ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

Thailand

Status of Consent for Processing Personal Data

AUGUST 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTORS

Prof. Thitirat Thipsamritkul

Lecturer, Faculty of Law, Thammasat University

Auradee Wongsaroj

Attorney-at-Law

ACKNOWLEDGEMENTS

Cover photograph by Anil Nallamotu on Unsplash.

This Report benefitted contributions and editing support from Catherine Shen.

DISCLAIMER

Views expressed in this Report are not necessarily those of the Project Lead, the Asian Business Law Institute (ABLI), the Singapore Academy of Law (SAL), or the Future of Privacy Forum (FPF). While every effort has been made to ensure that the information contained in this Report is correct, the Authors, the Project Lead, ABLI, SAL, and FPF disclaim all liability and responsibility for any error or omission in this Report, and in respect of any thing, or the consequences of any thing, done or omitted to be done by any person in reliance, whether wholly or partially, upon the whole or part of the consequences of this Report.

TABLE OF CONTENTS

1. INTRODUCTION

This report summarizes the roles played by consent and related provisions, including alternatives to consent, in Thailand's data protection framework and highlights provisions which can serve as indicators for convergence of laws and regulations in this area across Asia Pacific.

The Personal Data Protection Act ("**PDPA**")[1] – which was passed on May 2019 and took effect on June 1, 2022 – now provides the main requirements under Thai law governing collection, use, and disclosure (collectively, "**processing**"[2]) of personal data by data controllers[3] and data processors.[4]

The key principles of the PDPA are as follows:

- "Personal data" under the PDPA refers to any information pertaining to a person that enables the identification of such a person, whether directly or indirectly, but not including the information of deceased persons.[5]
- The collection of personal data must be limited to the extent necessary to pursue a lawful purpose for processing by the data controller.[6]
- In order to process personal data, a data controller or data processor must satisfy the conditions for one or more of the PDPA's legal bases for processing personal data, which include, but are not limited to, consent.[7]
- The processing of legislatively-defined categories of "sensitive personal data," which include health data and criminal records (among others), is subject to more stringent requirements.[8]
- When a data controller transfers personal data out of Thailand, then by default, the data controller must ensure that the destination jurisdiction has adequate personal data protection standards.[9] However, this requirement does not apply if the data controller obtains the data subject's consent for the transfer, or if another exception applies.

The PDPA also allows for "sectoral standards" in the form of legally binding sector-specific regulations or non-legally binding model forms to specify how notice and consent should be collected in various circumstances.

2. ROLE OF THE PERSONAL DATA PROTECTION COMMISSION ("PDPC")

The PDPA establishes the Office of the Personal Data Protection Commission ("**PDPC**") as a government agency tasked with protecting personal data and encouraging and supporting Thailand's development in the area of personal data protection.[10]

Broadly, Chapter IV of the PDPA provides for the legal status, organization, and mandate of the PDPC, while Chapter V sets out the PDPC's role and powers in investigating and addressing complaints regarding potential non-compliance with the PDPA.

---

[1] The original text in Thai and an unofficial English translation are available on the website of Thailand's Ministry of Digital Economy and Society ("**MDES**").

[2] Note that the PDPA itself does not use the overarching term "processing" and instead distinguishes between collection, use, and disclosure of personal data. However, the PDPA does use the term "data processor" (see below).

[3] A "**data controller**" is defined as a natural or juristic person who has the power and duties to make decisions regarding the collection, use, or disclosure of personal data (PDPA, s 6).

[4] A "**data processor**" is defined as a natural or juristic person who, in relation to the collection, use, or disclosure of personal data, operates according to orders given by or on behalf of a data controller (PDPA, s 6).

[5] PDPA, s 6.

[6] PDPA, s 22.

[7] PDPA, s 24.

[8] PDPA, s 26.

[9] PDPA, s 28.

[10] PDPA, s 43.

The PDPC was fully established in January 18, 2022, when the appointment of its chairperson and members was announced in the Government Gazette. The PDPC held its first meeting on February 10, 2022.[11] Since the PDPA took full effect in June 2022, the PDPC has also issued a number of subordinate regulations and guidelines to facilitate organizations' compliance with the PDPA (see below).

2.1. Subordinate regulations to the PDPA

On June 20, 2022, Thailand's newly constituted PDPC issued a set of four subordinate regulations to the PDPA:

- PDPC Notification Re: Exemption of Data Controllers that are Small Businesses from the Requirement to Record Processing Activities;[12]
- PDPC Notification Re: Rules and Procedures for Data Processors on the Preparation and Retention of Records of Personal Data Processing Activities;[13]
- PDPC Notification Re: Security Measures for Data Controllers;[14]
- PDPC Notification Re: Criteria for Issuing Administrative Penalties by the Expert Committee.[15]

This first set of subordinate regulations does not substantially affect the PDPA's provisions on consent or other legal bases for processing.

However, it is expected that a second set of subordinate regulations will be issued later in 2022 and provide further clarification of the PDPA's consent requirements as consent requirements featured prominently in two rounds of public consultation on draft subordinate regulations to the PDPA (collectively, "**Draft Sub-regulations**") held by Thailand's Ministry of Digital Economy and Society ("**MDES**") between 2021 and early 2022. These public consultations are summarized below.

a. First public consultation on Draft Sub-regulations

From February to September 2021, the MDES held a public consultation on the first of two sets of draft subordinate regulations. The first set was released in three tranches, based on the importance and urgency of issues covered.

Notably, the **first tranche**, released in February 2021, proposed rules and procedures on consent and privacy notices, in addition to other issues, including:

- appropriate measures for processing sensitive personal data,
- cross-border data transfer mechanisms,
- various responsibilities of the data controller,
- security safeguards,
- the requirement to designate a data protection officer, and
- procedures for managing complaints and determining administrative liability.

The **second tranche**, released in June 2021, addressed:

- the scope of the PDPA, including exceptions and derogations from the PDPA,
- cooperation and consistency,
- data subjects' rights,
- responsibilities of data processors, and
- archiving historical records in the public interest, research, and statistics.

---

[11] See press release (in Thai) on MDES's website.
[12] Available in Thai on MDES's website.
[13] Available in Thai on MDES's website.
[14] Available in Thai on MDES's website.
[15] Available in Thai on MDES's website.

The **third tranche**, released in September 2021, addressed:

- codes of conduct,
- data protection impact assessments,
- the data subject's right not to be subject to automated decision-making,
- standards and certifications, and
- international cooperation with foreign regulators and expert communities.

In response to the public consultation, the MDES has released updated drafts of the subordinate regulations in three reports published on its website[16] – however, these have not yet been enacted, and their future remains uncertain.

b. Second public consultation on Draft Sub-regulations

In May 2022, the MDES held a public consultation on the second of two sets of draft subordinate regulations. These drafts contained several proposals for further guidance on specific matters in the PDPA including, notably, draft guidelines on consent ("**Draft Consent Guidelines**")[17] and notification ("**Draft Notification Guidelines**"),[18] as well as proposals to exempt small businesses from certain obligations under the PDPA, and provide rules on record-keeping in relation to processing activity and security measures.

As discussed above, PDPC has since enacted and issued a first round of subordinate regulations which – notably – covered all matters raised in the May 2022 public consultation, except for consent and notification. It is therefore expected that PDPC will release subordinate regulations based on the Draft Consent Guidelines and Draft Notification Guidelines in the coming months.

2.2. PDPC Guidelines

As of the date of this report, the PDPC has issued two sets of guidelines to facilitate understanding of and compliance with the PDPA, now that the PDPA has fully taken effect:

- PDPA Guide for Small and Medium Enterprises ("**SMEs**"), published on June 22, 2022;[19] and
- PDPA Guide for Citizens, published on June 23, 2022.[20]

Both sets of guidelines briefly summarize core concepts under the PDPA, such as personal data and the distinction between data subjects, data controllers, and data processors.

The PDPA Guide for SMEs provides an overview of key obligations in relation to the collection, use, and disclosure of personal data, brief examples of how small businesses may comply with these obligations in practice, and more detailed guidance on compliance with record-keeping and security obligations under the PDPA and the recently enacted first round of subordinate regulations.

By contrast, the PDPA Guide for Citizens provides a high-level summary of key topics in the PDPA, including notification, consent, and data subject rights, and outlines examples of how key requirements in the PDPA would apply in everyday scenarios, such as sharing photographs and videos containing personal data on social media.

---

[16] The three reports, titled "Documents of the results of the hearing on the first group of draft subordinate regulations" ("**Group 1 Report**"), "Documents of the results of the hearing on the second group of draft subordinate regulations" ("**Group 2 Report**"), and "Documents of the results of the hearing on the third group of draft subordinate regulations" ("**Group 3 Report**"), are available in Thai on MDES's website.

[17] "Memorandum of Principles and Reasons of the Personal Data Protection Committee for the Implementation of Guidelines and Procedures for Obtaining Consent from Data Subjects" ("**Draft Consent Guidelines**"), available in Thai on MDES's website.

[18] "Memorandum of Principles and Reasons of the Personal Data Protection Committee for the Implementation of Guidelines and Procedures Regarding the Purpose and Details of Collection, Use and Disclosure of Personal Data" ("**Draft Notification Guidelines**"), available in Thai on MDES' website.

[19] Available in Thai on MDES's website.

[20] Available in Thai on MDES's website.

3. SECTORAL LAWS AND REGULATIONS

In addition to the PDPA, several other laws and regulations provide for protection of personal data in specific contexts. On the interaction between these laws and regulations and the PDPA, Section 3 of the PDPA provides that any other law which provides for the protection of personal data takes precedence over the PDPA, except in relation to the PDPA's requirements as to collection, use, and disclosure of personal data.

In the public sector, the Official Information Act (1997),[21] which governs citizens' access to government data, contains several specific provisions (especially those in Chapter III) on retention and disclosure of personal data by government entities. Section 24 of this Act prohibits a government entity from disclosing personal data under its control to another government entity or person without the consent of the data subject, subject to certain exceptions.

