PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPC 9

Case No. DP-2010-B7267

In the matter of an investigation under section 50(1)
of the Personal Data Protection Act 2012

And

Eatigo International Pte. Ltd.

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised disclosure of personal data – Insufficient security arrangements – Failure to maintain personal data asset inventory – Failure to conduct sufficient security monitoring*

Data Protection *– Financial Penalty – Voluntary Admission of liability*

Eatigo International Pte. Ltd.

[2022] SGPDPC 9

Lew Chuen Hong, Commissioner — Case No. DP-2010-B7267

21 December 2022

Introduction

1. For an organisation to effectively safeguard the personal data in its possession or control, it must first know what its personal data assets *are*. The surest way to ensure such visibility is to maintain a comprehensive personal data asset inventory. This case is, amongst other things, a cautionary tale of the consequences of not maintaining a proper personal data asset inventory.

2. On 29 October 2020, the Personal Data Protection Commission (the "**Commission**") was notified by a third party about a possible data leak by Eatigo International Pte. Ltd. (the "**Organisation**"). A cache of personal data that was suspected to be from the Organisation's database was being offered for sale on an online forum (the "**Incident**").

Facts of the Case

3. The Organisation provides an online restaurant reservation platform which offers incentives such as discounts to its users. In its daily operations, it regularly collects and

processes the personal data of its users in order to facilitate restaurant reservations and the provision of incentives.

4. After the Commission was notified of the Incident, it informed the Organisation on 30 October 2020 of an online forum purportedly selling the personal data from various ecommerce websites, including a database containing personal data that were suspected to have been obtained from the Organisation. Separately, the Organisation was also notified of the Incident on the same day by a user and a Channel News Asia journalist. The Organisation proceeded to carry out investigations.

5. The Organisation's investigations revealed that the personal data for sale on the online forum did not match any current databases in use by the Organisation at the time of the Incident, but matched the structure of a legacy database which contained user data as of late 2018, when the database was last updated (the "**Affected Database**"). The Affected Database was hosted on the infrastructure of a Cloud Service Provider located in Singapore, and was previously in use by the Organisation until 2018. Thereafter, the Organisation migrated to its current online platform, which entailed a complete redevelopment of data storage and infrastructure. Whilst the Organisation did not intend to continue to utilise the personal data contained in the Affected Database, it was nevertheless retained to support the migration of data to the new platform. After the migration, the Affected Database was not included in the Organisation's Virtual Private Network ("**VPN**") infrastructure. Unfortunately, as the Organisation transitioned to the current engineering team, knowledge of the Affected Database was lost.

6. The Organisation was unable to ascertain exactly when the threat actor gained unauthorised access to the Affected Database. However, since the Affected Database was last updated in late 2018, the Incident was likely to have occurred some time between 2018 and

2020 (when the Affected Database was put up for sale on an online forum). Investigations revealed the following:

(a) At the time of the Incident, the Affected Database was accessible from the internet and accessible by anyone who had the requisite credentials;

(b) None of the Organisation's employees at the material time had knowledge of the Affected Database or possessed the credentials to access the Affected Database;

(c) The databases inside the Cloud Service Provider's Relational Database Services ("**RDS**") were intended to have randomly generated alphanumeric passwords of a minimum 13-character length. However, there had been no such password rotation rules implemented for the Affected Database;

(d) There was no security review conducted on the protection provided to the personal data contained in the Affected Database;

(e) There was no system in place to monitor the exfiltration of large volumes of data from the Affected Database; and

(f) No personal data asset inventory or access logs were maintained, and the Organisation was unable to establish how or when the threat actor gained unauthorised access to the Affected Database.

7. The Affected Database held the personal data of approximately 2.76 million of the Organisation's users. Because the Organisation had effectively lost track of a database of that size, network security and access control measures deployed by the Organisation were not applied to the Affected Database.

8. Consequently, the Affected Database was accessed and likely exfiltrated in the Incident and put up for sale on an online forum. A sample of 154 personal data sets were also posted on the online forum. The types of personal data affected (the "**Dataset**") were as follows:

(a) Name;

(b) Email;

(c) Telephone number;

(d) Gender;

(e) Passwords in MD5 Hash; and

(f) Facebook ID number and tokens of around 10 users, which can provide access to the Facebook accounts of users and their accounts with the Organisation's online platform.

9. The personal data of a total of 154 of the Organisation's users were displayed in the forum post, and appeared to have been randomly selected from the Affected Database. As of 13 November 2020, the post on the online forum no longer lists the Organisation's personal data for sale.

10. Upon discovery of the Incident, the Organisation implemented, or has been in the process of implementing, the following remedial actions:

(a) The Affected Database was securely backed-up and then deleted;

(b) All databases were ensured to be accessible only inside VPN (i.e. no direct internet access);

(c) All passwords to access databases were changed as of 30 October 2020;

(d) Affected individuals were notified;

(e) Security Settings on Systems Infrastructure were upgraded;

(f) Different VPN for different categories of staff were created:

(g) Access security for data storages and cloud services was improved, including increasing the password rotation and strengthening the password rules.

(h) All personal data in all non-production was anonymised;

(i) The logging and monitoring systems was reviewed to detect data access anomalies and trace access;

(j) Access for external services used with the Organisation's platform was reviewed;

(k) Penetration Testing was conducted;

(l) All staff were updated on policies relating to network security, and subject to Data protection and social engineering prevention training;

(m) All internal users in the Organisation's cloud infrastructure and data storage were subject to review;

(n) Access and error logging for all databases were added;

(o) The entire infrastructure, including which servers are currently inside vs. outside demilitarized zone (DMZ), was subject to review; and

(p) Accelerated implementation of recommendations of security audit completed by an external consultant in September 2020.

Findings and Basis for Determination

The Protection Obligation under section 24 of the PDPA

11. Based on the circumstances of the Incident as set out above, the Commission's investigations centred on whether the Organisation had breached its obligation under section 24 of the Personal Data Protection Act 2012 ("**PDPA**") to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised

access, collection, use, disclosure, copying, modification, disposal or similar risks ("**the Protection Obligation**").

12. For the reasons set out below, it is determined that the Organisation failed to implement reasonable security arrangements to protect the Affected Database from the risk of unauthorised access. This includes a failure to ensure that the Affected Dataset was properly accounted for in the Organisation's personal data asset inventory, and a failure to implement reasonable data protection processes.

13. In determining what constitutes reasonable security steps or arrangements, an organisation should have regard to the nature of the personal data in its possession and control, as well as the impact that the disclosure of the data might have on the affected persons. As stated in the Commission's Advisory on Key Concepts in the PDPA (the "**Advisory**")[1] at [17.2]:

> "There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration **the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.** For example, in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on."

[1] Advisory Guidelines on Key Concepts in the PDPA (Rev 1 February 2021)

14. The Affected Database contained personal data relating to approximately 2.76 million individuals, encompassing personal data such as passwords, access IDs and Facebook tokens. Given the high volume of personal data contained in the Affected Database, it was incumbent on the Organisation to implement policies and practices to meet such security needs to discharge its obligation under the Protection Obligation.

Lapses in managing of personal data asset inventory

15. For organisations with substantial personal data assets, the maintenance of an accurate and up-to-date personal data asset inventory is a pre-requisite for complying with the Protection Obligation. The personal data asset inventory should catalogue all personal data assets in the organisation's possession or control, so as to ensure that such personal data is covered by the organisation's security measures. Maintaining such an inventory ensures that the organisation retains the necessary institutional memory of the personal data assets that is or was previously under its possession or control even if there is turnover of staff. Any significant lapse in an organisation's inventory management and maintenance would impair the organisation's ability to know whether the data protection processes it implemented are sufficient to cover all its personal data assets.

16. This requirement to maintain a personal data asset inventory is not novel. As stated in *Re Management Corporation Strata Title Plan No. 3400* [2020] SGPDPC 10 at [13]:

> "In addition, **it is important for an organisation to be aware of and track its personal data assets. The creation and maintenance of a personal data asset register (i.e. a record identifying all personal data in the organisation's possession or control) is a good practice that would assist organisations to comply with the Protection Obligation. An up-to-date personal data asset register provides the**

organisation with an accurate record of all the personal data in its possession or control, and enables the organisation to ensure its periodic security reviews covers the personal data assets. It also enables the organisation to more effectively review the implementation of its data protection policies, for example, the access control list setting out the employees who have access to the IT systems the personal data asset is stored in, whether the internal business owner of the personal data asset has reviewed it for data quality issues, and initiating the process for disposing personal data that have reached the end of its life cycle within the organisation."

