PERSONAL DATA PROTECTION COMMISSION

[2024] SGPDPC 4

Case Nos. DP-2210-C0303 & DP-2306-C1172

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

And

Consumers' Association of Singapore (CASE)

… *Organisation*

DECISION

Data Protection – Protection obligation – Unauthorised access to personal data – Insufficient security arrangements - Inadequate password policies – Failure to stipulate clear security responsibilities in contracts with vendors – Failure to conduct staff training

Data Protection – Accountability obligation – Lack of data protection policies and practices

Consumers' Association of Singapore (CASE)

Wong Huiwen Denise, Deputy Commissioner — Case Nos. DP-2210-C0303 & DP-2306-C1172

9 July 2024

Introduction

1 On 11 October 2022, the Consumers' Association of Singapore (CASE) (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a data breach incident involving a threat actor accessing the Organisation's email accounts, and sending phishing emails on 8 October 2022 and 9 October 2022 with the Organisation's official email addresses[1] ("**Incident 1**").

2 The Commission commenced investigations to determine the Organisation's compliance with the Personal Data Protection Act 2012 ("**PDPA**") in relation to Incident 1.

3 On 22 June 2023, while the Commission was still investigating Incident 1, the Commission received a complaint against the Organisation regarding another data breach incident involving phishing emails being sent to the Organisation's consumers, from email addresses which did not originate from the Organisation's domain ("**Incident 2**"). Hence, the Commission also initiated investigations to determine the Organisation's compliance with the PDPA in relation to Incident 2.

[1] The email addresses were *"online-submission@case.org.sg"* and *"mediator1@case.org.sg".*

4 The Organisation requested for Incident 1 to be handled under the Expedited Decision Procedure ("**EDP**"), which the Commission acceded to. After the Commission commenced its investigations into Incident 2, the Organisation likewise requested for this incident to be handled under EDP, which the Commission also acceded to. To this end, the Organisation voluntarily and unequivocally admitted to all the facts set out in this decision, and also to contraventions of sections 24 and 12(a) of the PDPA (as explained below).

Facts of the Case

5 The Organisation is a non-profit, non-governmental organisation which aims to promote consumer interests, and fair and ethical trade practices. Amongst others, the Organisation handles consumer-to-business disputes, where a consumer may engage the Organisation to negotiate with the businesses with a view to reaching an amicable settlement.

6 Personal data in the Organisation's possession or under the Organisation's control involved, amongst others, consumer complaints made to the Organisation. These consumer complaints contained personal data such as the names, email addresses, contact numbers and complaint details.

Incident 1 and Incident 2 (collectively, the "Incidents")

Incident 1

7 For Incident 1, a total of 5,205 phishing emails were sent to 4,945 email recipients from *"online-submission@case.org.sg"* and *"mediator1@case.org.sg"* (collectively, the "**Affected Accounts**").

8 On 8 October 2022, some of the Organisation's consumers received unsolicited emails from *"online-submission@case.org.sg"*, informing them that their complaints had been escalated to the "collections and compensation department", and that they were eligible for a compensation payout. They were requested to click on a chat icon to fill in their banking details to complete the payment process. The account, *"online-submission@case.org.sg"*, was utilised by the Organisation to communicate with consumers who lodge complaints on the Organisation's website ("**Complaint**" or "**Complaints**").

9 Subsequently on 9 October 2022, similar emails were sent from *"mediator1@case.org.sg"* to the Organisation's consumers. The account, *"mediator1@case.org.sg"*, was utilised by the Organisation to communicate with consumers whose complaints were escalated to mediation.

10 Thereafter, in January 2023 and February 2023, the Organisation received complaints of further phishing emails being sent to the Organisation's consumers from email addresses which did not originate from the Organisation's domain. Based on the circumstances, these affected consumers' emails were likely harvested by the threat actor during the course of Incident 1. Further, based on the fact that the threat actor sent phishing emails to these consumers through external email addresses, the Commission considers that personal data relating to these consumers would have been exfiltrated.

11 In connection with the above, 3 of the Organisation's consumers informed the Organisation that they had clicked on the chat icon embedded in the phishing emails, and had money withdrawn from their bank accounts. These individuals allegedly

suffered monetary losses of S$900, S$68,000 and S$149,000. The Organisation had made a police report, and was informed by the police to let them handle the investigations.

12 The phishing emails sent in Incident 1 were generally of the same content and format, did not contain any Complaint-specific details, and consisted of fictitious data.