In the healthcare sector, the National Health Act (2007)[22] requires that "personal health information" must be kept confidential and may not be disclosed to a third party without the data subject's consent unless required by law.[23] The Act also requires medical professionals to obtain patients' informed consent before involving them in medical research.[24] Non-compliance with either of these requirements is an offense punishable with up to 6 months' imprisonment and/or a fine of up to THB 10,000.[25]

In the financial sector, the Financial Institution Business Act (2008)[26] and the Payment System Act (2017)[27] prohibit financial institutions and their officers from disclosing a customer's confidential information without the customer's consent.[28] Breach of these requirements is an offense punishable with imprisonment for up to one year and/or a fine of up to THB 100,000. Further, the Credit Information Business Act (2002)[29] requires a credit information company to obtain a member's prior written consent before disclosing information relating to the member to a third party for the purpose of credit analysis or issuing a credit card, subject to exceptions.[30]

4. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE PDPA

Consent is one of several, equal bases for processing personal data under the PDPA. The PDPA Guide for Citizens clarifies that consent is not required where a data controller can rely on an alternative legal basis.[31]

The PDPA prohibits a data controller from collecting personal data, unless the data controller either obtains the data subject's consent or satisfies the conditions for at least one of the six alternative legal bases for collecting personal data. The relevant provisions are as follows:

- Section 19 of the PDPA prohibits a data controller from collecting, using, or disclosing personal data without the data subject's consent, except where the processing is permitted under the PDPA or any other law. Section 19 also requires that consent must be obtained prior to or at the time of collection, use, or disclosure of the personal data in question.
- Section 24 of the PDPA provides six alternative legal bases for collecting personal data without the data subject's consent. These bases are similar to those provided by Article 6(1) of the GDPR.

---

[21] The original text in Thai and an English translation are available on the website of Thailand's Parliament.
[22] The original text in Thai and an English translation are available on the website of Thailand's National Health Commission.
[23] National Health Act, s 7.
[24] National Health Act, s 9.
[25] National Health Act, s 49.
[26] The original text in Thai and an unofficial English translation are available on the Bank of Thailand's website.
[27] The original text in Thai and an unofficial English translation are available on the Bank of Thailand's website.
[28] Financial Institution Business Act, s 154(8); Payment Services Act, s 54.
[29] The original text in Thai and an unofficial English translation are available on the Bank of Thailand's website.
[30] Credit Information Business Act, s 20.
[31] PDPA Guide for Citizens, page 13.

- Section 26 of the PDPA requires a data controller to obtain the "explicit consent" of the data subject for processing of certain classes of sensitive personal data, unless the data controller fulfills the conditions for an alternative legal basis for processing sensitive personal data, which are generally stricter than those under Section 24 of the PDPA.
- Section 27 of the PDPA prohibits a data controller from using or disclosing personal data without the data subject's consent unless the data was validly collected under Section 24 or Section 26 of the PDPA.

By default, personal data may only be collected, used, or disclosed for a purpose that has been notified to the data subject before or at the time of data collection.[32] If a data controller wishes to collect, use, or disclose personal data for a different purpose, the data controller must inform the data subject of this new purpose, and obtain fresh consent prior to collecting, using, or disclosing the personal data for the new purpose, unless an exception in the PDPA or another law applies.[33]

Further, data controllers are ordinarily required to collect personal data directly from the data subject. However, the PDPA permits collection of personal data about the data subject from a source other than the data subject himself/herself if the data controller informs the data subject of the collection from other sources without delay (i.e., within thirty days of the date of collection) and obtains consent from the data subject.[34]

5. CONDITIONS FOR CONSENT

5.1. Definition and forms of consent

a. PDPA

The PDPA does not define "consent" or elaborate on the forms that valid consent may take, save that consent for processing of sensitive personal data must be "explicit."[35]

However, Section 19 of the PDPA does specify in detail the requirements for a *request for consent* to be considered valid. Such a request must be:

- explicitly made in a written statement or via electronic means, unless this its not possible due to the nature of the request;
- accompanied by information on the purpose of the collection, use, or disclosure of the personal data; and
- presented in a manner that clearly distinguishes the request for consent from any other matters, in an easily accessible form which uses clear and plain language and is not deceptive or misleading to the data subject.

A request for consent which does not comply with these requirements has no binding effect on the data subject and will not permit the data controller to collect, use, or disclose personal data.

Section 19 anticipates that the PDPC may require personal data controllers to apply for data subjects' consent using a prescribed form and statement. Although the PDPC has not prescribed any particular forms to date, it is possible that in future, the PDPC may prescribe a standard form or, at least for certain industries, permit a sectoral regulator or industry body to do so (see below).

b. PDPA Guidelines

The PDPA Guide for Citizens clarifies that consent given in response to a request under Section 19 of the PDPA must be clear, unambiguous, and free in the sense that the data subject had an opportunity to make a genuine choice.[36]

---

[32] PDPA, s 21.
[33] PDPA, s 21.
[34] PDPA, s 25(1).
[35] PDPA, s 26.
[36] PDPA Guide for Citizens, pages 4-5; Draft Consent Guidelines, page 3.

c. Draft Sub-regulations

In both rounds of public consultation on the Draft Sub-regulations, the MDES proposed allowing sectoral regulators to determine mandatory consent forms for their respective sectors and encouraging industry groups and associations to develop non-binding, voluntary standards for consent forms to facilitate businesses' compliance with the PDPA.[37]

The Draft Consent Guidelines propose further clarifying the requirements for valid consent under Section 19 of the PDPA by expressly requiring that unless there is any specific law to the contrary, consent must be informed and freely given, in the sense that it was not obtained through fraud, deception, intimidation, or misrepresentation.[38]

The Draft Consent Guidelines propose that consent should be regarded as "informed" if prior to collection, use, or disclosure of the personal data, the data subject was provided with the information required under Section 23 of the PDPA.[39] The Draft Consent Guidelines add that notification of the purpose for the collection, use, or disclosure of the personal data could be made by a number of different means, including electronically, verbally, or in writing.