(emphasis added)

17. Similarly, it was stated in *Re Civil Service Club* [2020] SGPDPC 15 at [15]:

"From the Appointed Day, the Organisation's failure to take any reasonable steps to ensure sufficient obligations are imposed on the Vendor (when developing and troubleshooting the CMS, Membership Portal and Virtual Cards) to protect the Members Data was a breach of its obligations under section 24 of the PDPA. A period of about five years had elapsed since 2 July 2014 to 2 July 2019. **The Organisation, as owner of the CMS, should have included it as part of its personal data asset inventory and ensured that its data protection policies covered personal data held in the CMS. Had this been done, the Organisation would have identified these gaps in the business requirements for the CMS, which would have set it down the path to rectifying these gaps through one or both of the options discussed in the preceding paragraph.** The Organisation, as owner of the CMS, is responsible for identifying the omission and articulating its business requirements relating to the protection of personal data stored in the CMS. This would have led to action by the

> Vendor in recommending technical fixes to enhance the CMS. It is the failure to identify the omission and articulate business requirements, and for a not-trivial period of five years, that is the gravamen of the Organisation's breach of the PDPA."
>
> (emphasis added)

18. In this connection, the Commission's Guide to Developing a Data Management Programme (the "**Guide**") states that an organisation should establish a personal data asset inventory as part of Data Protection Impact Assessment ("**DPIA**"), and sets out the information that should be recorded by the organisation at pages 13 and 23:

> "By conducting a DPIA, an organisation would be in a better position to assess if the handling of personal data complies with the PDPA or data protection best practices, and to implement appropriate policy, technical or process measures. For more information on the DPIA, please refer to the Guide to Data Protection Impact Assessments.
>
> As part of a DPIA, **it is recommended to establish a data inventory** (see Data Inventory Maps, Data Flow Diagrams and Other Registers on page 23) **and classify the risk level of the data in the context that it is collected, used and disclosed throughout the data life cycle, from creation, distribution, storage, to disposal. This may be mapped onto a risk matrix for assessment and implementation of appropriate control for the identified risk levels.**
>
> ...
>
> **Data Inventory Maps, Data Flow Diagrams and Other Registers**

> Known risks should be managed through a good understanding of the life cycle and flow of personal data in your organisation. This can be done through documenting the personal data handled using diagrams and charts such as data inventory maps or data flow diagrams, as illustrated in Annex C.
>
> **The data inventory map and data flow diagram should also include information on the business purposes for collection, use and disclosure of personal data, the individuals and third parties who handle personal data under the organisation's possession or control, as well as the classification of the data to manage user access. They should also deal with when and how the organisation should dispose of or anonymise the personal data for long-term archival.** As good practice, it is important that employees and third parties access personal data on a need-to-know basis. Different sets of data may be accessed by different parties."
>
> (emphasis added)

19. In the present case, the Organisation's oversight in failing to maintain the Affected Database in its personal data asset inventory resulted in the omission to extend its extant security arrangements to the Affected Database. This resulted in the following:

(a) The Organisation did not maintain proper records of the Affected Database and was unable to locate documentation related to user permission for the Affected Database. There was a dearth of records of the details of the data lifecycle of the personal data in the Affected Database from collection to disposal.

(b) After the re-development and migration of the Organisation's online platform, the Organisation did not conduct a proper handover of the Affected Database despite the

turnover in staff. This led to the Organisation's engineering team in 2020 having no knowledge of the existence of the Affected Database or its access credentials.

(c) Since the Organisation lacked visibility of the Affected Database, it was omitted from the Organisation's periodic security review. The Organisation thus did not have the opportunity to assess whether the Affected Database needed to be retained, or whether its security arrangements should be updated. During the Commission's investigations, the Organisation indicated that the Affected Database should not have been retained following the successful migration of the Organisation's online platform in 2018. It stands to reason that if the Organisation had covered the Affected Database in its periodic security reviews and assessed that it should be deleted, the Incident could have been prevented.

(d) Since the Affected Database was effectively forgotten about, the Organisation also did not put in place any systems to monitor the exfiltration of data from the Affected Database, thus impeding its ability to react swiftly to mitigate the effects of the Incident.

20. The Organisation's negligence in this regard left an internet-accessible database containing the personal data of approximately 2.76 million individuals (i.e. the Affected Database) outside its data protection architecture, creating a clear vulnerability that was exploited by threat actors.