13 The Organisation engaged a private forensic expert ("**PFE**") to ascertain the cause and extent of Incident 1. The PFE's forensic investigations revealed that:

(a) The threat actor had successfully signed into the Affected Accounts using the correct login credentials.

(b) It is likely that the correct login credentials were obtained from a successful phishing attack on an employee of the Organisation.

(c) By gaining unauthorised access to the Affected Accounts, the threat actor was (1) able to harvest email addresses of the Organisation's consumers from emails in the Inbox and Sent mailboxes of these accounts; and (2) send phishing emails on behalf of the Organisation with the Organisation's verified domain name.

(d) Further, some of the Organisation's computers were running on end-of-life operating systems, and had vulnerable software with unapplied upgrades / security patches, which put the Organisation at risk of remote code execution vulnerability.

14 In terms of the volume of personal data affected in Incident 1, the Commission notes that:

(a) The compromising of the account "*online-submission@case.org.sg"* exposed up to 22,542 email addresses to harvesting by the threat actor. This account was used to send system-generated acknowledgment emails to the Organisation's consumers upon receipt of their Complaints through the Organisation's website.

(b) The other compromised account, *"mediator1@case.org.sg"*, did not contain any data.

(c) Beyond these 22,542 email addresses, investigations did not reveal any further personal data that the threat actor had access to.

Incident 2

15 On 22 June 2023, in the course of investigating the circumstances surrounding Incident 1, the Commission received a complaint from a consumer of the Organisation. The complainant had received a targeted phishing email sent by an email address which did not originate from the Organisation's domain. The email was addressed to the consumer, and reproduced the consumer's Complaint submitted to the Organisation.

16 Subsequently, the Organisation was informed of the occurrence of more of such similar incidents. In total, 28 individuals informed the Organisation that they received phishing emails (reflecting the same details they shared in their original Complaints to the Organisation) from email addresses which did not originate from the Organisation's

domain. Since such data was contained within the Organisation's systems, the unavoidable conclusion is that their personal data (at the very least, their email addresses and Complaints) had been exfiltrated from the Organisation's systems.

17 Whilst the investigations did not yield a definitive conclusion regarding how the data breach in Incident 2 actually occurred, the Commission concludes that based on the circumstances set out below, Incident 2 likely occurred during a data migration exercise conducted by the Organisation.

18 All of the 28 individuals had filed Complaints with the Organisation between 8 January 2019 to 19 December 2019. Investigations found that these Complaints were included as part of a data migration exercise the Organisation undertook when it changed from a former vendor, Exabytes Network (Singapore) Pte Ltd, to a new vendor, Total eBiz Solutions Pte Ltd ("**TES**") (collectively, the "**Vendors**") sometime between 24 December 2019 to 1 January 2020 (the "**Data Migration**"). The Organisation had contacted both Vendors, and there was no evidence of suspicious activity during the weeks preceding the sending of the phishing emails. As such, the Organisation indicated that it was likely that the data breach occurred during the Data Migration, which the Commission accepted.

19 The Commission notes that the personal data of approximately 12,218 individuals involved in the Data Migration was put at risk of unauthorised access and exfiltration.

20 The following types of personal data were affected:

Types of personal data	**Number of affected individuals**
Name, email address, contact number and Complaint details	4,074
Name, email address and contact number	192
Name, contact number and Complaint details	2,012
Name and contact number	1,742
Name, email address and Complaint details	155
Name and email address	52
Contact number	3,991
Total	**12,218**

21 The Commission ascertained and was notified by the Organisation that none of the affected individuals for Incident 2 suffered monetary losses.

Remedial actions

22 Following the Incident, the Organisation took the following remedial actions:

Actions to mitigate and contain Incident 1

(a) Engaged a third party PFE to assist in investigations and perform a vulnerability assessment;

(b) Informed email recipients who had received phishing emails from the Affected Accounts not to click on any links within the email;

(c) Published a media release, and alerts on the Organisation's website and Facebook account to alert consumers to the phishing emails;

(d) Suspended the Affected Accounts, and reset passwords of all administrator accounts with increased complexity requirement; and

(e) Assembled a taskforce to manage the incident, conduct investigations, and provide recommendations to improve the cybersecurity of the Organisation.

Actions to mitigate and contain Incident 2

(a) Informed consumers not to click on phishing emails, and remained in communication with the 28 consumers who had informed the Organisation of the phishing emails; and

(b) Published a media release, and alerts on the Organisation's website and Facebook account to alert consumers to the phishing emails.