As to the forms that valid consent could take, the Draft Consent Guidelines appear to recognize a wide range of different forms, including mouse-clicks or keystrokes on a website and use of biometrics (including in conjunction with Internet-of-Things devices).[40] However, it remains to be seen if the PDPC will adopt such an approach in practice, as the Draft Consent Guidelines have not yet been enacted.

5.2. Withdrawal of consent

Section 19 of the PDPA provides that data subjects may withdraw their consent at any time and requires that the procedure for withdrawing consent must be no more difficult than that which the data controller initially employed to obtain consent from the data subject. This is subject to any limitation of the right to withdraw consent, whether in another law or in a contract which gives benefits to the data subject.

The PDPA Guide for Citizens[41] clarifies that withdrawal of consent may take any form (e.g., electronic, written, etc.) provided that it is clear and easy to understand. The Guide also requires that the data subject must be informed of the impact to him/her if he/she withdraws consent and that if the data subject then proceeds to withdraw consent, the data controller must cease processing of the personal data in question.

The Draft Consent Guidelines propose to introduce a further requirement that the method, conditions, and form for withdrawing consent must be clearly and prominently stated in the written or electronic request for consent.[42]

5.3. Bundled consent

Section 19 of the PDPA requires that a request for consent must not be deceptive or misleading as to the data controller's purpose for collecting, using, or disclosing the personal data in question. This provision appears to prohibit the practice of "bundling consent."

Section 19 further requires that a contract for provision of a service may not make the giving of consent for the collection, use, or disclosure of personal data a condition for provision of the service, if the personal data in question is unnecessary for, or irrelevant to, conclusion of the contract or provision of the service.

---

[37] Group 1 Report, pages 4-5.
[38] Draft Consent Guidelines, page 3.
[39] Draft Consent Guidelines, page 5. As to the information to be provided under Section 23 of the PDPA, see "TRANSPARENCY AND NOTICE" below.
[40] Draft Consent Guidelines, page 7.
[41] PDPA Guide for Citizens, page 7.
[42] Draft Consent Guidelines, page 6.

6. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

6.1. PDPA

Section 26 of the PDPA prohibits collection of "sensitive person data" unless the data controller obtains explicit consent from the data subject or satisfies the conditions for another legal basis for collecting sensitive personal data.[43]

The classes of sensitive personal data identified in Section 26 of the PDPA comprise personal data pertaining to ethnicity, race, political opinions, doctrinal, religious or philosophical beliefs, sexual behavior, criminal records, health records, disability, labor union information, genetic information, biological information, or any data which may affect the data subject in a manner prescribed by the PDPC.

Additionally, Section 26 of the PDPA provides that collection of personal data with respect to criminal records must be done under the control of the competent authorities under the law, or with measures to protect the personal data pursuant to rules prescribed by the PDPC. As of the date of this report, draft subordinate regulations on processing of criminal record data have been released for public consultation (see below) but have not yet been enacted.

6.2. Draft Sub-regulations

The Draft Sub-regulations propose that data controllers should only be permitted to process a data subject's criminal record data during recruitment procedures if a criminal record check is required by law or if the data subject explicitly consents in writing to such processing.[44]

The Draft Sub-regulations further propose that where a data controller seeks consent for processing of criminal record data, the data controller must state in the recruitment announcement whether a criminal record check is significantly necessary and if so, what the consequences of failing to consent to a criminal record check would be.[45] The PDPC has also indicated that it may issue guidance in relation to the employment positions for which conducting a criminal record check during recruitment procedures would be considered significantly necessary.[46]

6.3. Children

Section 26 of the PDPA does not classify children's data as sensitive personal data. However, Section 20 of the PDPA establishes requirements regarding the personal data of minors, i.e., persons under the age of 20 who are not *sui juris* by marriage or have no capacity as a *sui juris* person under Section 27 of the Civil Commercial Code.

A data controller must seek consent from a person who exercises parental responsibility over the minor and has the power to act on behalf of the minor if:

- the minor is not entitled to act alone in giving consent pursuant to Section 22, Section 23, or Section 24 of the Civil Commercial Code, or
- the minor is aged 10 years or below.

The Draft Consent Guidelines propose further clarifying the PDPA's consent requirements in relation to minors' personal data.[47]

Specifically, the Guidelines would require data controllers to implement appropriate and reliable measures to verify the age of the minor and, where necessary, the age and identity of the person exercising parental responsibility over the minor and keep appropriate records. Further, if the data

---

[43] See "Collecting, using, and disclosing sensitive personal data without consent" below.
[44] Group 1 Report, page 15.
[45] Group 1 Report, page 15.
[46] Group 1 Report, page 15.
[47] Draft Consent Guidelines, pages 8-9.

controller requests consent from a person exercising parental responsibility over the minor, then the Draft Consent Guidelines propose that the request should be in clear and intelligible language. Finally, the Draft Consent Guidelines propose explicitly stating that the PDPA's requirements as to capacity to consent and withdrawal of consent also apply to consent to processing of a minor's data which has been obtained from a person exercising parental authority over the minor.