21. The Organisation's poor knowledge management often led to it providing inconsistent, extraneous and dilatory responses to the Commission's notices to produce specified information and documents ("**NTPs**") relating to the Organisation's access models, causing the Commission to expend substantial time and resources to seek various rounds of clarifications

with the Organisation. This includes, but is not limited to, the following responses to the Commission's NTPs:

(a) On 16 November 2020, the Organisation stated that the Affected Database was only accessible through VPN via certificates. After the Commission sought further clarifications, the Organisation stated on 14 December 2020 that it was in fact not included in the Organisation's VPN structure;

(b) On 16 November 2020, the Organisation stated that only 14 users had VPN access, but subsequently stated on 14 December 2020 that a total of 29 users with access without VPN; and

(c) The Organisation also gave conflicting information about its password policies regarding the Affected Database. On 16 November 2020, it purported to have put in place a password policy for the Affected Database prior to the Incident. However, on 10 February 2021, it indicated that no specifically predefined password rules applied to the Affected Database. On 4 March 2021, after further clarifications were sought, the Organisation stated that it no longer had the username and password for the Affected Database, and that nobody from its engineering team had any knowledge of the username and password.

Other lapses in the Organisation's data protection policies and processes

22. Besides failing to adequately maintain its personal data asset inventory, investigations also revealed other lapses and shortcomings in the Organisation's data protection policies and processes. As referenced in paragraph 18, the Guide states that by establishing a personal data asset inventory as part of an organisation's DPIA, it would be better positioned to assess if the handling of personal data complies with the PDPA or data protection best practices, and to

implement appropriate policy, technical or process measures. In this regard, aside from its lapses in its management of its personal data asset inventory, the Organisation also did not implement some other basic data protection processes.

23. First, organisations that have a high volume of personal data within their possession and / or control should implement sufficiently robust processes to protect personal data through reasonable security monitoring. This ensures that organisations have sufficient situational awareness of its network security, enabling it to react timeously to data breaches. This step is embedded into the responsibilities of a data protection officer, as stated in the Advisory at [21.4]:

> "An organisation's DPO plays an essential role in how the organisation meets its obligations under the PDPA. The responsibilities of the DPO often include working with senior management and the organisation's business units to develop and implement appropriate data protection policies and practices for the organisation. In addition, the DPO would undertake a wide range of activities, which may include producing (or guiding the production of) a personal data inventory, **conducting data protection impact assessments, monitoring and reporting data protection risks**, providing internal training on data protection compliance, engaging with stakeholders on data protection matters and generally acting as the primary internal expert on data protection."
>
> (emphasis added)

24. Examples of such security monitoring measures are provided in the Commission's Guide to Securing Personal Data in Electronic Medium at [4.1(j)] and [9.1] applicable at the material time[2]:

> "**Conduct periodic checks for personal data stored in ICT systems. For personal data that is not required in any form anymore, securely dispose the data (refer to section 8).** If there is a need to retain the data but not in identifiable form, e.g. for performing data analytics, consider anonymising the data.
>
> ….
>
> Computer networks allow communication between computers and devices that are connected to them. Internal corporate computer networks may be connected to external networks, such as the Internet. It is important for an organisation to ensure that its corporate computer networks are secure. Vulnerabilities in the network may allow cyber intrusion, which may lead to theft or unauthorised use of electronic personal data. Defences that may be used to improve the security of networks include:
>
> - **Intrusion prevention systems ("IPS") - a device or software application that monitors network or system activities and prevents malicious activities or policy violations**;
> - Intrusion detection systems ("**IDS**") – a network security appliance that monitors network and system activities for malicious activities and may raise alerts upon detecting unusual activities;
> - Security devices that prevent the unauthorised transfer of data out from a computer or network;

[2] The guide has been replaced by the Guide to Data Protection Practices for ICT Systems (updated 14 September 2021), which recommends similar security monitoring measures at pages 10 and 17.

- Firewalls; and
- Web proxies, anti-virus and anti-spyware software."

(emphasis added)

25. In this case, the high volume of personal data in the Affected Database necessitated a higher level of security awareness through robust security monitoring. However, the Organisation's monitoring system extended only to performance and latency monitoring. The Organisation did not implement security monitoring for exfiltration of sizeable volumes of data based on pre-set limits. Given the considerable volume of personal data in the Organisation's possession and / or control, including the personal data of the approximately 2.76 million individuals contained in the Affected Database, this is a reasonable security arrangement that the Organisation should have implemented.

26. Second, given the volume of personal data under the Organisation's possession and / or control, the Organisation also should carry out periodic security audits which should include a reasonable vulnerability assessment of its IT infrastructure. This would entail the discovery and mapping of all parts of the Organisation's network, including the Affected Database. If this had been carried out, it might have led to the re-discovery of the Affected Database, which would have allowed the Organisation to take the necessary steps to either improve the security of the Affected Database or delete it entirely. However, based on the Commission's investigations, the Organisation conducted no such security audits in relation to the Affected Database.

