PERSONAL DATA PROTECTION COMMISSION

[2024] SGPDPC 1

Case No. DP-2304-C0943

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

And

Horizon Fast Ferry Pte. Ltd.

… *Organisation*

DECISION

Horizon Fast Ferry Pte. Ltd.

[2024] SGPDPC 1

Denise Wong, Deputy Commissioner - Case No. DP-2304-C0943

21 February 2024

Introduction

1. On 25 April 2023, Horizon Fast Ferry Pte. Ltd. (the "**Organisation**"), a Singapore-based ferry operator, that provides ferries between Singapore and Batam, Indonesia, notified the Personal Data Protection Commission (the **"Commission"**) that there had been unauthorised access and exfiltration of the personal data of 108,488 individuals who booked tickets on the Organisation's website from its server (the **"Incident"**).

2. The personal data affected included the individuals' name, passport number, date of birth, passport issue and expiry date, nationality, email address (if provided) and telephone number (if provided).

3. The Organisation requested, and the Commission agreed, for this matter to be handled under the Commission's Expedited Decision Procedure. This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out in this Decision and that it was in breach of section 24 of the Personal Data Protection Act 2012 (the "**PDPA**").

4. Section 24 of the PDPA requires an organisation to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks (the "**Protection Obligation**").

Facts of the Case

5. The Organisation admitted that it does not have its own Information Technology ("**IT**") department. The Organisation relied informally on the goodwill of a single individual (the "**IT Supervisor**") employed by an overseas IT vendor (the "**IT Support Vendor**") who had access to the Organisation's IT systems to provide IT support.

6. The Organisation did not have any service contract with the IT Support Vendor. The IT Support Vendor was in fact engaged by PT Prima Sembilan, the Organisation's ticket sales partner in Batam, to provide IT services.

7. The IT Supervisor also acted on the Organisation's behalf to liaise with other contractors engaged by the Organisation – first, PT Mareco Prima Mandiri ("**Contractor I**") which was engaged in 2019 to set up the Organisation's website, and subsequently, PT Rintas Inovasi Indonesia ("PTRII") ("**Contractor II**") which was engaged from 1 June 2022 to maintain and service the Organisation's website before the termination of this contract on 22 November 2022. For clarity, the Commission should add that the Organisation engaged Contractor II to maintain and service its website as the key personnel from the Contractor I who had helped to set up the Organisation's website founded Contractor II.

8. The Organisation admitted that the Incident occurred because valid credentials to its Ubuntu operating system root account (the "**Root Account**"), which is akin to a super-user account, had been misused to gain unauthorised access to the personal data in the Organisation's possession and/or control.

9. Access to the Root Account had initially been granted to Contractor I to set up the Organisation's website in 2019. When Contractor I claimed that the Root Account was no longer accessible sometime in 2019, the IT Supervisor sought to verify this claim and tried to login to the Root Account but was unable to do so. The IT Supervisor then assumed that the Root Account was no longer accessible.

10. When the Organisation terminated its website maintenance and servicing contract with Contractor II on 22 November 2022, the IT Supervisor acted on the Organisation's behalf to acknowledge the receipt of certain items related to the project. However, as can be seen from the Incident, the user credentials of the Root Account remained active and was used to gain unauthorised access to the Organisation's system. The IT Supervisor was once again not able to verify if the credentials for the Root Account had been disabled or reassigned to him.

11. It is also relevant to add that after the termination of its contract with Contractor II, the Organisation did not have any contract in force with any other IT vendor from 22 November 2022 till the time of the Incident.

12. From 19 March 2023 onwards, the Organisation received several ransomware emails which revealed that personal data of the Organisation's customers had been exfiltrated. The threat actor demanded payment in exchange for fixing the vulnerability in the Organisation's system. The Organisation's internal investigations revealed that

valid credentials for the Root Account had been used to gain unauthorised access to the Organisation's server. Upon making this discovery on 29 March 2023, the IT Supervisor promptly changed the credentials for the Root Account on the same day.

13. The Organisation admitted that the IT Supervisor's lack of familiarity with the Ubuntu operating system led the latter to mistakenly believe Contractor I's claim that the Root Account was no longer active, and that the Contractors involved had only been able to login to the Organisation's system through a different customer account.

Remedial Action

14. After the Incident, the Organisation took the following remedial actions:

a. Engaged a cyber incident response vendor to perform digital forensics investigations and implemented all the recommendations made by the vendor to improve its cybersecurity;

b. Engaged a vendor to develop a new website; and

c. Conducted penetration testing on the new website and rectified all the vulnerabilities identified before the website's launch.

15. The Organisation also informed the Commission that it would take the following remedial actions:

a. Train its managers on the obligations and requirements of the PDPA. The IT Support Vendor and the current web development vendor will also be invited to attend the training;

b. Enter into a written agreement with the IT Support Vendor for the access and management of the Organisation's systems and website. The Organisation will require the IT Support Vendor to designate a staff member with the relevant IT knowledge required;

c. Enhance its internal guidelines on data protection; and

d. Develop guidelines and protocols for its vendors, outlining the procedures for handling personal data and establishing processes for access, password management and other security measures.

Findings and Basis for Determination

16. As the Organisation is in possession of the personal data of its customers, the Organisation is required to comply with all the data protection obligations under the PDPA, including making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks, pursuant to section 24 of the PDPA. This is regardless of whether the Organisation engaged a data intermediary as defined under the PDPA or an external IT vendor.