Note that the first round of Draft Sub-regulations also proposed requiring data controllers to undertake a data protection impact assessment before profiling or marketing online services directly to minors.[48]

6.4. Cookies, Internet of Things, online tracking

Section 26 of the PDPA does not categorize cookies, Internet of Things, or online tracking to be sensitive personal data.

6.5. Direct marketing

The PDPA does not contain specifics provisions on direct marketing. However, note that the Computer Crime Act (2007) (as amended in 2017)[49] prohibits sending computer data without opt-out/unsubscribe functions.

6.6. Biometric and genetic data

Biometric and genetic data both fall within the scope of sensitive data under Section 26 of the PDPA. Section 26 of the PDPA defines "biometric information" as personal data arising from the use of techniques or technology related to the physical or behavioral traits of a person that can be used to confirm the person's identity, such as facial model data, iris model data, or fingerprint model data.

Note also that the first round of Draft Sub-regulations proposed requiring data controllers to undertake a data protection impact assessment before processing biometric or genetic data.[50]

6.7. Financial information

Section 26 of the PDPA does not categorize financial information as sensitive personal data.

6.8. Pseudonymized data

The PDPA does not provide specific requirements for pseudonymized data.

6.9. Location data

The PDPA does not provide specific requirements for location data and does not categorize location data as sensitive personal data.

However, note that the first round of Draft Sub-regulations proposed requiring data controllers to undertake a data protection impact assessment before tracking users' locations.[51]

7. CONSENT FOR CROSS-BORDER DATA TRANSFERS

Under Section 28 of the PDPA, the default requirement for transferring personal data outside of Thailand is that the destination jurisdiction or receiving international organization must have sufficient

---

[48] See "COLLECTING, USING, AND DISCLOSING PERSONAL DATA SUBJECT TO A RISK IMPACT ASSESSMENT" below.

[49] Available in Thai on the website of the Government Gazette.

[50] See "COLLECTING, USING, AND DISCLOSING PERSONAL DATA SUBJECT TO A RISK IMPACT ASSESSMENT" below.

[51] See "COLLECTING, USING, AND DISCLOSING PERSONAL DATA SUBJECT TO A RISK IMPACT ASSESSMENT" below.

personal data protection standards, and the transfer must be conducted in accordance with the rules for the protection of personal data prescribed by the PDPC pursuant to Section 16(5) of the PDPA.

Section 28 of the PDPA further provides that in the event that there is a problem with regard to the adequacy of the destination jurisdiction or receiving international organization that receives personal data, the problem must be submitted to PDPC for determination. PDPC's decision is subject to review when there is new evidence to believe that the destination jurisdiction or receiving international organization has developed sufficient personal data protection standards.

Consent functions as one of six exceptions to the default rule in Section 28 of the PDPA. Compared with the general consent requirements in Section 19 of the PDPA, the only specific requirement for consent for cross-border transfers of personal data under Section 28 is that the data controller must give prior notice to the data subject that the destination country or receiving international organization has insufficient personal data protection standards compared to those in the PDPA.

8. TRANSPARENCY AND NOTICE

8.1. PDPA

Section 23 of the PDPA requires a personal data controller to provide the data subject with the following information prior to or at the time of data collection (unless the data controller can prove that the data subject is already aware of the information):

- the purpose of the collection, use, or disclosure of the personal data, including, where applicable, the purpose under Section 24 for collecting personal data without the data subject's consent;[52]
- whether the data subject will be required to provide his/her personal data to comply with a relevant law or a contract, or whether it is necessary for the data subject to provide the personal data to conclude a contract, and the possible effect if the data subject does not provide the personal data;[53]
- the personal data to be collected and the time period during which the data will be retained;[54]
- the categories of persons or agencies to whom the collected personal data may be disclosed;[55]
- contact information of the data controller and its representative or data protection officer, including address and means of contact;[56] and
- the data subject's rights under the PDPA to withdraw consent, access his/her personal data, have his/her personal data rectified, suspend the use of his/her personal data, object to the use of his/her personal data, have his/her personal data erased, and lodge complaints, as well as the right to data portability.[57]

Additionally, where there is a change in the purpose for collecting, using, or disclosing personal data, Section 21 of the PDPA requires the data controller to inform the data subject of the new purpose and obtain fresh consent to collect, use, or disclose the data for the new purpose.

By default, the above requirements apply whether the data subject's personal data is collected from the data subject directly or from a third party.[58]

However, where personal data is collected from a third party, Section 25 of the PDPA provides a number of exceptions to the above requirements. These exceptions apply where:

- the data subject has acknowledged the new purpose or details;

[52] PDPA, s 23(1).
[53] PDPA, s 23(2).
[54] PDPA, s 23(3),
[55] PDPA, s 23(4).
[56] PDPA, s 23(5).
[57] PDPA, s 23(6).
[58] PDPA, ss 23 and 25.

- the data controller can prove that the notice of the new purpose or details cannot be given or will be an obstacle to the use or disclosure of the personal data, particularly in order to achieve a purpose with respect to scientific, historical, or statistical research;
- it is necessary to use or disclose the personal data on an urgent basis pursuant to a legal requirement, and appropriate measures have been provided to protect the interests of the data subject;
- the personal data controller is aware of, or acquires, such personal data from his/her duty or occupation or profession and keeps confidential the new or specific purposes or details, as required by law.[59]

8.2. Draft Sub-regulations

The Draft Sub-regulations propose certain clarifications as to the notification requirements under the PDPA, outlined below.

a. Notification of the purpose of processing

The first round of Draft Sub-regulations proposed explicitly stating that whatever the legal basis that the data controller relies on to collect personal data, the data controller must provide a notification of the purpose for processing data unless the data controller can prove that an exception under Section 23 or 26 of the PDPA applies.[60]

This round of Draft Sub-regulations also proposed clarifying the formal requirements for a notification of the purpose of processing. Specifically, such a notification would have to be drafted in a way that is easy for the data subject to understand, taking into account the specific circumstances of the data subject in question, and that would enable the data subject to anticipate and understand the impact of processing.[61] To that end, the Draft Sub-regulations recommend that data controllers minimally consider the following factors:

- the completeness of the purposes of data processing;
- the ease of understanding the purposes of data processing;
- ways of bringing the data subject's attention to the purposes of processing;
- whether the data controller should adopt a standardized approach to giving the notifications in relation to its goods and/or services; and
- consistency in the context of how notifications are given, to ensure that data subjects can more easily understand the information and make decisions more efficiently.[62]

The Draft Sub-regulations also recommended that data controllers should document their consideration of these factors.[63]

In the second round of Draft Sub-regulations, the Draft Notification Guidelines, reiterated the above proposals and recommended adding a clarification that the notification of purpose:

- could be made via a number of different formats, including the data controller's privacy policy or another notification to the data subject concerning collection, use, or disclosure of his/her personal data;[64] and
- would have to explicitly identify the specific lawful purpose and the legal basis for processing the personal data.[65]

---

[59] PDPA, s 25
[60] Group 1 Report, page 9.
[61] Group 1 Report, pages 8-9.
[62] Group 1 Report, page 9.
[63] Group 1 Report, page 9.
[64] Draft Notification Guidelines, page 3.
[65] Draft Notification Guidelines, page 4.

b. Notification of data collection

The Draft Sub-regulations propose that data controllers should be required to provide details of the personal data that will be collected in a manner that would be easy for data subjects to understand and that would enable data subjects to reasonably anticipate the types of information that would be collected.[66]

If possible, and provided that the interests of data controllers or data processors are not unreasonably affected, data controllers would have to provide the following information:

- the group of data subjects, e.g., employees, clients, business partners, from whom data is collected.;
- the purposes for which the data is used;
- the frequency of data collection;
- the qualitative and quantitative precision of the data; and
- other details which may affect the data subject's expectation as to the effect of processing on the his/her rights and freedoms.[67]

If it is not possible to specify how long collection will take, data controllers would have to prove that the time specified is strictly necessary for those purposes — i.e., the time it takes to process personal data in attainment of the purposes notified to the data subjects.

c. Notification of disclosure

The Draft Sub-regulations propose that data controllers would also have to identify the types of persons or entities to which collected data might be disclosed.

If explicit identification is possible, data controllers would have to clearly identify to the data subjects the persons or agencies to whom collected data might be disclosed. If explicit identification is not possible, data controllers would have to provide adequate information on the profile of the persons or agencies to whom the data may be disclosed, so that data subjects can reasonably anticipate the types of information that may be disclosed to such persons or agencies.

d. Change in the purpose of processing

The Draft Sub-regulations propose that a data controller should bear the burden of proving that a notification of a change in the purpose of processing was transparent, understandable, and accessible to the data subject.[68] Minimally, the data controller would have to provide the following information:

- the difference between the original and new purposes;
- the content of the previous notification of purpose;
- the legal basis under Sections 24 or 26 of the PDPA for processing the personal data;
- the potential impact on the rights and freedoms of the data subject from the new purpose;
- the potential benefits to stakeholders, including the data subject and the controller of personal data, of processing the personal data for different purposes;
- the date and/or time when processing for the new purpose will begin.[69]

e. Change in the purpose of processing for scientific, historical, or statistical purposes

The Draft Sub-regulations propose that the following factors should be taken into account in determining whether a data controller has notified the data subject of a change in the purpose of processing, where the new purpose is for scientific, historical, or statistical research:

---

[66] Group 1 Report, page 10.
[67] Group 1 Report, page 10.
[68] Group 1 Report, page 7.
[69] Group 1 Report, page 7.

- whether the new purpose is related to the previous purpose;
- the context of data collection, including the relationship between the data controller and the data subject, and reasonable expectations of the data subject;
- the qualities of the personal data, including whether it falls under the categories of sensitive personal data;
- the effect on the data subject and relative benefits to society from processing for the new purpose; and
- the nature and suitability of measures in place to protect the personal data.[70]

f. Proposed exemptions from notification requirements

The Draft Sub-regulations also propose to exempt data controllers from certain notification obligations if:

- compliance with these obligations would undermine the purpose of processing the personal data in question;
- the personal data in question is processed for the purpose of exercising or defending a legal claim;
- the data controller is a legal professional who is subject to a legal duty to maintain confidentiality and is advising or taking action on behalf of a client; or
- the personal data in question is processed for the purpose of marking examination scripts.[71]

9. SANCTIONS AND ENFORCEMENT

Generally, data controllers and data processors that fail to comply with the requirements of the PDPA may be subject to:

- civil liability;[72]
- criminal penalties, which may include an imprisonment for a period of up to 1 year, and/or fines not exceeding THB 1,000,000; [73] and/or
- administrative fines, ranging from THB 500,000 to THB 5,000,000.[74]

9.1. Criminal liability

It is a criminal offense under the PDPA for a data controller to use or disclose sensitive personal data without the data subject's consent in violation of Section 27 of the PDPA.

If the data controller uses or discloses sensitive personal data in a manner that is likely to cause the other person to suffer any damage, impair his/her reputation, or expose the person to scorn, hatred, or humiliation, then the data controller faces imprisonment of up to 6 months and/or a fine of up to THB 500,000.[75]

If the data controller uses or discloses sensitive personal data in order to unlawfully benefit himself/herself, or another person, then the data controller faces imprisonment for up to 1 year and/or a fine of up to THB 1,000,000.[76]

9.2. Administrative liability

A data controller who fails to:

---

[70] Group 1 Report, page 8.
[71] Group 2 report, pages 10-11.
[72] See, generally, PDPA, Chapter VI.
[73] See, generally, PDPA, Chapter VII, Part I.
[74] See, generally, PDPA, Chapter VII, Part II.
[75] PDPA, s 79.
[76] PDPA, s 79.

- provide information to the data subject pursuant to Sections 23 or 25(2) of the PDPA;
- obtain consent using a form or statement prescribed by the PDPC under Section 19 of the PDPA; or
- notify the data subject of the effect of withdrawal of consent under Section 19 of the PDPA

faces an administrative fine of up to THB 1,000,000.[77]

Further, a data controller who:

- collects personal data without obtaining the data subject's consent or satisfying the conditions for another legal basis for collecting personal data under the PDPA;
- collects data from a source other than the data subject without notifying the data subject and/or obtaining the data subject's consent;
- uses or discloses personal data without the data subject's consent; or
- obtains consent by deceiving or misleading the data subject about the data controller's purpose for processing the data subject's personal data

faces an administrative fine of up to THB 3,000,000.[78]

Finally, a data controller who collects sensitive personal data without explicit consent or a valid legal basis under Section 36 of the PDPA faces an administrative fine of up to THB 5,000,000.[79]

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

The PDPA's provisions on the legitimate interests basis are substantially similar to their equivalent in Article 7(1)(f) of the GDPR.

Under the PDPA, a data controller may collect personal data without the data subject's consent if such collection is necessary for the legitimate interests of the data controller or any other person, except where such interests are overridden by the fundamental rights of the data subject in relation to his/her personal data.[80]

Where a data controller has collected personal data on the basis of a legitimate interest, the data controller does not need to obtain consent to use or disclose that personal data for a purpose specified at the time of data collection.[81] However, in this situation, the data controller would be required to retain a record of the use or disclosure containing certain prescribed details for review by the data subject or the PDPC.[82]

There are currently no guidelines or subordinate regulations on how to interpret or apply the legitimate interests basis in practice.

However, note that the first round of Draft Sub-regulations proposed guidance on the circumstances in which the PDPC may require data controllers to undertake a data protection impact assessment ("**DPIA**") in future.[83]

Specifically, the Draft Sub-regulations proposed requiring data controllers to undertake a DPIA before any processing of personal data that: (1) uses new technologies or is likely to present a significant risk to the rights and freedoms of data subjects; and (2) has been notified as such by the PDPC. The proposed categories of processing activities that present a significant risk to the rights and freedoms of the data subject include:

- processing of personal data using new technologies such as artificial intelligence);

---

[77] PDPA, s 82.
[78] PDPA, s 83.
[79] PDPA, s 84.
[80] PDPA, s 24(5).
[81] PDPA, s 27.
[82] PDPA, ss 27 and 39.
[83] Group 3 Report, pages 9-13.

- use of profiling or sensitive data to deny access to services;
- mass profiling of individuals;
- processing of biometric or genetic data;
- combining link data or datasets from multiple sources;
- collecting personal data from sources other than the data subject directly without giving notice to the data subject;
- tracking of a person's location or behavior;
- profiling or targeting marketing or online services directly to minors or vulnerable persons;
- processing of information that may jeopardize the health or safety of individuals if made public.

Under these proposals, data controllers would also be required to publish a document containing the results of the DPIA and make this document accessible to the public by reasonable means, redacting only confidential information.

11. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

11.1. Collecting, using, and disclosing personal data without consent

Personal data other than sensitive personal data may be collected without consent where collection of personal data is:

- for achieving a purpose relating to the preparation of historical documents or archives for public interest, or for the interests of education, research, or statistics, provided that the data controller implements measures prescribed by the PDPC to protect the rights and liberty of the data subject;[84]
- for preventing or suppressing danger to a person's life, body, or health;[85]
- necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;[86]
- necessary for the performance of a task carried out in the public interest by the data controller, or it is necessary for the exercising of official authority vested in the data controller;[87]
- necessary for the legitimate interests of the data controller or of persons or legal entities other than the data controller, except where such interests are overridden by the fundamental rights of the data subject in his/her personal data;[88] or
- necessary for compliance with a law to which the personal data controller is subject. [89]

Where a data controller has collected personal data pursuant to any of the foregoing legal bases, the data controller would not be required to obtain consent to use or disclose that personal data for a purpose specified at the time of data collection.[90] However, in this situation, the data controller would be required to retain a record of the use or disclosure containing certain prescribed details for review by the data subject or the PDPC.[91]

---

[84] PDPA, s 24(1).
[85] PDPA, s 24(2).
[86] PDPA, s 24(3).
[87] PDPA, s 24(4).
[88] PDPA, s 24(5).
[89] PDPA, s 24(6).
[90] PDPA, s 27.
[91] PDPA, ss 27 and 39.

11.2. Collecting, using, and disclosing sensitive personal data without consent

Sensitive personal data may be collected without explicit consent where data collection is:[92]

- to prevent or suppress a danger to a person's life, body, or health, where the data subject is incapable of giving consent by whatever reason;
- carried out:
  - in the course of legitimate activities of a foundation, association, or not-for-profit body with a political, religious, philosophical, or trade union purpose,
  - for the members or former members of such a body, or for persons having regular contact with such foundations, associations or not-for-profit bodies
  - in connection with their purposes,
  - with appropriate safeguards, and
  - without disclosing the personal data outside of such foundations, associations or not-for-profit bodies;
- in respect of data that has been disclosed to the public with the express consent of the data subject;
- necessary for the establishment, exercise, or defense of, or compliance with, legal claims; or
- necessary to comply with the law to achieve a purpose with respect to:
  - preventive medicine or occupational medicine, the assessment of employee ability, medical diagnosis, health care or social service provision, medical treatment, health management, and social work system and service provision.
    - If collection of personal data is not in compliance with relevant law, and the personal data is under the responsibility of the occupational or profession practitioner or person having the duty to keep such personal data as confidential under the law, collection must be in compliance with an agreement between the data subject and the medical profession practitioner;
  - the public interest in public health, with appropriate and specific measures to protect the rights and liberty of the data subject, particularly for the confidentiality of the personal data according to the professional duty or ethics;
  - labor protection, social security, national health security, welfare with respect to the medical treatment of persons who have rights under the law, protection of road accident victims, or social protection in which the collection of personal data is necessary for compliance with rights or duties of the data controller or the data subject and the appropriate measures have been provided to protect the fundamental rights and interest of the data subject;
  - scientific, historical or statistic research, or other public interests, insofar as necessary to achieve such purposes, and after implementing measures prescribed by the PDPC to protect the fundamental rights and interest of the data subject; or
  - substantial public interest, by providing suitable measures to protect the fundamental rights and interest of the data subject.

Where a data controller has collected sensitive personal data pursuant to any of the foregoing legal bases, the data controller would not be required to obtain consent to use or disclose that personal data for a purpose specified at the time of data collection.[93] However, in this situation, the data controller would be required to retain a record of the use or disclosure containing certain prescribed details for review by the data subject or the PDPC.[94]

---

[92] PDPA, s 26.
[93] PDPA, s 27.
[94] PDPA, ss 27 and 39.

11.3. Transferring personal data across borders without consent

The PDPA permits cross-border transfer of personal data without consent where transfer is:

- for compliance with law;[95]
- necessary to perform a contract to which the data subject is a contracting party or to comply with a request from the data subject before entering into such a contract;[96]
- in compliance with a contract between the data controller and other persons or juristic persons for the interests of the data subject;[97]
- to prevent or cease harm to life, body or health of the data subject or another person, where the data subject is unable to give consent at the time;[98] or
- necessary to carry out activities in relation to substantial public interest. [99]

11.4. Exemptions from the scope of the PDPA

The PDPA does not apply to the:

- collection, use, or disclosure of personal data that a person has collected solely for his/her personal benefit or household activity;[100]
- operations of public authorities tasked with maintaining state security, including financial security of the state, public safety, prevention and suppression of money laundering, forensic science, and cybersecurity;[101]
- use or disclosure of personal data that has been collected solely for the activities of mass media, fine arts, or literature, in accordance with professional ethics or for public interest;[102]
- House of Representatives, Senate, and Parliament;[103]
- trial and adjudication by courts and the work of officers in legal proceedings, legal execution, and deposit of property, including operations in accordance with the criminal justice procedure;[104]
- data operations undertaken by a credit bureau company and its members, pursuant to the law governing the operations of a credit bureau business;[105] or
- any class of personal data processing specified by Royal Decree.[106]

The first round of Draft Sub-regulations included a draft Royal Decree[107] proposing to add an exemption for personal data processing which is not automated, is not performed electronically, and is not intended to be part of a structured filing system.

---

[95] PDPA, s 28(1).
[96] PDPA, s 28(3).
[97] PDPA, s 28(4).
[98] PDPA, s 28(5).
[99] PDPA, s 28(6).
[100] PDPA, s 4(1).
[101] PDPA, s 4(2).
[102] PDPA, s 4(3).
[103] PDPA, s 4(4).
[104] PDPA, s 4(5).
[105] PDPA, s 4(6).
[106] PDPA, s 4.
[107] Group 2 Report, pages 10-12.

ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005 FPF.ORG | INFO@FPF.ORG