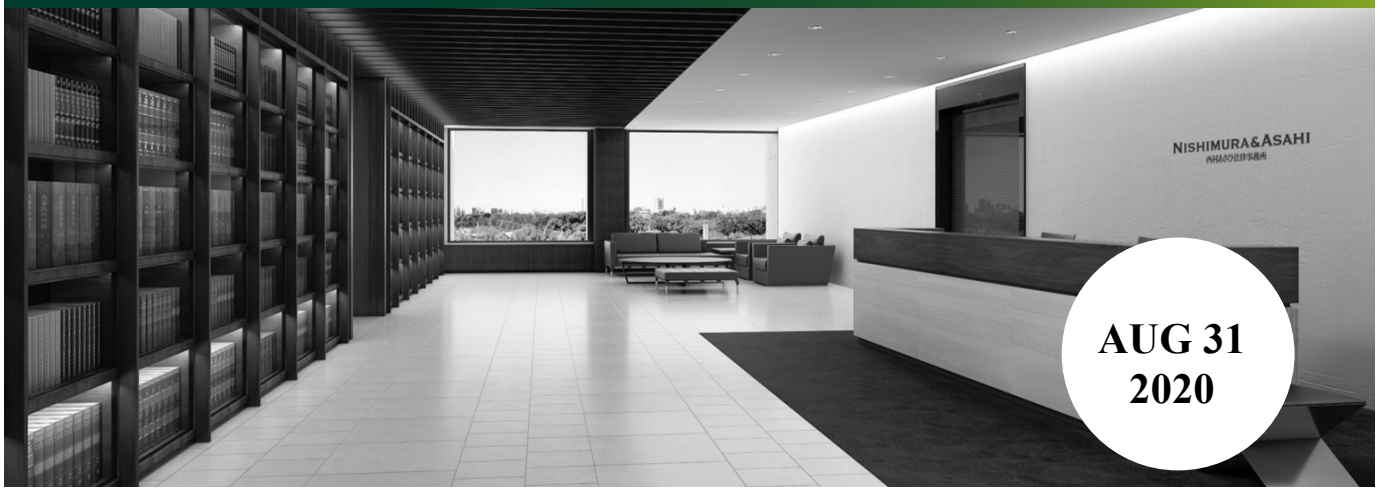
西村あさひ法律事務所
NISHIMURA & ASAHI
Corporate Crisis Management Newsletter
Asia Newsletter



Handling of Data Breach under Thai PDPA

Jun Katsube, Chanakarn Boonyasith, Pitchabsorn Whangruammit

1. What happened in May 2020?

In early May 2020, security researcher Justin Paine "found" approximately 8.3 billion electronic records that had leaked on to the internet. According to Paine, he simply stumbled upon a database that did not require any form of authentication to access; thus the information contained therein was publicly accessible. This "exposed" database was controlled by Advanced Wireless Network (AWN), a subsidiary of Advanced Info Service (AIS), the largest mobile phone operator in Thailand. Paine further stated that the leak contained DNS query logs and NetFlow logs which appeared to belong to AWN customers, and using this data it is quite simple to paint a picture of what a person does on the internet. For example, it allows you to know both the types of devices they use to access the net and the social networking websites they visit thereon. Paine attempted to contact AIS several times to get the database secured, but was unsuccessful. After receiving no response from AIS, Paine contacted the Thailand Computer Emergency Response Team (ThaiCERT), an official contact point for dealing with computer security incidents within the Thai internet community. ThaiCERT was able to contact and coordinate with AIS to have the database successfully secured; unfortunately only after it was found to be exposed and publicly accessible for about two weeks.

In a 25 May 2020 public statement, AIS apologised for the incident, confirmed that only a small amount of non-personal and non-critical information was exposed, and stated that the leaked data did not contain any personal information which could be used to identify customers or cause them any financial, or other, harm.[1] Despite this, the National Broadcasting and Telecommunication Commission (NBTC) raised concerns that the incident might affect AWN users and therefore requested that AWN provide more details about the incident. According to AWN, it was improving a system for provision of services by randomly pulling data during a certain period to be kept in the database in question, separate from the company's actual database. They also claimed that the leaked

[1] http://investor.ais.co.th/news.html/id/780975/group/newsroom_press

information did not identify any natural person to whom the data belonged and did not contain any numbers or banking transactions. AWN confirmed that it has strict security procedures in place, especially for the retention of personal information, but also admitted that its staff were not aware of the importance of data security and had dealt with data negligently up through the occurrence of the incident. After receiving such explanations from AWN, the NBTC issued an official warning letter to AWN highlighting that AWN must place strict importance on cyber security and that AWN employees must be made fully aware of the importance of security measures for protecting users' information.[2]