17. For completeness, we would add that based on the admissions made by the Organisation, the IT Support Vendor and the Contractors involved did not carry out any processing activities with regards to personal data on the Organisation's behalf such that they would fall within the definition of a "data intermediary" under section 2(1) of the PDPA.

18. For the reasons set out below, the Deputy Commissioner determines that the Organisation failed to implement reasonable security arrangements to protect the personal data in its possession and/or control, thus acting in breach of section 24 of the PDPA. In particular, the Organisation failed to:

a. Ensure the proper management of the IT Support Vendor by having written policies and procedures for vendor management;

b. Implement an Information and Communications Technology ("**ICT**") policy that covers the critical aspects of IT security; and

c. Ensure that security solutions were implemented for its web server.

Poor Vendor Management

19. The Organisation admitted that it did not have any written policies and procedures for vendor management or policies relating to how outsourced vendors should ensure the protection of personal data when handling personal data.

20. The Organisation admitted that even though it relied on the IT Support Vendor to provide IT support and to act on its behalf when liaising with external vendors such as the Contractors involved, the Organisation failed to define and capture the job scope, responsibilities and competencies required of key personnel through a formal contractual agreement with the IT Support Vendor.

21. The importance of clarifying the obligations of an organisation and a service provider had been made by the Commission in several cases. In *Re Smiling Orchid (S) Pte Ltd*[1]*,* the Deputy Commissioner stated at [51] of the decision as follows:

> "Data controllers that engaged outsourced service providers have to be clear about the nature and extent of services that the service provider is to provide. There must be a clear meeting of minds as to the services that the service provider has agreed to undertake, and this should be properly documented. Data controllers should follow through with the procedures to check that the outsourced provider is indeed delivering the services."

22. In the handbook titled *How to Guard* against *Common Types of Data Breaches* issued by the Commission in May 2021[2], the Commission had identified the failure among organisations to establish clear responsibility for ICT security as one of the top five most common gaps leading to a data breach based on an analysis of past cases. In the handbook, the Commission recommended that organisations should establish clear responsibility for ICT security to either an assigned person or team. Further, where ICT security is to be performed by a vendor, the scope of work and areas of responsibilities should be clearly stated in a contract.

23. The Organisation admitted that it failed to ensure that the IT Support Vendor had personnel who were sufficiently familiar with the Ubuntu operating system so that they could perform basic system administrator functions like access management. As a result, the Organisation was not aware at the time of the Incident that the Root

[1] [2017] PDP Digest 133.
[2] Available at https://www.pdpc.gov.sg/news-and-events/announcements/2021/05/handbook-on-how-to-guard-against-common-types-of-data-breaches-now-available (as at 14 December 2023).

Account had remained active. Competent vendor administration of the Organisation's Ubuntu operating system would have reasonably reduced the risk of the Incident occurring.

Failure to implement an ICT policy that covers critical aspects of IT security

24. The Organisation also admitted that it did not have any ICT policy at the time of the Incident. In its *Checklists to Guard Against Common Types of Data Breaches*, the Commission recommends at page 6 that organisations, as a ***basic practice***, "*develop an ICT policy that covers the critical aspects in IT security such as account and access control, password, email, IT risk management, asset and configuration, backup and recovery, hardening and patching*".

Failure to implement security solutions on its web server

25. The Organisation further admitted that it had not implemented any security solutions on its web server at the time of the Incident. As stated in the Commission's *Checklists to Guard Against Common Types of Data Breaches* at page 10, organisations should, as a ***basic practice***, equip networks with defence devices such as firewalls to protect computer networks connected to the Internet.

26. Examples of security solutions that the Organisation could have implemented includes web application scanning, which might have reduced the likelihood of the Incident occuring. However, the Organisation simply assumed that the Contractor II would conduct regular web application scanning despite this not being specified in their contract with Contractor II. In any case, the contract had already been terminated

a few months before the Incident, and the Organisation did not have any contract in force with any IT vendor to do so at the material time.

27. For the reasons given above, the Organisation is found to have breached the Protection Obligation under section 24 of the PDPA.

The Deputy Commissioner's Decision

28. In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and if so, the amount of such financial penalty, the Commission considered the factors listed at section 48J(6) of the PDPA.

29. The Commission considered that the data breach affected 108,488 individuals and that the type of personal data affected included the passport details. The Organisation's non-compliance with section 24 of the PDPA was also serious as the Organisation had failed to implement basic levels of data protection policies and practices.

30. Furthermore, this was not the Organisation's first instance of non-compliance with the PDPA. A financial penalty of $54,000 had previously been meted on the Organisation in the Commission's decision dated 25 July 2019 for a personal data breach on the Organisation's website. More recently, the Commission issued a warning to the Organisation on 16 October 2020 for failing to have reasonable security arrangements to protect the personal data in the Organisation's email account.

31. The Commission nevertheless recognises the following mitigating factors:

a. The Organisation cooperated with the Commission in the course of its investigations and took prompt remedial actions to address the Incident.

b. The Organisation voluntarily accepted responsibility for the Incident, thus facilitating the expeditious investigation and resolution of this case through the Expedited Breach Procedure.

32. Having considered all the factors listed above, the Deputy Commissioner hereby finds the Organisation in breach and directs the Organisation to pay a financial penalty of S$28,000 within 30 days from the notice accompanying date of this decision, failing which interest at the rate specified in the Rules of Court in respect of judgement debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

33. The Organisation is also directed to provide written confirmation to the Commission that it has implemented the remedial measures described at paragraphs 15(a) to 15(d) above, by 31 March 2024.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION