February, 2023 No.22

Personal Data Breach Notification

Shunsuke Minowa/ Poonyisa Sornchangwat/ Nuttida Doungwirote

1. Background

On 15 December 2022, the Notification of the Personal Data Protection Committee re: Rules and Methods for Notification of the Personal Data Breach B.E. 2565 (2022) dated 6 December 2022 ("**Notification**") was published in the Government Gazette and became immediately effective thereafter.

One of the obligations of the data controller under the Personal Data Protection Act ("**PDPA**") is to make a notification of any personal data breach ("**Personal Data Breach**")[1] to the Office of the Personal Data Protection Committee ("**PDPC Office**") and/or the data subject[2]. The Notification therefore elaborates on the definition of a Personal Data Breach and the details of the Personal Data Breach notification, which we aim to provide a summary thereof in this article.

2. Summary of the Notification

2.1 Characteristics of a Personal Data Breach that a notification thereof must be made

The data controller has the duty to notify the PDPC Office when a Personal Data Breach incident as defined in the Notification occurs due to an action of the data controller, data processor, or a staff, employee, contractor, representative, or related person of the said data controller or the data processor, or any other persons, or any other factors ("**Data Breach Incident**"). Such Data Breach Incident may occur in various forms, as follows:

- confidentiality breach (for example, when personal data is accessed by an attacker or is disclosed by an unauthorized employee of the company);
- integrity breach (for example, when personal data is edited by an unauthorized person or is recorded incorrectly due to the malfunction of a program); and/or
- availability breach[3] (for example, when personal data is locked up due to an attack by a ransomware or is deleted due to the malfunction of an electronic system).

2.2 Obligations of the data controller in the case of a Data Breach Incident

In the case of a Data Breach Incident, the data controller must:

(1) assess the credibility of such information and preliminarily investigate the Personal Data Breach without undue delay, which includes assessing the risk level of such Personal Data Breach;

---

[1] Clause 3 of the Notification. In this Notification,
"Personal Data Breach" means a breach of security measures that causes loss, unauthorized or unlawful access, use, alteration, editing, or disclosure of personal data, whether it is intentional, willful, negligent, an unauthorized or unlawful act, computer crime, cyber threat, error or accident, or other causes.

[2] Section 37(4) of the PDPA.

[3] Clause 4, Paragraph One of the Notification. A Personal Data Breach of which the data controller has the duty to notify the Office or the data subject…may involve a breach of one or more categories as follows:
(1) A Confidentiality Breach, which is an access or disclosure of personal data caused by either unauthorized or unlawful means, or an error or accident;
(2) An Integrity Breach, which is an alteration or editing of personal data in an incorrect, incomplete, or incomprehensive manner, caused by either unauthorized or unlawful means, or an error or accident; or
(3) An Availability Breach, which causes personal data to be inaccessible, or there is a destruction of personal data that makes such personal data unavailable as opposed to the usual situation.

(2) prevent, cease, or rectify the Personal Data Breach if the data controller finds that such Personal Data Breach poses a high risk of impacting the rights and freedom of a person;
(3) notify the PDPC Office of the cause of the Data Breach Incident without undue delay and within 72 hours from the time that it becomes aware of the cause, unless such breach does not pose a risk of impacting the rights and freedom of a person;
(4) notify the data subject of the cause of the Data Breach Incident together with the remedy approach without undue delay in the case of such breach posing a high risk of impacting the rights and freedom of a person; and
(5) proceed with the necessary and appropriate measures to cease, response, rectify, or remedy the condition resulting from the Personal Data Breach, and to prevent and reduce the impacts of any similar Personal Data Breach in the future, which includes the review of security measures to ensure their effectiveness.

2.3 Details of the notification of Data Breach Incident

To supplement the obligations in item 2.2 (3) and (4) above, the details of the notification of the Data Breach Incident shall be as follows:

(1) A notification of the Data Breach Incident to the PDPC Office shall be performed in accordance with the following details:

Method of notification	The notification shall be made in writing, or through an electronic method, or any other method prescribed by the PDPC.[4]
Timeline of notification	Within 72 hours from the time that the data controller becomes aware of the cause of the Data Breach Incident, as early as practicable
Details to be provided upon notification	(a) brief details in relation to the characteristics and category of the Personal Data Breach, the characteristics and number of data subjects, or characteristics and number of records of personal data related to the Data Breach Incident; (b) name and contact details of the Data Protection Officer (DPO), or name and contact details of the person whom the data controller assigned to coordinate the notification and provide further information; (c) information related to impacts that may occur due to the Personal Data Breach; and (d) information related to measures taken or will be taken by the data controller to prevent, cease, or rectify the Personal Data Breach, or remedy the damage – measures in respect of personnel, procedures, or technology, etc.[5]
Delay of notification	If the notification of the Data Breach Incident is delayed for more than 72 hours from the time that the data controller becomes aware of the cause of the Data Breach Incident due to any reason of necessity, the data controller may request the PDPC to consider exempting it from the liability related to the delayed notification of the Data Breach Incident. The data controller shall clarify the reason of necessity and relevant details thereof to show that there was a reason of necessity that caused the notification of the Data Breach Incident to be delayed. Such details shall be notified to the PDPC Office immediately; moreover, such notification shall be made no later than 15 days from the time that the data controller becomes aware of the cause of the Data Breach Incident.[6]

[4] Clause 6 of the Notification.
[5] Clause 6 of the Notification.
[6] Clause 7 of the Notification.