2. Postponement of the Personal Data Protection Act[3]

Originally, the Personal Data Protection Act BE 2562 (2019) (the "**PDPA**") was to become effective on 27 May 2020. However, due to the COVID-19 outbreak, a Royal Decree was issued on 21 May 2020 suspending enforcement until 31 May 2021, thus allowing more time for business operators to prepare for full enforcement of the PDPA. However, in the meantime, data controllers are required to provide security measures at the required standard,[4] unless otherwise notified by the relevant authority. According to the measures prescribed by Notification of the Ministry of Digital Economy and Society, administrative safeguards, technical safeguards and physical safeguards should be taken into consideration in order to set security measures for personal data access control. It should also be noted that the term 'security of personal data' was defined in the notification as '*maintenance of confidentiality, integrity and availability of personal data; in order to prevent unauthorised or unlawful loss, access to, use, alteration, correction or disclosure of Personal Data*', which is an obligation of data controllers and data processors required under the PDPA.

Since the PDPA also focusses on security measures for personal data, we analyze what would happen if this type of data breach were to occur assuming the PDPA had been in effect as below.

3. Legal implications for AWS had the PDPA been in force earlier

First, there is some overlap between the PDPA and the current legislation governing protection of personal information used or collected in particular business sectors ("**Sector-specific Legislation**"). Indeed, Sector-specific Legislation was in place prior to the considered adoption of the PDPA and AIS, as a telecommunications company, remains governed by it.[5] As such, it is important to note that when the PDPA becomes fully effective in 2021, the PDPA will also apply, in addition to or in replacement of such Sector-specific Legislation, in the following scenarios:

- For provisions with respect to the collection, use or disclosure of personal information, and provisions with respect to the rights of a data subject, including relevant penalties – the provisions of the PDPA will apply additionally regardless of whether or not they are in repetition of the Sector-specific Legislation; and

---

2 https://www.nbtc.go.th/News/Press-Center/45313.aspx

3 As to the outline of PDPA, please see "Outline of the 2019 Personal Data Protection Act in Thailand" written by Jun Katsube, Chanakarn Boonyasith and Pitchabsorn Whangruammit in Corporate Crisis Management Newsletter / Asia Newsletter (June 30, 2020).

4 As specified in the Announcement of the Ministry of Digital Economy and Society re: Security Measures for Personal Data BE 2563 (2020), effective from 18 July 2020 until 31 May 2021.

5 The National Telecommunications Commission (NBTC's predecessor), by virtue of the Telecommunications Act BE 2544 (2001), prescribed various requirements to which telecommunications companies were to adhere in the protection of users' personal information and right to privacy.

- For provisions with respect to complaints, provisions granting power to the Expert Committee to issue an order to protect the data subject and provisions with respect to the power and duties of the competent official, including relevant penalties, the provisions of the PDPA shall apply in the following circumstances:
  - in the event that the Sector-specific Legislation has no provision with respect to certain complaints; and
  - in the event that the Sector-specific Legislation has provisions giving the power to the competent official, who has the power to consider the complaints under such law and to issue an order to protect the data subject, but such power is not equal to the power of the Expert Committee under the PDPA, and either such official makes a request to the Expert Committee or the data subject files a complaint with the Expert Committee under the PDPA, as the case may be.

In light of the above, it is clear the PDPA will play an important role with regard to personal information and should be taken into consideration by entrepreneurs in the telecommunications business, such as AIS and AWN, already governed by Sector-specific Legislation.

Second, it is important to identify whether leaked information is considered 'Personal Information' under the PDPA.[6] If leaked information is personal information, the associated company's responsibilities under the PDPA will be impacted. However, according to the facts given by AIS and AWN, all of the leaked data in their case was merely "internet usage patterns" and did not contain any personal information that could be used to identify a customer. Based on the fact that the leak did not contain personal information, the PDPA would not apply to their case. Nonetheless, had the leaked information contained 'personal information', e.g. the name and surname of any individual customer or any other information which enables the identification of such individual, such as IP addresses, AIS and AWN - as a data controller and/or data processor who collected and maintained such personal information - would not have been able to deny their duties and responsibilities under the PDPA.

Third, assuming that the leaked AWN information was personal information and the PDPA therefore applied, we need to consider what duties would have been imposed on AWN and AIS. If either AIS or AWN were in a position to determine which personal information should be collected and the purpose or outcome for which such personal information were to be processed, they would be considered a "data controller" under the PDPA. If, however, they were following the instructions of another entity regarding collection, use and/or disclosure of personal information, e.g. if AWN were following AIS's instructions to collect, use and/or disclose such personal information, it would be more likely that AWN were considered a "data processor", and AIS the "data controller", under the PDPA.

The PDPA sets out a multitude of duties with which data controllers and data processors must comply. Most importantly, the PDPA requires both the data controller and the data processor to, among other things, put in place appropriate security measures to prevent unauthorised or unlawful loss, access to, use, alteration, correction or disclosure of personal information/data.[7] Such measures must be reviewed as and when necessary, or when the applicable technology is changed or upgraded, in order to efficiently maintain the appropriate security and safety of personal information. In the case of the data controller, such measures shall also be in accordance with the minimum standard to be specified and announced by the Personal Data Protection Committee. Even though further details regarding security measures required by the Personal Data Protection Committee are not available at this stage, taking into consideration the measures prescribed by the Notification of the Ministry of Digital Economy and Society and the NBTC's

6 Section 6 of the PDPA defines Personal Information as 'any information relating to a natural person, which enables the identification of such person, whether directly or indirectly, but not including the information of deceased persons'.

7 Based on Section 37 in the case of the data controller and Section 40 in that of the data processor.

decision on the incident, as referred to above, it is safe to conclude that AWN's security measures, at that time, were far below the required standard. If the leaked information was personal information, AWN and/or AIS would have been considered in violation of Section 37 and/or 40 of the PDPA, as the case may be.

Furthermore, in the case of personal data breaches, the data processor is legally required to notify the data controller of such breach. Within 72 hours of becoming aware of the breach, the data controller, without delay and where feasible, must notify the Office of Personal Data Protection Committee; unless such breach is unlikely to result in a high risk to the rights and freedoms of natural persons. However, if the breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall also notify the data subjects of the breach and take remedial measures without delay. The PDPA remains silent on the rules and procedures on notification and exemption of notification, which will be prescribed by the Personal Data Protection Committee. As mentioned above, it is possible that if the leak contained any personal information, and AWN and/or AIS was considered a data controller, AWN and/or AIS would have been required to comply with this duty to notify. Based on the incident, it appears that AWN and AIS lacked proper contact channels; consequently, Paine was not able to contact them to remedy the incident. Both AWN and AIS's lack of contact points with regard to personal data breaches would have likely hindered their ability to notify the Office of Personal Data Protection Committee of the personal data breach within the timeframe required by the PDPA (thereby constituting a breach of their obligations defined therein).

4. Liabilities under the PDPA

Assuming that the leaked AWN information was personal information as defined by the PDPA, AWN and/or AIS may have faced civil liability and/or administrative fines as imposed by the Expert Committee. In such scenarios, data subjects who suffer damage caused by violation of or non-compliance with the PDPA will also be entitled to claim compensation. The PDPA provides that the court has the authority to award punitive damages not exceeding twice the amount of actual damages in addition to the actual damages which occur. Furthermore, for data controllers and/or data processors who fail to comply with their duties, i.e. fail to put in place appropriate security measures and to report personal data breaches, fines not exceeding Baht 3,000,000 could be imposed by the Expert Committee. The Expert Committee nevertheless may, at its discretion, require the data controller or the data processor to remedy or take any necessary actions before imposing said fines.

The PDPA limits criminal liability for offences committed by the data controller involving sensitive data that are likely to cause damage to a data subject, impact his or her reputation, or expose such data subject to scorn, hate or humiliation; or in order to unlawfully benefit him/herself or another person. However, in the case of accidental leakage of personal information, it is unlikely that the data controller will be subject to criminal liability under the PDPA.

Jun Katsube
Partner, Nishimura & Asahi
j_katsube@jurists.co.jp

Jun Katsube joined Nishimura & Asahi in 2006. He obtained his LL.M. from the University of Southern California Gould School of Law in 2013, was admitted in New York and California in 2014 and 2017, respectively, and worked for the Asia Pacific Legal Division of Mitsui & Co. from 2014 to 2016. He specializes in corporate crisis management matters, including competition law issues, accounting fraud, and quality data falsification.

Chanakarn Boonyasith
Partner, SCL Nishimura
chanakarn@siamcitylaw.com

Chanakarn Boonyasith specialises in corporate & commercial law, labour & employment law, and commercial contracts. She advises multinational clients on matters of private and public transactions from a wide range of industries. Chanakarn Boonyasith has been a guest speaker on Thai employment law and data protection law in various domestic and international events and a part-time lecturer with several universities in Thailand. Chanakarn is also a regular contributor to a number of domestic and international law journals.

Pitchabsorn Whangruammit
SCL Nishimura
pitchabsorn@siamcitylaw.com

Pitchabsorn Whangruammit is an enthusiastic associate specializing in employment and personal data protection law-related matters. She provides timely advice, deals with relevant authorities, and reviews and provides comments on various types of contracts and legal documents. As a versatile member of the SCL team, she also has experience in international arbitration and trade and commercial law.

Public Relations Section, Nishimura & Asahi
Otemon Tower, 1-1-2 Otemachi, Chiyoda-ku, Tokyo 100-8124, Japan
Tel: +81-3-6250-6202 Fax: +81-3-6250-7200 E-mail: newsletter@jurists.co.jp URL: https://www.jurists.co.jp/en