Actions to prevent recurrence or similar incidents

(a) Implemented multi-factor authentication ("**MFA**") for all web-based applications including Customer Relationship Management ("**CRM**") software;

(b) Procured a security package against malware, spams, and phishing emails;

(c) Implemented enhanced password strength / complexity requirements, and mandatory password change for all mailboxes every 3 months;

(d) Reviewed and tightened access rights to system functions;

(e) Implemented measures to ensure that contracts with all outsourced vendors include data protection clauses, and that vendors comply with

the PDPA and the Organisation's standard operating procedures for handling personal data;

(f) Implemented data protection training for all new staff, and annual refresher training for all existing staff;

(g) Decommissioned all end-of-life devices;

(h) Installed patch management software for security updates to be pushed through remotely;

(i) Arrangements are being made for the Organisation to obtain the Cyber Essentials Mark and subsequently the Data Protection Trust Mark; and

(j) Arranged to perform a penetration test to identify cybersecurity gaps after the vulnerabilities identified by the PFE have been rectified.

Findings and Basis for Determination

23 Based on the circumstances of the Incidents, the Commission's investigation centred on whether the Organisation had breached its obligations under Section 24 of the PDPA to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**"). Further, as the Organisation indicated that it did not have any Information and Communications Technology ("**ICT**") policies in place, the

Organisation's compliance with Section 12 of the PDPA (the "**Accountability Obligation**") was also investigated.

24 The issues for determination are as follows:

(a) Whether the Organisation had complied with its obligations under the Protection Obligation.

(b) Whether the Organisation had complied with its obligations under the Accountability Obligation.

Whether the Organisation had complied with its obligations under the Protection Obligation

25 To comply with the Protection Obligation, an organisation must implement security arrangements that are reasonable and appropriate in the circumstances. This includes a consideration of the nature of the personal data in the Organisation's possession and control, as well as the potential impact that unauthorised disclosure of the personal data might have on the affected persons[2].

Inadequate enforcement and formulation of password policies

26 Poor management of accounts and passwords are one of the most common causes of data breaches. As a necessary measure of data protection, organisations must adopt, implement, and **enforce** a strong and robust password policy[3] to ensure

[2] See the Commission's Advisory Guidelines on Key Concepts in the PDPA (Revised 16 May 2022) at [17.2].
[3] See *Cognita Asia Holdings Pte Ltd* [2022] SGPDPCS 14 at [7].

that their IT systems are not vulnerable to common hacking attempts such as brute force attacks[4].

27 In terms of basic practices, a password policy should include reasonable password controls such as mandating a minimum level of password complexity and/or length, and enforcing a maximum validity period for a password, the duration of which is in turn tied to the complexity of the password[5]. Having set an internal password policy, it is incumbent on an organisation to enforce its password policy to ensure compliance.

28 The Commission takes the view that the Organisation's password management policy was manifestly insufficient to safeguard the personal data in its possession. First, the Organisation did not enforce its own password policy. Investigations disclosed that the Organisation's password policy required (i) a minimum length of 8 characters for passwords; and (ii) a mixture of alphabets and numbers (the "**Password Complexity Policy**"). However, the password for one of the Affected Accounts was *"olse432"*, which has 7 characters and would not have satisfied the Organisation's Password Complexity Policy. Yet, this password was in use because the Organisation did not system-enforce its Password Complexity Policy requirements.

29 Second, the Organisation admitted that it failed to adopt and enforce a policy on how frequently the passwords ought to be changed. The Affected Accounts were created in January 2019 and February 2019, and the passwords for both Affected Accounts had remained unchanged for almost 4 years prior to Incident 1. In the Commission's view, if the Organisation had formulated a password policy setting out

[4] See *LoveBonito Singapore Pte Ltd* [2022] SGPDPC 3 at [18].
[5] See the Commission's Guide to Data Protection Practices for ICT systems.

how long a password would remain valid and how frequently the password ought to be changed as a result, it is unlikely that the period of 4 years would have been deemed reasonable. The Organisation's failure to adopt and enforce a password policy that included the maximum validity period for a password was a serious lapse of its obligation to protect the personal data in its possession or control by adopting reasonable security arrangements.

30 As a result of the above weaknesses, the threat actor successfully managed to access the Affected Accounts, resulting in the data breach that occurred in Incident 1.

