relevant stakeholders should be held again to determine their current consistency conditions prior to the dissemination of the Guidelines on Personal Data Protection in the tourism business. The discussion includes the details of the secondary regulations that the Personal Data Protection Committee will issue later to clarify the guidelines under the Act. However, the preparation for the implementation of the Act will benefit tourism groups in preparing for the European Union's GDPR, which is a higher standard.

(b) Recommendations on the dissemination of guidelines on personal data protection after promulgation

Following the initial publication of guidelines on personal data protection in all seven areas, the research team believes that the Office of the Permanent Secretary, Ministry of Digital Economy and Society, which currently acts as the Office of the Personal Data Protection Commission, or the next Office of the Personal Data Protection Commission, may consider taking some additional actions to ensure that the established guidelines are effectively enforced.

Figure 3: Timeline to publishing personal data protection guidelines



Source: Somkiat Tangkitvanich and others, 2021.

First, the Office of the Permanent Secretary, Ministry of Digital Economy and Society, which acts as the Office of the Personal Data Protection Commission, may add additional content to the guidelines in seven areas in order to be consistent with the secondary regulations that the Personal Data Protection Commission will further issue.

Second, because the Personal Data Protection Act, B.E. 2562 (2019) is still in the early stages of developing secondary laws and interpretation guidelines, the display of guidelines content on the Office of the Personal Data Protection Commission's website is for the general public as personal data subjects, personal data controllers, and personal data processors, where they can conveniently track the contents of the secondary regulation, interpretation guidelines, and explanations of new issues in the personal data protection law. The website may employ a presentation format similar to that used on the United Kingdom's Information Commissioner's Office website.

5.2 Policy Recommendations

The research team has complied recommendations from various studies on additional topics that will benefit personal data protection in Thailand. The details are as follows:

(a) Guidelines for personal data management on the front of identity cards according to Section 26 of the Personal Data Protection Act, B.E. 2562 (2019)

The researchers recognized practical issues with the use of identity cards and copies due to the fact that religious information is considered personal data (sensitive personal data) under Article 26 of the Act. Once the Personal Data Protection Committee is formed, it may be necessary to consider issuing

secondary regulation to prohibit the use of identity card copies in the identification process in doing transaction. Currently, entrepreneurs strike out the religious information on the identity card copies as a way to conceal it.

The method, however, results in a complex transaction process and procedure due to the fact that entrepreneurs have to employ their personnel to strike out the religious information and recheck whether each copy has been struck out or not. If there is no inspection, it will cause consistency problems in accordance with the law. Furthermore, entrepreneurs, particularly the legal compliance department, oppose this method as it is ineffective at reducing the risk of legal compliance as well as creating difficulties in court citation, and recommend a consent request method instead. As a result, in order to ensure clarity in legal compliance, the researchers were of the opinion that identity cards and copies should be exempted from the enforcement of the law.

(b) Solution to the problem of unclear provisions concerning the exceptions of personal data processing under Article 4 paragraph one (2) of the Personal Data Protection Act, B.E. 2562 (2019)

The research team is of the opinion that the provisions relating to the exceptions in Section 4, paragraph one (2) of the Act should be clarified by requiring that the exemptions from the law apply solely to personal data processing activities and not to all government agencies automatically as stated in the Act that "This Act shall not apply to the operations of public authorities having the duties to maintain state security, including financial security of the state or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cyber security." It is unclear whether the provision intends to exempt all processing activities or the entire performance of that government agency. When compared to the same provisions in the GDPR, the model law used in the drafting of the Act, it is shown that the GDPR provisions describe the nature of the exceptions that are not applied to personal data processing activities in the fields of national security and common security,[29] without the intention of automatically excluding all security-related government agencies. Consequently, the exemption from law enforcement should clearly state that the intention is to exclude personal data processing activities in relation to the purpose, rather than all government entities.

(c) Provisions on exceptions to the processing of personal data under Article 4 paragraph one (2) of the Act

If an amendment cannot be made to Section 4 paragraph one (2) of the Act by clarifying that the characteristic of an activity should be considered, the research team believes that the Office of the Personal Data Protection Commission may be required to specifically establish personal data protection

[29] *GDPR, Recital 16.*

guidelines for government agencies regarding security to clearly define the scope of the nature of security-related activities to be excluded. Some participants in the data collection interviews and small group meetings expressed concern that the provisions still remains unclear, especially when compared to similar provisions in Article 15, paragraph one (1) of the Official Information Act, B.E. 2540 (1997), which focus on security issues in particular.

(d) Restrictions on the enforcement of the Personal Data Protection Act, B.E. 2562 (2019) in conjunction with other legislation

The researchers are of the opinion that, in many cases when considering personal data processing activities, the data was collected not because of the actual need to process personal data but because of legal obligations requiring the personal data controller to comply,[30] such as the collection of personal data by hotels under the Hotel Act, B.E. 2547 (2004),[31] or the collection of patients' personal data under various public health laws.[32] In practice, problems arise in cases where the personal data controller intends to minimize the collection of personal data in accordance with the data minimization principle but is unable to do so because several regulations require agencies to collect personal data even when it is not necessary. For example, while the hotel operator is obligated to report hotel occupancy information to the Department of Provincial Administration under the Ministry of Interior, the law still requires the operator to preserve the guest registration for at least one year to be ready for inspection by government officials.[33]

Furthermore, relying on law enforcement to collect personal data may put the subject's human rights or privacy rights at risk, especially with regard to laws relating to the security of the state and public order in various dimensions,[34] where the state may claim data collection without consent on the basis of state security and arbitrary exercise of power to access personal data and therefore affect the data subject. Although the principles in Thailand's Personal Data Protection Act B.E. 2562 (2019) are congruent with international principles, in practice people may not be fully protected by the Act because of other laws that provide the power to collect personal data. This problem may be related to the international standard issues regarding personal data transfers, which must be secured by countries with personal data protection standards.[35]

The aforementioned restrictions represent the problems with Thailand's implementation of

[30] *Processing of personal data, in which case the data controller uses a legal obligation base to process personal data. See Somkiat Tangkitvanich and others, "Project on Preparing Personal Data Protection Guidelines on Data Controllers and Processors under the Personal Data Protection Act, B.E. 2562 (2019)" (Submitted to the Office of the Permanent Secretary of the Ministry of Digital Economy and Society 2021) Chapter 3.*

[31] *Ibid., Chapter 10.*

[32] *Ibid., Chapter 5.*

[33] *Hotel Act, B.E. 2547 (2004), Section 35.*

[34] *See Kanathip Thongraweewong, Description of the Personal Data Protection Law (คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล) (Nititham (นิติธรรม) 2021):495 and 496.*

[35] *Ibid.*

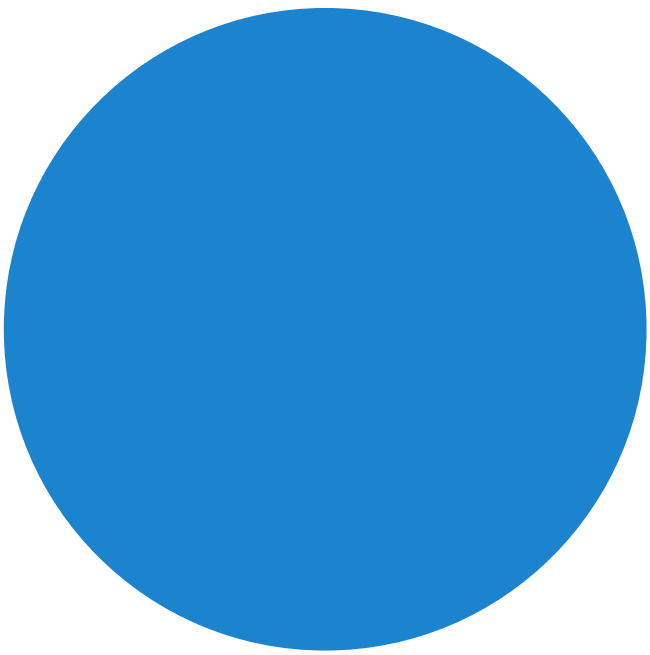
the Personal Data Protection Act B.E. 2562 (2019), which may result in inconsistency with the Personal Data Protection Law's principles and may affect the availability of sufficient international standards for the transfer of personal data between countries.

6. CONCLUSION

The Personal Data Protection Act, B.E. 2562 (2019) is an important Thai primary law that will help raise standards for personal data protection with regard to data controllers and data processors under the law. However, due to the law's complicated nature, it is difficult to comprehend and may impede the operator's compliance. The establishment of appropriate guidelines is very important because it will help clarify the contents for users so that they can apply the law properly to their context.

There is no fixed method for developing good guidelines for complying with personal data protection laws. According to an international study, the guideline models can vary depending on the context and availability of the relevant parties. Previous studies by the Thailand Development Research Institute, however, found that in order to draft good guidelines, it is necessary to consider form, content, and the target audience who are expected to implement the guidelines, so that the guidelines are drafted to meet their actual needs and expectations. Education, real estate, retail, transport and logistics, government agencies, tourism, and hospitals, all of which process large amounts of personal data with various operators but still lack a central agency in the preparation of guidelines, are the groups that have a high demand for such guidelines. Additionally, while developing a good guideline, the activities in which the target audience must engage should be taken into consideration in order for the users to benefit from the guideline's complete execution.

However, after the guidelines have been approved by the relevant agencies, it's necessary to have a proper strategy in terms of time frame and sequence of promulgation to enable the relevant parties to adjust themselves in accordance with the primary law's regulations. All of these factors are critical to the development and promulgation of personal data protection guidelines in Thailand.



REFERENCES

European Data Protection Board (EDPB). 2020. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, accessed April 4, 2022.

Ferracane, Martina Francesca, and van der Marel, Erik. 2021. Regulating Personal Data: Data Models and Digital Services Trade. World Bank, Washington, D.C. https://openknowledge.worldbank.org/bitstream/handle/10986/35308/Regulating-Personal-Data-Data-Models-and-Digital-Services-Trade.pdf?sequence=1&isAllowed=y, accessed April 4, 2022.

Heck, Z. S. 2018. "A Litigator's Primer on European Union and American Privacy Laws and Regulations." Litigation 44(2): 59–61. https://www.jstor.org/stable/26402126.

Kanathip Thongraweewong. 2021. Description of the Personal Data Protection Law (*คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล*), Nititham (*นิติธรรม*).

National Legislative Assembly. 2019. Minutes of the 18/2019 National Legislative Assembly, (27 February).

Somkiat Tangkitvanich and others. 2021. Report on Preparing Personal Data Protection Guidelines on Data Controllers and Processors under the Personal Data Protection Act, B.E. 2562 (2019), submitted to the Office of the Permanent Secretary of the Ministry of Digital Economy and Society.