The Commissioner's Preliminary Decision

27. In determining whether any directions should be imposed on the Organisation under section 48I of the PDPA, and/or whether the Organisation should be required to pay a financial penalty under section 48J of the PDPA, the factors listed at section 48J(6) of the PDPA were considered, with particular emphasis on the following factors:

Mitigating Factors

(a) The Organisation had implemented the remedial measures set out in paragraph 10 swiftly to address the Incident.

Aggravating Factors

(b) The Organisation was grossly negligent in its failure to keep proper records or documentation of the Affected Database and to effect a proper handover to new employees vis-à-vis the Affected Database. Most egregiously, there was no institutional memory amongst the Organisation's employees of the Affected Database by late 2020, or of the access credentials.

(c) The Organisation had left the Affected Database exposed to a risk of unauthorised access and exfiltration for a protracted period of time, from October 2018 to late 2020.

(d) As stated in paragraph [21], the Organisation's dilatory responses to the Commission's NTPs resulted in delays in the investigations.

28. Additionally, the Organisation also impeded the Commission's investigations by responding in an uncooperative and evasive manner to the Commission's NTPs:

(a) The Organisation objected to the Commission's request for information about the access models implemented for current production databases, giving the excuse that it might create "additional security risks"; and

(b) Similarly, objecting to provide information regarding access to the Affected Database, citing the reason that this was against their policy and might create "additional security risks" even though the Affected Database had already been deleted on 3 November 2020.

29. Organisations that are uncooperative and that throw up objections will only prolong investigations. The Commission will not be deterred by such tactics. If, as is possible in this case, the Organisation did not have the information or needed more time to recover the information, honesty is the best policy. Hiding behind vague notions like "additional security risks" without providing details can and will be interpreted as cavalier and obstructive, and will be taken as an aggravating factor when the eventual outcome is determined.

30. Based on the foregoing, the Commission made a preliminary decision to impose a financial penalty on the Organisation for its breach of the Protection Obligation.

Representations Made by the Organisation

31. The Organisation was notified of the preliminary decision by way of the Commission's letter dated 26 November 2021 and was invited to make representations. On 10 December 2021, the Organisation made the following representations to the Commission urging the Commission to impose a warning in lieu of a financial penalty, or to reduce the financial penalty to be imposed:

(a) The Organisation had not intended to frustrate the Commission's investigation. Instead, the Organisation's internal investigations and responses to the Commission's NTPs were hampered due to diminished corporate knowledge of the Affected Database at the material time and the impact of the COVID-19 pandemic on its management and operations. In support, the Organisation stated that:

i. On July 2018, the Organisation's former Chief Technology Officer ("**CTO**") resigned, with the various back-end engineers that he recruited following suit. Consequently, the new CTO and team of back-end engineers lacked corporate memory and had no knowledge of the Affected Database;

ii. The internal investigations on the Incident were hampered by turbulence in the Company's organisation during the Covid-19 pandemic, and despite the steps taken to maintain system documentation, the Affected Database was not uncovered; and

iii. The conduct cited in [21] and [28] above stemmed from a misunderstanding of the Commission's queries and the new CTO, being from a different cultural background, being reluctant to provide sensitive data to the Commission;

(b) The contemplated financial penalty in the preliminary decision would be crushing on the Organisation and would likely lead to financial distress and the closure of its business. As the Organisation operates in the food and beverages industry, its business suffered during the COVID-19 pandemic and left it in a risky financial position from which is it has yet to recover from. Any financial penalty imposed would adversely affect the Organisation's business, and deter any further investors or lenders from providing any further loans or investments to the Organisation; and

(c) The impact of the Incident was limited. The Organisation raised the following points in support:

i. The Organisation did not collect NRIC numbers, birth dates and sensitive financial data such as credit card information. The login passwords that were collected were encrypted using MD5 Hash ;

ii. As of 10 December 2021, the Company received less than 100 requests from users to delete their accounts following the Incident; and

iii. The online forum post initially offering personal data from the Affected Database for sale appears to have been taken down as of 13 November 2020.

Diminished corporate knowledge and conduct during the Commission's investigations

32. The Organisation's representations in [31(a)] do not merit a waiver or reduction in the financial penalty imposed. Staff turnover is no excuse for a lack of corporate knowledge, and it is incumbent on organisations to take reasonable steps to bolster institutional memory to manage any security risks arising thereof. This includes the implementation of practices such as the maintenance of a personal data asset inventory as detailed in [16] to [18], which would have enabled it to conduct proper handovers to new staff.

33. As for the difficulties experienced by the Organisation during its own internal investigations and any misunderstandings it may have had in relation to the Commission's NTPs, it should have been candid with the Commission about its difficulties and sought clarifications and extensions of time to respond to the NTPs. Instead, its lack of transparency during the investigation stage caused the Commission to expend substantial time and resources in engaging the Organisation. In its representations, the Organisation has also admitted that it

should have substantiated its position during the NTP stage to avoid giving the Commission the impression that it was being uncooperative and evasive.

Likely impact of a financial penalty on the Organisation

34. One of the considerations in the imposition of a financial penalty is the likely impact of the imposition of such penalty on an organisation, including the ability of the organisation to continue its usual activities: see section 48J(6)(i). When determining the appropriate financial penalty, the Commission has consistently considered the financial circumstances of the organisation or person involved, bearing in mind that financial penalties imposed should avoid imposing a crushing burden or cause undue hardship on the organisation or person[3].

35. After careful consideration, the Commission accepts the Organisation's representation at [31(b)] that the imposition of the financial penalty proposed would likely lead to financial distress and the closure of its business. However, a mere warning is inappropriate in view of the egregiousness of the Organisation's breach of the PDPA and the impact of the Incident. Hence, the imposition of a reduced financial penalty, to be paid out in instalments, would be more proportionate and appropriate in ensuring the Organisation's compliance with the PDPA.

36. In arriving at its decision, the Commission had regard for the following factors concerning the Organisation's financial situation, and the likely impact that the proposed financial penalty in the preliminary decision would have on it:

(a) In the Organisation's audited financial statements for the financial year ending 31 December 2020, its independent auditor stated that there was significant doubt on

[3] *Re Jigyasa* [2021] SGPDPCR 1; *Commeasure Pte Ltd* [2021] SGPDPC 11; and *Neo Yong Xiang (trading as Yoshi Mobile)* [2021 SGPDPC 12

the ability of the Organisation to continue as a going concern and to realise its assets and discharge its liabilities in the ordinary course of business;

(b) The Organisation's monthly income statements from 2021 indicated that it was incurring heavy net losses on a month-to-month basis (with the exception of one month); and

(c) The Organisation had various substantial short-term loans due in the near future.

37. The above evinces a clear picture of an organisation in a parlous financial situation caused by the COVID-19 pandemic, with various debts and liability (some incurred to keep the business afloat) coming due in the near future. In view of this situation, the Commission shall refrain from imposing a financial penalty that might push the Organisation's business even closer to the brink.

Impact of the Incident

38. The Commission had already taken into account the impact of the Incident when calibrating the financial penalty in the preliminary decision. At the same time, the Commission also took into consideration the fact that the Affected Database contained the personal data of a very high number (2.76 million) of individuals, which necessitated the implementation of more robust security measures by the Organisation. The impact of the Incident should not be minimised, and the financial penalty imposed should reflect this.

Acceptance of the Commission's findings

39. Additionally, the Commission notes that the Organisation voluntarily accepted the Commission's findings in the preliminary decision that it had failed to comply with the

Protection Obligation and explicitly indicated that it would not seek to challenge these findings. The Organisation's voluntary acceptance of liability (even at this late stage) ought to be reflected in the financial penalty. Had the Organisation accepted responsibility for the Incident at an earlier stage of the investigation, it could have significantly shortened the time for investigations and resolution of this case through the expedited breach procedure and also benefited from greater mitigatory considerations. Nonetheless, an organisation that voluntarily accepts responsibility for its non-compliance with the PDPA should be recognised as an organisation that demonstrates its commitment to the Accountability Obligation and shows that it can be responsible for the personal data in its possession or under its control[4]: see [46] of *Farrer Park Hospital Pte Ltd* [2022] SGPDPC 6.

40. Having considered all the relevant factors in this case including the representations made by the Organisation, the Commission hereby requires the Organisation to pay a financial penalty of $62,400 in 12 monthly instalments by the due dates as set out in the notice accompanying this decision, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

41. In view of the remedial actions already been taken by the Organisation, no further directions need be issued to the Organisation

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION

[4] Refer to section 11(2) of the PDPA.