31 The Organisation accepted that it had failed to (i) enforce its own Password Complexity Policy requiring the use of passwords of sufficient complexity, and (ii) adopt and enforce a password policy that requires the login passwords to be changed at a fixed duration.

32 For the above reasons, and by the Organisation's own admissions, the Organisation is found to have breached the Protection Obligation by failing to implement and enforce an adequate password policy to protect the personal data in its possession or under its control.

Failure to stipulate clear security responsibilities in contracts with the Organisation's Vendors

33 The Commission had highlighted in previous decisions the need for an organisation to put in place appropriate contractual provisions with its data intermediaries that set out the obligations and responsibilities of the data intermediary to protect the organisation's personal data, and the parties' respective roles to protect

the personal data[6]. This applies to all cases where service providers / vendors process personal data on behalf of a data controller.

34 Further, in the Commission's handbook on *How to Guard against Common Types of Data Breaches*[7], it is recommended that organisations establish clear responsibility for ICT security. Where such responsibilities are to be carried out by a vendor, the scope of work and area of responsibilities ought to be clearly stated in the contract.

35 As highlighted at [18] above, Data Migration took place between the Organisation's Vendors between 24 December 2019 to 1 January 2020.

36 However, investigations revealed that the Organisation's contract with one of the Vendors involved did not stipulate clear security responsibilities in relation to its ICT systems or data.

37 In relation to TES, the Organisation indicated that it had engaged TES to develop a customised CRM solution based on off-the-shelf software. The Organisation indicated that TES was required to conduct proactive monitoring to identify possible unauthorised access or disclosure and inform the Organisation of any possible system breach. However, the contract with TES did not contain any provisions for cybersecurity protection services and such security responsibilities were not expressly specified in the contract between the Organisation and TES.

---

[6] See *Re Singapore Health Services Pte Ltd & Ors* [2019] SGPDPC 3 at [59]; *Times Software Pte Ltd and others* [2020] SGPDPC 18 at [19] and *Re Smiling Orchard (S) Pte Ltd and Ors* [2016] SGPDPC 19 at [45].

[7] See the Commission's handbook on *How to Guard against Common Types of Data Breaches* (at page 13).

38 On this basis, the Organisation admits negligence in failing to manage its vendor closely.

39 Whilst the investigations did not definitively conclude how the threat actor gained unauthorised access to the affected personal data in Incident 2 during the Data Migration, the Organisation's negligent vendor management put personal data under its control at risk of unauthorised access and disclosure.

40 For the above reasons, and by the Organisation's own admissions, the Organisation is found to have breached the Protection Obligation by failing to stipulate clear security responsibilities in the contracts with the Vendors.

Failure to conduct staff training

41 In *Tanah Merah Country Club* [2021] SGPDPCS 16, the Commission had emphasised that staff training is a critical and necessary component to ensure that an organisation is well placed to protect the personal data in its possession and/or control. The Protection Obligation extends to and includes the training of all employees who have to handle personal data in the course of their work so that an organisation's employees can then successfully adopt and implement the policies and best practices necessary to ensure the protection of personal data in an organisation's possession and/or control[8].

42 In this regard, the Organisation admitted that it had failed to conduct regular security awareness training for its staff. The Organisation had last conducted data protection training in 2017, around 5 years before Incident 1. Since then, there had not

[8] See *Tanah Merah Country Club* [2021] SGPDPCS 16 at [13].

been any other training including but not limited to proper device usage or cybersecurity awareness. While the Organisation's IT department would send out email alerts to its staff from time to time to warn staff against phishing attacks, this alone, in the absence of regular security awareness training for its staff was inadequate.

43 This lack of adequate staff training to address cybersecurity risks rendered the Organisation more vulnerable to risks that target its staff, such as phishing attacks. Indeed, the Organisation admitted that the credentials for the Affected Accounts were likely leaked by successful phishing attacks.

44 More should have been done by the Organisation to build awareness and educate its staff on the potential cyber security risks, including risks of phishing attacks.

45 For the above reasons, and by the Organisation's own admissions, the Organisation is found to have breached the Protection Obligation by failing to conduct adequate staff training.

Whether the Organisation had complied with the Accountability Obligation

46 The Accountability Obligation requires organisations to undertake measures in order to ensure that they meet their obligations under the PDPA and, importantly, demonstrate that they can do so when required[9]. One such requirement is Section

[9] See the Commission's Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Revised 16 May 2022) at [21.2].

12(a) of the PDPA which requires an organisation to develop and implement policies and practices that are necessary to meet its obligations under the PDPA.