The data controller may rely on an exemption not to make a notification to the PDPC Office if the data controller can prove, for example, that such Data Breach Incident does not pose a risk of affecting the rights and freedom of a person, etc. In this regard, to rely on such an exemption, the data controller has the duty to provide information or evidence for the PDPC Office to consider.[7] However, the method and timeline of the provision of information and evidence in relation to such exemption is not stipulated in the Notification.

(2) Notification of the Data Breach Incident to the data subject shall be performed in accordance with the following details:

Method of notification	- notification in writing or by electronic means; or - notification to a group, or general notification via public media, online social media, or electronic means or any other means that the affected data subject or the public are able to access in case the data controller is not able to notify the data subject individually in writing or by electronic means because there are no contact details, or due to any other reason of necessity.[8]
Timeline of notification	As soon as practicable without undue delay
Details to be provided upon notification	(a) brief information related to the characteristics of the Personal Data Breach; (b) name and contact details of the Data Protection Officer (DPO) or the person whom the data controller assigned to coordinate the notification; (c) information related to impacts that may occur to the data subject due to the Personal Data Breach; and (d) approach to remedy the damage incurred by the data subject and brief information related to measures taken or will be taken by the data controller to prevent, cease, or rectify the Personal Data Breach – measures in respect of personnel, processes, or technology, or any other measures, including recommendations related to measures that the data subject may additionally take to prevent, cease, or rectify the Personal Data Breach, or remedy the damage incurred.

2.4 <u>Required provision in the data processing agreement between the data controller and data processor</u>

In the case where the data controller enters into an agreement with the data processor with respect to an entrustment of data processing, the data controller shall stipulate in such agreement the obligation of the data processor to notify the data controller of the Data Breach Incident without delay within 72 hours from the time which the data processor becomes aware of the cause.[9]

2.5 <u>Assessment of risk of the Personal Data Breach</u>

For the assessment of risk of the Personal Data Breach regarding its impact on the rights and freedom of a person, the data controller may take into account factors as itemized in the Notification, such as the category of the breach, personal data that has been compromised, number and status of affected data subjects, security measures that have been taken or will be taken by the data controller, and the impact of the breach on the public, etc.[10]

[7] Clause 9 of the Notification.
[8] Clause 11 of the Notification.
[9] Clause 8 of the Notification.
[10] Clause 12 of the Notification. For an assessment of risk that the Personal Data Breach poses in relation to the degree of impact on the rights and freedom of a person, the data controller may take into account the following factors:
(1) characteristics and category of the Personal Data Breach;
(2) characteristics or category of personal data relating to the breach;
(3) volume of personal data related to the breach, which may be considered from the number of data subjects or records of personal data relating

3. Conclusion

The notification of the Data Breach Incident to the PDPC Office and the data subject is one of the key obligations of the data controller and/or data processor in the perspective of the personal data protection.

To enhance the understanding of the said obligation, the PDPC also published the Manual on Guideline for Assessment of Risk and the Notification of the Personal Data Breach Version 1.0, dated 15 December 2022.

If the data controller fails to make a notification of the Data Breach Incident as required under the PDPA and the Notification, it shall be liable for an administrative fine not exceeding THB 3,000,000 (Three Million Baht).[11] Therefore, any person who is considered as a data controller and/or data processor should ensure that they duly comply with the obligation related to the Data Breach Incident under the PDPA and the Notification.

[Authors]

Shunsuke Minowa
shunsuke_minowa@noandt.com
Since he joined the Bangkok Office, he has been supporting Japanese companies in their expansion of business into Thailand and other South-east Asian countries and providing advice to Japanese affiliated companies in Thailand. He has a wide range of experience in a variety of projects, including real property development, M&A, joint venture, infrastructure, dispute, labor and pharmaceutical industries, medical and healthcare businesses.

Poonyisa Sornchangwat
poonyisa_sornchangwat@noandt.com
She is a Thai qualified lawyer based in the Bangkok office. She has been involved in several cross-border transactions, joint ventures and mergers & acquisitions, and has assisted Japanese companies that aimed to expand their businesses into Thailand, and provided legal advice on corporate matters and legal compliance to several businesses since 2015.

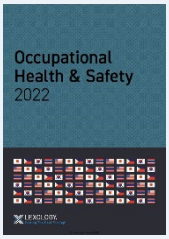
Nuttida Doungwirote
nuttida_doungwirote@noandt.com
Nuttida graduated with a First-Class Honors LL.B. from Chulalongkorn University. Her main practices include corporate law, mergers and acquisitions, PDPA, and compliance matters. She has assisted in various commercial transactions for both local and international clients.

to the breach;
(4) characteristics, category, or status of the affected data subjects, as well as the fact whether or not the affected data subjects, including minors, disabled persons, incompetent persons, quasi-incompetent persons, or vulnerable persons, lack the capability to protect the rights and benefits of themselves due to their limitations;
(5) severity of the impact and damage that occurred or may occur to the data subject due to the Personal Data Breach, and the effectiveness of the measures that the data controller has taken or will take to prevent, cease, or rectify the Personal Data Breach, or remedy the damage, to alleviate the impact and damage that occurred or may occur to the data subject;
(6) wide-ranging effects to the business or the operation of the data controller or the public due to the Personal Data Breach;
(7) characteristics of the storage system of the personal data relating to the breach and relevant security measures of the data controller or the data processor, including organizational, technical, and physical measures; and
(8) legal status of the data controller, such as whether it is a natural person or a juristic person, including the size and nature of the business of the data controller.

[11] Section 83 of the PDPA.

Other Publications

Recently we also featured in a number of articles and books covering a wide range of legal areas to address the latest legal issues. Please follow the link below to access each publications.



Lexology GTDT - Occupational Health & Safety 2022 – Thailand

This article enabling side-by-side comparison of local insights into legislation, regulations and codes of practice; employer duties and responsibilities; worker duties and responsibilities; workplace hazards and risk management; liabilities, enforcement and penalties; and recent trends.

Lexology GTDT - Real Estate 2022 – Thailand

This article provides comparative analysis of real estate regulations in different jurisdictions worldwide, with answers to crucial questions in key areas such as: acquisition of real estate, including recording conveyance documents, foreign investors, investment entities, leases and mortgages and contracts and financing, including liens, interest, enforcement, protection of collateral, covenants and bankruptcy.

www.noandt.com

NAGASHIMA OHNO & TSUNEMATSU

JP Tower, 2-7-2 Marunouchi, Chiyoda-ku, Tokyo 100-7036, Japan
Tel: +81-3-6889-7000 (general) Fax: +81-3-6889-8000 (general) Email: info@noandt.com

Nagashima Ohno & Tsunematsu is the first integrated full-service law firm in Japan and one of the foremost providers of international and commercial legal services based in Tokyo. The firm's overseas network includes locations in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi, Jakarta and Shanghai, and collaborative relationships with prominent local law firms throughout Asia and other regions. The over 500 lawyers of the firm, including about 40 experienced attorneys from various jurisdictions outside Japan, work together in customized teams to provide clients with the expertise and experience specifically required for each client matter.

Singapore Office
(Nagashima Ohno & Tsunematsu Singapore LLP)

6 Battery Road Level 41
Singapore 049909
Tel: +65-6654-1760 (general)
Fax: +65-6654-1770 (general)
Email: info-singapore@noandt.com

Bangkok Office
(Nagashima Ohno & Tsunematsu (Thailand) Co., Ltd.)

34th Floor, Bhiraj Tower at EmQuartier
689 Sukhumvit Road, Klongton Nuea
Vadhana, Bangkok 10110, Thailand
Tel: +66-2-302-4800 (general)
Fax: +66-2-302-4899 (general)
Email: info-bangkok@noandt.com

HCMC Office
(Nagashima Ohno & Tsunematsu HCMC Branch)

Suite 1801, Saigon Tower
29 Le Duan Street, District 1
Ho Chi Minh City, Vietnam
Tel: +84-28-3521-8800 (general)
Fax: +84-28-3521-8877 (general)
Email: info-hcmc@noandt.com

Hanoi Office
(Nagashima Ohno & Tsunematsu Hanoi Branch)

Suite 10.04, CornerStone Building
16 Phan Chu Trinh, Hoan Kiem District
Ha Noi City, Vietnam
Tel: +84-24-3266-8140 (general)
Fax: +84-24-3266-8141 (general)
Email: info-hanoi@noandt.com

Jakarta Office (*Associate office)
(IM & Partners in association with
Nagashima Ohno & Tsunematsu)

Jakarta Mori Tower 14th Floor, Unit 1401
Jalan Jenderal Sudirman Kav. 40-41
Jakarta 10210, Indonesia
Tel: +62-21-25098080 (general)
Fax: +62-21-25098090 (general)
Email: info-jakarta@noandt.com

Shanghai Office
(Nagashima Ohno & Tsunematsu
Shanghai Representative Office)

21st Floor, One ICC, 999 Middle Huaihai Road
Xuhui District, Shanghai 200031, China
Tel: +86-21-2415-2000 (general)
Fax: +86-21-6403-5059 (general)
Email: info-shanghai@noandt.com

For more details on our global practice

If you would like to receive future editions of the NO&T Thailand Legal Update by email directly to your Inbox, please fill out our newsletter subscription form at the following link: https://www.noandt.com/en/newsletters/nl_thailand_legal_update/
Should you have any questions about this newsletter, please contact us at <thailand-legal-update@noandt.com>.
Please note that other information related to our firm may be also sent to the email address provided by you when subscribing to the NO&T Thailand Legal Update.