47 During investigation, the Organisation confirmed that prior to Incident 1, it did not have any ICT policies to cover critical aspects in IT security (including aspects of applying security patches / software updates). The Organisation admitted it had simply "relied on its IT staff to conduct maintenance and updates, as and when necessary".

48 This was manifestly inadequate. In *Re Marshall Cavendish Education Pte Ltd* [2019] SGPDPC 34, the Commission had stressed that "relying solely on employees to perform their tasks diligently is not a sufficient reasonable security arrangement, and the organisation would need to take proactive steps to protect personal data".[10]

49 Investigation also revealed that:

(a) There were insufficient email security measures. In this regard, inadequate email security solutions may fail to detect or prevent suspicious login attempts or unauthorized access.

(b) The Organisation did not have in place sufficient logging and monitoring practices to detect suspicious or unusual activities or unauthorized access promptly.

(c) There were no controls internally to monitor the security of the Organisation's systems. The Organisation did not have a documented IT

[10] See *Re Marshall Cavendish Education Pte Ltd* [2019] SGPDPC 34 at [21].

Infrastructure management plan or process for the protection and security of its systems.

(d) The Organisation admitted that it had not performed any security reviews of its systems in the 3 years preceding Incident 1.

50 As a result of the Organisation's lack of such policies, it was discovered by the PFE that more than 30 out of the Organisation's 45 computers had critical and high-risk vulnerabilities which put the Organisation at risk of threat actors compromising or exploiting the systems.

51 For the above reasons, and by the Organisation's own admission, the Commission finds that the Organisation has failed to meet its obligations under section 12(a) of the PDPA.

The Deputy Commissioner's Decision

52 In determining 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.

53 In terms of the type and nature of the personal data affected by the Organisation's non-compliance:

(a) In relation to Incident 1, the Commission notes that given the nature of the usages of the Affected Accounts, the threat actor was confined to accessing and harvesting the email addresses of the Organisation's consumers contained in the emails in the Inbox and Sent mailboxes of

these accounts. In this regard, the threat actor was able to harvest up to 22,542 email addresses.

(b) In relation to Incident 2, the Commission notes that that the personal data of approximately 12,218 individuals was put at risk of unauthorised access and exfiltration. The personal data affected included a combination of names, email addresses, contact numbers and Complaint details. Some targeted phishing emails sent in Incident 2 aimed at causing financial losses to the affected individuals, and used the relevant Complaint details exfiltrated to appear more convincing and legitimate. This exposed the affected individuals to greater risks of actual financial losses.

54 In terms of the nature, gravity and duration of the non-compliance by the Organisation, the Organisation's breach of the Protection Obligation and Accountability Obligation in relation to both Incidents continued for a long duration of more than three years. Additionally, there was a dearth of basic policies or security measures to safeguard the personal data in the Organisation's possession and/or control, and ensure compliance with the PDPA such an ICT policy to cover critical aspects such as patching or proper staff training.

55 Notwithstanding the above, the Commission recognises that in relation to both Incidents:

(a) The Organisation took prompt actions after being alerted about the Incidents to mitigate the effects of the Incidents and to prevent a recurrence;

(b) Investigations were handled under the EDP, under which the Organisation admitted to the facts set out in this decision and to its contraventions of the Protection Obligation and Accountability Obligation; and

(c) The Organisation was cooperative with the Commission's investigations.

56 Further, for the purposes of assessing what amount of financial penalty would be effective to deter non-compliance with the PDPA, the Commission also took into consideration the size of the Organisation's annual turnover[11].

57 Based on the above, the Commission determined that the Organisation should pay a financial penalty of $20,000 within 30 days from the date of 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.

58 Having considered all the relevant factors of this case, the Organisation is hereby directed to take the following actions:

(a) Review and update policies relevant to personal data protection, including the Organisation's ICT policy and password policy;

(b) Rectify all security gaps identified by the PFE by:

[11] See *Re Fullerton Healthcare Group Pte Limited and Agape CP Holdings Pte Ltd* [2023] SGPDPC 5 at [39].

(i) Applying all third-party patches and/or renewing the third-party applications with the most updated versions;

(ii) Applying all Microsoft security and software patches to address the identified vulnerabilities;

(iii) Enabling all necessary security settings to protect endpoints; and

(iv) Ensuring proper configuration of service paths and to align their system's setup with the Organisation's corporate IT policies; and

(c) Update the Commission within 1 week from the completion of the above.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION