## Breach of the Protection Obligation by Payroll2U Pte. Ltd.

## [2024] SGPDPCS 2

| **Case Number** | : | DP-2303-C0848 |
| --- | --- | --- |
| **Decision Date** | : | 07 March 2024 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | [Wong Huiwen Denise](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/result-page?p_p_id=legalresearchresultpage_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchresultpage_WAR_lawnet3legalresearchportlet_action=browseByCoramAuthorMP&typeOfBrowse=browseByCoram&filtering=Wong%20Huiwen%20Denise&searchFacetName=Coram) |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Payroll2U Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements* – *Failure to implement reasonable access controls*

1. Payroll2U Pte. Ltd. (the “**Organisation**”) is a payroll service provider that offers payroll outsourcing services and online payroll Software as a Service (SaaS) solutions.

2. On 27 March 2023, the Personal Data Protection Commission (the **“Commission”**) was notified by the Organisation that the personal data of its client’s employees had been posted on a ransomware leak site. The leak arose from a ransomware attack on the servers of the Organisation around 29 December 2022 (the **“Incident”**).

3. On 16 January 2023, the Organisation received extortion emails from a threat actor identified as a LockBit affiliate. The Organisation immediately conducted an internal investigation and engaged an external forensics investigator to investigate the Incident and undertake remedial actions. Upon further investigations, it was determined that a total of 81.95 GB of data had been exfiltrated in the Incident and posted on the dark web. The personal data of 5,640 employees from the Organisation’s client was affected, including their full name, bank account number, salary information, NRIC number, address, date of birth and email address.

4. Investigations revealed that unauthorised activity had occurred from 29 December 2022 to 16 January 2023, with a single compromised account used for Remote Desktop Protocol (RDP) access to five servers on the Organisation’s AWS environment. Once connected to the working network, the threat actor gained unauthorised access to the developer’s drive and the company’s shared drive that were both mapped to the compromised account. These drives gave access to the affected personal data.

5. While the investigations were unable to conclusively determine how the threat actor obtained the credentials to the compromised user account, the investigation revealed the following lapses that could have contributed to the Incident:

a. Employees were given local administrator rights on their laptops, thus enabling a user to install/uninstall applications without restriction. The Organisation confirmed that the compromised user had reformatted his laptop and installed an unlicensed Windows Operating System that might have downloaded ransomware and removed the Symantec Endpoint Protection. In addition, the compromised user also left the computer powered and web connected, allowing the threat actor to use the account to login to the Remote Desktop Servers.

b. Multi-Factor Authentication (“**MFA**”) was not implemented for administrator accounts and non-administrative accounts with access to personal data.

c. There was an absence of tools to detect and remove the download of unauthorised software on company-issued laptops.

d. There was an absence of effective incident response and management control, enabling the threat actor’s presence and activity within the Organisation’s network to remain undetected between 29 December 2022 to 16 January 2023.

6. Following the Incident, the Organisation took the following remedial action:

a. Deactivated the compromised user account and forced change password for all users accessing the network.

b. Implemented MFA for users accessing internal and remotely accessible resources and environments.

c. Implemented documentation and quarterly review of Windows network drives and folder access. Collected log details and log reviews on a monthly basis.

d. Conducted checks on all workstations to ensure they are equipped with SentinelOne and Symantec Endpoint Protection (SEP).

e. Implemented host-checking for SSL VPN users vis FortiClient to verify that the SentinelOne and SEP processes are running before granting the device access.

f. Reviewed firewall configurations and rules. Fine-tuned web-filtering using Fortinet UTM. Implemented secured file transfer for inbound and outbound traffic. Block sharing over cloud storage and whitelisted URLs based on need to use basis.

g. Performed regular service account reviews to validate that all active accounts are authorised.

7. The Organisation requested for the matter to be handled under the Commission’s Expedited Breach Decision Procedure (“**EDP**”). This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out below; and admitted that it was in breach of section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”).

8. The Organisation admitted that it failed to implement reasonable access control. While the investigation noted and acknowledged the existence of proactive cybersecurity controls, the Organisation also admitted to storing the affected personal data sets that included the bank account numbers and salary information on unsecured internal shared drives. Given both the volume and types of personal data handled, the Organisation ought to have adopted additional access control beyond the baseline of password protection.

9. The Organisation had the option of either frontend access control or other options that focused on the backend. Frontend access control included MFA, at least for users with remote access to the more sensitive data mentioned. Backend access control included, for example, restrictive allocation according to the user’s need for administrator-level rights that would impact personal data security as well as network segmentation. Sensitive personal data could have been stored in segments of the network that allowed access only on the basis of need.

10. As stated in the Commission’s Guide to Data Protection Practices for ICT Systems (the “Guide”)[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/113430.xml&queryStr=(personal%20data%20protection%20act)#fn1), access control privileges should be restricted and defined based on the user roles/rights to data. Users should not be able to see information that they do not need to know, and this should be reflected in an organisation’s access control policy. In the present case, the Organisation should have assessed whether the developer in question needed account access rights to personal data of the type affected in the Incident.

11. Another backend access control option recommended in our Guide was disallowing non-administrator employees from installing software and/or changing security settings and restricting the right to do so to specific administrator accounts. The Organisation failed to do so and non-administrative accounts were able to download unauthorised software on issued devices without being detected.

12. For the above reasons, the Organisation was determined to have breached the Protection Obligation.

**The Deputy Commissioner’s Decision**

13. In determining whether the Organisation should be required to pay a financial penalty under Section 48J of the PDPA or if directions would suffice, the Commission considered that a financial penalty was appropriate given the role of the Organisation as a payroll service provider and the types of personal data handled. In deciding the appropriate financial penalty amount, the Commission first considered all the relevant factors listed at Section 48J(6) of the PDPA, in particular, the impact of the personal data breach on the individuals affected and the nature of Organisation’s non-compliance with the PDPA.

14. In deciding what would be the appropriate financial penalty amount, the Commission also considered the Organisation’s turnover to arrive at a figure that would be a proportionate and effective amount, to ensure compliance and deter non-compliance with the PDPA. The Commission also considered the following mitigating factors, which led to a further reduction in the financial penalty:

a. The Organisation was cooperative during the course of our investigations;

b. The Organisation voluntarily admitted to a breach of the Protection Obligation under the Commission’s Expedited Decision Procedure; and

c. This is the Organisation’s first instance of non-compliance with the PDPA.

15. For the reasons above, the Commission hereby requires the Organisation to pay a financial penalty of $4,000 within 30 days of the date of the relevant 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.

## Breach of the Protection Obligation Academy of Medicine Singapore

## [2024] SGPDPCS 4

| **Case Number** | : | DP-2308-C1326 |
| --- | --- | --- |
| **Decision Date** | : | 10 June 2024 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | [Wong Huiwen Denise](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/result-page?p_p_id=legalresearchresultpage_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchresultpage_WAR_lawnet3legalresearchportlet_action=browseByCoramAuthorMP&typeOfBrowse=browseByCoram&filtering=Wong%20Huiwen%20Denise&searchFacetName=Coram) |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Academy of Medicine Singapore |

*Data Protection* – *Protection obligation* – *Unauthorised access to and disclosure of personal data* – *Insufficient administrative and technical security arrangements*

1 Academy of Medicine Singapore (the “**Organisation**”) is a professional institution providing postgraduate medical education and specialist training in Singapore. On 4 August 2023, the Personal Data Protection Commission (the “**Commission**”) was informed about a data breach incident involving the Organisation’s servers being infected by ransomware on or about 13 July 2023. Consequently, personal data of 6,574 individuals had been exfiltrated and posted on the dark web (the “**Incident**”).

2 The Organisation requested, and the Commission agreed, for the investigation to proceed under the Expedited Decision Breach Procedure. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision. It also admitted to a breach of the Protection Obligation under Section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”).

**Facts of the Case**

3 The Organisation first discovered malware artifacts in its servers after reports by staff members of network connectivity issues on 13 July 2023. The Organisation immediately disconnected the affected servers and sought an external IT forensic investigator to investigate the extent of the Incident and undertake remedial action.

4 Investigations revealed that data from the Organisation had been uploaded on the dark web (the “**Leaked Data**”), including full credit card information of over 1,000 individuals. Separately, a total of 4.4TB of files in the Organisation’s servers had been encrypted due to ransomware deployment.

5 From system event logs, upon gaining initial entry the threat actor accessed 6 servers (the “**Affected Servers**”) and 1 staff computer using Remote Desktop Protocol (“**RDP**”) connections, then deployed malicious tools that could harvest credentials within folders and disarm antivirus and threat detection software. The investigation revealed the following lapses which could have contributed to the Incident:

(a) The Organisation’s firewall FortiOS had not been patched since July 2021 and had been susceptible to a critical severity attack[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/113918.xml&queryStr=(personal%20data%20protection%20act)#fn1) which could be exploited at pre-authentication to allow a remote attacker to gain entry to systems without using credentials.

(b) Endpoint Detection and Response (“**EDR**”) applications installed on the Affected Servers and devices did not detect and prevent the execution of malicious tools. The EDR Manager was compromised early and disabled by the threat actor before executing ransomware and file encryption.

(c) The Organisation’s environment was highly vulnerable to exploitations due to operating systems in 2 of the Affected Servers having reached End-of-Life stages in July 2015 and January 2020 respectively.

(d) Critical hosts and staff computers had not been regularly scanned for vulnerabilities.

(e) There had been a lack of essential threat detection solutions and proper logs retention as EDR applications installed in the Organisation’s environment either could not be supported by its operating systems or had outdated network signatures[[note: 2]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/113918.xml&queryStr=(personal%20data%20protection%20act)#fn2).

(f) There had been a lack of documented robust processes implemented at the time of the Incident to ensure regular patching and updates of important software.

6 The Organisation informed the Commission that the exfiltrated data contained personal data of 6,574 current and former members, participants of events, activities and/or in-training examinations organised/administered by the Organisation. The types of affected personal data are set out below. Not every affected individual had all of the personal data below in their personal data sets.

i. Name;

ii. Address;

iii. Personal email address;

iv. Telephone number;

v. NRIC number;

vi. Passport number;

vii. Photograph number;

viii. Photograph (ID photo);

ix. Date of birth; and

x. Financial information, including bank account details, partially redacted credit card numbers, and credit card numbers with CVV and expiry date of 1,083 individuals.

7 The Commission’s analysis of the Leaked Data by the threat actor found that it had contained approximately 12.7GB of data from the Organisation. It was observed that bank account details and credit card numbers with CVV and expiry dates had been stored in clear text without password protection or current standard file encryption. A list of login credentials to various online platforms used by the Organisation could also be found within the Leaked Data, including credentials to its website management system and passwords to various administrative emails.

*Remedial Action*

8 Following the Incident, the Organisation promptly notified the affected individuals about the Incident. The Organisation also took the following remedial actions:

(a) Activated a Crisis Response Team to facilitate forensic investigations and address queries related to the Incident;

(b) Notified the relevant authorities i.e. Singapore Police Force, Cyber Security Agency of Singapore and Ministry of Health of the Incident;

(c) Replaced its outdated firewall firmware to a newer version;

(d) Tightened access controls by enabling geo-blocking on the firewall and VPN configured to only allow access to its networks via local IP addresses;

(e) Installed and activated two-factor authentication for all staff members;

(f) Implemented Action 1 Patch Management that automated vulnerability remediation for operating systems and third-party applications, and continuous patch compliance for all servers;

(g) Implemented monthly checks on system and software patches;

(h) Conducted vulnerability scans on all staff-issued computers and devices;

(i) Restored files from their tape backup and performed malware scans of the restored files and all staff-issued laptops and devices; and

(j) Engaged a third-party vendor to provide credit monitoring services to affected individuals at no charges, whose financial information had been affected in the Incident, to help detect any suspicious transactions that might affect the affected individuals’ credit reputation.

**Findings and Basis for Determination**

*Whether the Organisation had contravened the Protection Obligation*

9 Under section 24(a) of the PDPA, organisations must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks.

10 The Organisation’s admissions amounted to the following breaches of section 24 of the PDPA:

(a) *Lack of sufficiently robust processes for updates or upgrades of important software or firmware*, which resulted in vulnerabilities that were not removed in the Organisation’s firewall and servers. The Organisation said that its IT vendor at the time of the Incident had only been onboarded in April 2023 and had been focused on troubleshooting issues that arose in 2 events of system downtime in May and June 2023. Prior to the system downtimes, the Organisation also conducted an IT infrastructure review completed on 26 June 2023 that included identifying obsolete devices to remove and improving network security. Hence, written procedures or policies on patch management for software and firmware had yet to be developed and implemented at the time. However, the Commission determined that these circumstances did not mitigate the lack of sufficiently robust processes for updating or upgrading important software and firmware that saw firewall patches not being carried out since July 2021 and servers with End-of-Life (“**EOL**”) operating systems not being upgraded.

(b) *Failure to have reasonable access control*, in response to the need to enhance access control to the type of financial information in its possession or under its control. This financial information had included credit card numbers with their security codes (CVVs). These had been stored in servers in plain text without password protection. Given the risk of harm due to the nature of this personal data, the Organisation could have considered additional security options to enhance access controls to protect this data. The Commission highlighted in *Re* *Tokyo Century Leasing (Singapore Pte Ltd [2023] SGPDPC 9* in paragraph 11 that such data has a heightened risk of identity theft and/or financial loss, which called for a higher standard of security arrangements. Examples may include separate password protection for the server holding this data, encryption of the data, restrictions to the export of this data, or, given the Organisation’s choice of endpoint security solutions, real-time security monitoring of the data server.

(c) *Failure to stipulate data protection requirements or clear job specifications in the contract of its IT vendor*, specifically in the areas of the management and maintenance of IT system security and the conduct of security reviews. Where organisations rely on vendors to perform IT security maintenance and/ or review, the scope of these services must be stipulated in the vendor contract as part of the duty of a data controller under the Protection Obligation.

11 For the above reasons, the Organisation was determined to have breached the Protection Obligation.

**The Deputy Commissioner’s Decision**

12 In determining whether the Organisation should be required to pay a financial penalty under Section 48J of the PDPA, the Commission considered all relevant factors listed at Section 48J(6) of the PDPA, in particular, the impact of the personal data breach on the individuals affected and the nature of Organisation’s non-compliance with the PDPA.

13 The Commission considered that the personal data of 6,574 individuals had been affected as a result of the above breach. Further, the affected data included financial information comprising of bank account numbers and full credit card information of 1,083 individuals were leaked on the dark web.

14 The Commission also considered the fact that for more than 3 years, the Organisation had continued to deploy vulnerable servers with EOL operating systems for which support and security updates had ceased since July 2015.

15 The Commission considered the following mitigating factors:

(a) The Organisation was cooperative during the course of our investigations;

(b) The Organisation voluntarily admitted to breach of the Protection Obligation under the Commission’s Expedited Decision Procedure; and

(c) This is the Organisation’s first instance of non-compliance with the PDPA.

16 For the reasons above, the Commission hereby requires the Organisation to pay a financial penalty of $9,000 within 30 days of the date of the relevant notices 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.

*Directions*

17 In addition, to ensure the Organisation’s compliance with the Protection Obligation, the Organisation is directed to report to the Commission on the completion of the following remedial actions:

(a) Assess the need for perimeter firewalls to restrict nonstandard outbound port access as per its network requirements and configure said firewalls if needed;

(b) Conduct a thorough security architecture review and assess the need to segregate sections of its network that support primary processing of personal data for its purposes from sections of the network that store personal data to reduce the risk of unauthorised access from within the network;

(c) Assess the need to implement hardening for endpoints, servers and network devices including password policies;

(d) Identify the sensitive personal data stored in its environment and remove or encrypt the information according to data security best practices e.g. the Payment Card Industry Data Security Standards for handling payment card data;

(e) Delete any stored CVV numbers and implement policy against storing CVV numbers after the initial transaction authorisation;

(f) Implement annual periodic security reviews of IT policies, processes and procedures to ensure compliance and alignment with security best practices; and

(g) Prepare and submit to the Commissioner a written report of the

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following section of the Personal Data Protection Act 2012 had been cited in the above summary of the Decision:

**Protection of personal data**

**24.** An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.

[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/113918.xml&queryStr=(personal%20data%20protection%20act)#fnref1) *CVE-2023-27997* is a critical heap buffer overflow vulnerability in Fortinet FortiOS’ SSL-VPN pre-authentication component that is exploitable by attackers to execute arbitrary code.

[[note: 2]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/113918.xml&queryStr=(personal%20data%20protection%20act)#fnref2) Network signatures match patterns of an attack that can crash applications or exploit the operating systems on client computers. It can be changed to block or allow traffic.

## Breach of the Protection Obligation by Whiz Communications

## [2023] SGPDPCS 7

| **Case Number** | : | DP-2304-C0935 |
| --- | --- | --- |
| **Decision Date** | : | 20 December 2023 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | [Wong Huiwen Denise](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/result-page?p_p_id=legalresearchresultpage_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchresultpage_WAR_lawnet3legalresearchportlet_action=browseByCoramAuthorMP&typeOfBrowse=browseByCoram&filtering=Wong%20Huiwen%20Denise&searchFacetName=Coram) |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Whiz Communications Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised access to and disclosure of personal data* – *Insufficient security arrangements* – *Failure to implement security requirements on vendors* – *Failure to implement reasonable access controls*

**Introduction**

1 Whiz Communications Pte. Ltd. (the “**Organisation**”) is a Singapore telecommunications service provider offering broadband internet access, local and long-distance digital IP telephony, prepaid and postpaid calling plans.

2 On 22 April 2023, the Personal Data Protection Commission (the “**Commission**”) was alerted by the Singapore Police Force of a personal data breach incident involving the Organisation (the “**Incident**”), which the Organisation confirmed on 24 April 2023.

3 The Organisation requested, and the Commission agreed, for this matter to proceed under the Expedited Decision Breach Procedure. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision and to a breach of the Protection Obligation under Section 24 of the PDPA. Section 24 of the Personal Data Protection Act 2012 (“**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 Incident**

4 The Organisation’s customer management system (“**CMS**”) was designed and developed in 2016 by an external vendor. This external vendor did not process personal data on behalf of the Organisation and was not the Organisation’s data intermediary. The Protection Obligation in respect of customer personal data processed by the CMS therefore fell solely on the Organisation.

5 The CMS from its initial design accepted any Python script requests that could be exploited for unauthorised exfiltration of customer personal data. This failure to block or manage scripts posed a data security risk and was a design flaw.

6 Post-Incident, the Organisation established through tracing web services and databased logs that Python scripts had indeed been used by the threat actor (“**TA**”) to extract .jpg files from the CMS. 29,903 attempts from 8 overseas IP addresses were made over 5 days in March and April 2023, with 24,323 successful extractions of the personal data of 24,323 individuals.

7 The types of personal data exfiltrated were the front and back images of identification documents (i.e., NRIC, passport, student pass and dependent pass) and other supporting documents such as tenancy agreements and letters of approval for work permits issued by the Ministry of Manpower, Singapore.

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

(a) Rejected and denied all Python requests to the CMS;

(b) Restricted overseas IP addresses from connecting to the Organisation’s network;

(c) Implemented two-factor authentication and enhanced the password complexity requirement for the CMS’ admin users via web access; and

(d) Conducted a penetration test on the CMS.

**Findings and Basis for Determination**

9 As a Singapore telecommunications service provider, the Organisation had higher-level security needs. This extended to the Organisation’s CMS that contained the personal data of individuals who subscribed to the telecommunications services provided by the Organisation.

10 First, the Organisation admitted it has breached the Protection Obligation under the PDPA as it failed to provide any security requirements to the CMS IT vendor, in particular, requirements that would have adequately addressed the data security risks posed by Python scripts.

11 The Organisation admitted that it failed to stipulate clear job specifications and security requirements to the IT vendor who developed the CMS. There was also no contractual obligation on the IT vendor to ensure that personal data would be protected. In SAP Asia Pte Ltd [2021] SGPDPC 6, the Commission had reiterated the need for organisations to provide clear job specifications and include data protection requirements when engaging IT vendors. Thereafter, organisations are also expected to ensure that the IT vendor has satisfied the job specifications and data protection requirements stipulated.

12 Secondly, the Organisation admitted that it was in breach of the Protection Obligation under the PDPA as it neither had a sufficiently complex password policy nor enforced one. In the Commission’s Guide to Data Protection Practices for ICT Systems[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/113312.xml&queryStr=(personal%20data%20protection%20act)#fn1), the Commission recommended a minimum of 12 alphanumeric characters with a mix of uppercase, lowercase, numeric and special characters. We also recommended using phrases or paraphrase, combined with numbers and uppercase, lowercase and special characters, as these characteristics will make a password stronger and harder to decode.

13 Prior to the Incident, the Organisation’s CMS admin user password complexity required only 9 alphanumeric characters with at least one uppercase, which clearly fell short of PDPC’s recommended password complexity. We urge organisations to meet PDPC’s recommended best practices relating to passwords, especially for privileged access accounts such as admin accounts.

14 Third, the Organisation also admitted to a breach of the Protection Obligation of the PDPA as it failed to ensure reasonable access control to its CMS. Given the nature of personal data the Organisation was in possession and control of, the Organisation should have enhanced the access control to its CMS beyond the baseline of password protection. This could have taken the form of implementing multi-factor authentication for its CMS admin accounts, restricting access from overseas IP addresses to its CMS, and, last but not least, having an up-to-date web application firewall to defend against typical web application attacks.

15 For the above reasons, the Organisation was determined to have breached the Protection Obligation.

**The Deputy Commissioner’s Decision**

16 In determining whether the Organisation should be required to pay a financial penalty under Section 48J of the PDPA or if directions would suffice, I considered that a financial penalty was appropriate given the Organisation involved and the nature of the personal data affected in the Incident.

17 In deciding the appropriate financial penalty amount, I first considered all the relevant factors listed at Section 48J(6) of the PDPA, in particular, the impact of the personal data breach on the individuals affected and the nature of Organisation’s non-compliance with the PDPA.

18 In deciding what would be the appropriate financial penalty amount, I also considered the Organisation’s turnover to arrive at a figure that would, in my mind, be a proportionate and effective amount, to ensure compliance and to deter non-compliance with the PDPA.

19 Finally, I considered the following mitigating factors, which led to a further reduction in the financial penalty:

(a) The Organisation was cooperative during the course of our investigations;

(b) The Organisation voluntarily admitted to breach of the Protection Obligation under the Commission’s Expedited Decision Procedure; and

(c) The Organisation took prompt remedial actions following discovery of the Incident.

20 For the reasons above, I hereby require the Organisation to pay a financial penalty of $9,000 within 30 days of the date of the relevant notices 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following are the provision of the Personal Data Protection Act 2012 cited in the above summary:

**Protection of personal data**

**24.** An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks and;

(b) the loss of any storage medium or device on which personal data is stored.

[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/113312.xml&queryStr=(personal%20data%20protection%20act)#fnref1) PDPC’s Guide to Data Protection Practices for ICT Systems, page 15. Accessible at https://www.pdpc.gov.sg/help-and-resources/2021/08/data-protection-practices-for-ict-systems.

## Breach of the Protection Obligation by Cortina Watch

## [2024] SGPDPCS 3

| **Case Number** | : | DP-2306-C1102 |
| --- | --- | --- |
| **Decision Date** | : | 28 March 2024 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Cortina Watch Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements* – *Inadequate password policy* – *Failure to implement reasonable access controls for privileged account*

1. Cortina Watch Pte. Ltd. (the “**Organisation**”) is mainly involved in the retail, import, and export of timepieces, branded pens, and luxury accessories. On 5 June 2023, the Personal Data Protection Commission (the “**Commission**”) received a Data Breach Notification (“**DBN**”) filed by the Organisation, regarding a ransomware attack on its server (the “**Incident**”).

2. The Organisation subsequently confirmed that the personal data of 3,953 individuals had been accessed and exfiltrated in the Incident. The breakdown of the different types of personal data affected for the individuals was as follows:

| Types of Personal Data Affected | No. of Affected Individuals |
| --- | --- |
| Full Name + Contact Number | 1,380 |
| Full Name + Address + Any Other Details | 930 |
| Full Name + Email | 688 |
| Full Name + Date of Birth + Any Other Details | 645 |
| Full Name + NRIC/Passport Number + Any Other Details | 234 |
| Full Name + Email + Any Other Details | 68 |
| Full Name + Bank Account Number + Any Other Details | 8 |

3. The Commission acceded to the Organisation’s request for the matter to be handled under the Commission’s Expedited Breach Decision Procedure (“**EDP**”). This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out below and admitted that it was in breach of section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”).

4. Based on the Commission’s own investigations and the efforts of an IT forensic investigation firm engaged by the Organisation, it was determined that the Organisation had experienced multiple brute force attacks between 30 April to 4 June 2023. On 27 May 2023, a Virtual Private Network (“**VPN**”) account which the Organisation had been using to test VPN access to live environments was compromised. The threat actor successfully accessed a password-protected master password file, and thereafter moved laterally across the servers. The threat actor exfiltrated 5.82 GB of data and deployed the “Lockbit 3.0” ransomware to encrypt other files on the Organisation’s servers. The personal data of the affected individuals was subsequently posted on the dark web.

5. The Organisation took the following remedial actions:

a. All the servers were taken offline between 4 to 9 June 2023;

b. An Endpoint Detection Response tool was deployed on all the servers and endpoints for security visibility;

c. Implemented a centralised log management to forward the firewall logs to a centralised server;

d. Introduced certificate-based authentication for VPN users, in addition to Two-Factor Authentication (“2FA”);

e. Implemented firewall VPN access with 2FA control;

f. Decommissioned all servers running on legacy Windows Server 2008 R2 and recreated new domains with Windows 2019 servers;

g. New network environments were created and hardened with a mandatory password complexity requirement and account lockout after 3 tries;

h. As the Organisation’s data was not secured with encryption, the Organisation implemented a new folder/file encryption solution; and

i. Proper backup was put in place with Managed Service Provider services from an IT Vendor.

6. The Organisation admitted to breaching section 24 of the PDPA by failing to have reasonable security arrangements in place to protect the personal data in its possession/control. The Organisation admitted that there was a lack of “house-keeping” on its “test” VPN user accounts and that it failed to implement reasonable access controls to its network through its “test” VPN user accounts.

7. Compliance with the Protection Obligation required the Organisation to conduct a security assessment of what would have amounted to reasonable access control to its network. After such an assessment, the Organisation could have considered adopting the following security arrangements which would have enhanced access control to its network:

a. Enforcing rules against the use of easy-to-guess usernames. Apart from the “test” VPN user account, the Organisation’s investigations revealed that there were several other default account names such as “Administrator” and “Guest” being used on its systems. The use of default account names makes it easier for a threat actor to target and mount an attack against these accounts.

b. Implementing multi-factor authentication (“MFA”) for all VPN accounts, firewall access and access to files holding passwords. The Organisation admitted it could have but had neglected to do so.

8. In its decision in *Lovebonito Singapore Pte. Ltd.* [2022] SGPDPC 3 published on 19 May 2022 (i.e. before the Incident), the Commission made clear that MFA was to be implemented as ***a baseline requirement*** for privileged accounts with remote access to confidential or sensitive personal data or large volumes of personal data:

“*Henceforth, the Commission adopts the following tiered approach:*

*a.* *First, 2FA / MFA should be implemented as a* ***baseline requirement for administrative accounts to systems that hold personal data of a confidential or sensitive nature, or large volumes of personal data****: see [46]-[47] above. Failure to do so can ipso facto amount to a breach, unless the organisation can show that its omission is reasonable or implementation of 2FA is disproportionate.*

*b.* *Second,* ***remote access by privileged accounts to information systems that host confidential or sensitive personal data, or large volumes of personal data, should a fortiori be secured by 2FA / MFA****. The risks concerning remote access are higher, thus the expectation to implement 2FA / MFA will correspondingly increase.*

*c.* *Third,* ***organisations using IT systems to host confidential or sensitive personal data, or large volumes of personal data, are expected to enable and configure 2FA / MFA****,* ***if this is a feature that is available out-of-the-box****. Omission to do so may be considered an aggravating factor*.”[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/113712.xml&queryStr=(personal%20data%20protection%20act)#fn1) (emphasis added in bold)

9. The Organisation admitted that it failed to enforce a strong password policy (by requiring a combination of alphanumeric characters in addition to its existing password policy of a minimum password length of 8 characters). The Commission finds the Organisation in breach of section 24 of the PDPA for failing to enforce a robust password policy. In the *Lovebonito* decision*,* the Commission had stated at [18] and [19] as follows:

*“A robust password policy is a key security measure that an organisation must have in place to ensure that its IT systems are not vulnerable to common hacking attempts such as brute force attacks. As noted in Re (1) The Cellar Door Pte Ltd; (2) Global Interactive Works Pte. Ltd. [2016] SGPDPC 22 (at [30(d)]):*

*“… The need to have a strong password is fundamental to the security of the database system. Weak passwords increase the chances of an intruder cracking the password and gaining full access to the database system, and, more importantly, the personal data stored therein.”*

10. In our Guide to Data Protection Practices for ICT Systems (the **“Guide”**), the Commission has encouraged organisations to implement as a basic practice, a minimum level of password complexity (12 alphanumeric characters with a mix of uppercase, lowercase, numeric and special characters) particularly where password changes are only enforced after periods of 6 months or more. In addition, we have also encouraged organisations to impose, as an enhanced practice, a limit on the number of failed logins to minimise brute force attacks.

11. The Commission’s starting point in assessing the robustness of an organisation’s data protection practices, are the practices recommended in our Guide. That said, it is always open to an organisation to show that its omission to implement any of the Guide’s recommended practices is reasonable, and/or that alternative and equivalent measures have been implemented.

12. Ultimately, it is an organisation’s responsibility to put reasonable security arrangements in place to protect the personal data in its possession or control, the design and implementation of which should reflect the volume and sensitivity of the data handled, the nature of business and the types of services offered. The Commission reiterates the importance of data protection by design and encourages organisations to design and implement the appropriate protection measures so as to maintain good governance over its personal data and mitigate data breach risks.

13. Having considered the impact of the Incident, the Organisation’s prompt remedial actions, and its cooperation during the course of the investigation, the Commission considered it appropriate, in lieu of imposing a financial penalty, to direct the Organisation to comply with the following:

(a) To engage a third-party cyber security vendor to conduct a targeted security audit to enhance access control to personal data in its possession within the network; and

(b) To complete the above Direction within 60 days and to submit a comprehensive report to PDPC within 7 days of its completion.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following section of the Personal Data Protection Act 2012 had been cited in the above summary:

**Protection of personal data**

**24(a).** An organisation shall 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.

[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/113712.xml&queryStr=(personal%20data%20protection%20act)#fnref1) See *Lovebonito Singapore Pte. Ltd.* [2022] SGPDPC 3 at [51].

## Breach of the Protection Obligation by Ezynetic Pte Ltd

## [2025] SGPDPCS 2

| **Case Number** | : | DP-2406-C2585 |
| --- | --- | --- |
| **Decision Date** | : | 03 March 2025 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | [Wong Huiwen Denise](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/result-page?p_p_id=legalresearchresultpage_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchresultpage_WAR_lawnet3legalresearchportlet_action=browseByCoramAuthorMP&typeOfBrowse=browseByCoram&filtering=Wong%20Huiwen%20Denise&searchFacetName=Coram) |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Ezynetic Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Disclosure of personal data* – *Lack of access controls* – *Failure to conduct reasonable periodic security review*

1 Ezynetic Pte. Ltd. (the “**Organisation**”) is a Singapore-incorporated Software- as-a-Service (“**SaaS**”) provider that provides information technology solutions and services to licensed moneylenders in Singapore.

2 On 26 June 2024, the Personal Data Protection Commission (the “**Commission**”) was informed about a data breach incident involving the Organisation’s servers being infected by ransomware on or about 24 June 2024. Consequently, 190,589 individuals’ personal data was exfiltrated and posted for sale on the dark web (the “**Incident**”).

3 The Organisation requested, and the Commission agreed, for the investigation to proceed under the Expedited Decision Procedure (“**EDP**”). This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. It also admitted to a breach of the Protection Obligation under Section 24 of the Personal Data Protection Act 2012 (“**PDPA**”).

**Facts of the Case**

4 The Organisation operates an information technology system which was linked to the Moneylenders Credit Bureau (“**MLCB**”) platform operated by Credit Bureau (Singapore) Pte Ltd[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/115802.xml&queryStr=(personal%20data%20protection%20act)#fn1) via Application Protocol Interfaces (“**APIs**”) (the “**moneylending system**”).

5 The Organisation’s clients would input personal data of their prospective loan applicants and borrowers into the moneylending system which would allow them to verify the applicants’ and borrowers’ loan eligibility, generate the MLCB credit reports, track the loans, instalments, collections, payments and generation of profit and loss reports.

6 On 24 June 2024, the Organisation discovered that it could not access the moneylending system, and the relevant databases had been deleted by a threat actor who managed to gain access to its database server.

7 Investigations found that the threat actor had exploited a vulnerable web service application to gain access and control of its system administrator (“**SA**”) account[[note: 2]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/115802.xml&queryStr=(personal%20data%20protection%20act)#fn2) to access the moneylending system. After gaining access to the moneylending system, the threat actor exfiltrated the personal data of the affected individuals.

8 The personal data exfiltrated included a combination of the name, address, email address, telephone number, NRIC number, date of birth and the financial information available in the MLCB Credit Reports of 190,589 individuals.

9 The MLCB platform was not compromised as the Incident only involved unauthorised access into the Organisation’s internal systems by the threat actor.

10 Investigations revealed the following lapses by the Organisation that had contributed to the Incident:

a. The Organisation failed to disable or adequately secure the SA account which is a well-known SQL server account, and is often targeted by malicious users. The access controls mechanism implemented for the SA account was inadequate. The password, at the time of the Incident, which was p@ssword1 or Password@1, was susceptible to brute force attacks; and

b. The Organisation did not perform any periodic vulnerability assessment or penetration testing of its infrastructure.

*Remedial Action*

11 Following the Incident, the Organisation promptly took the following remedial actions:

a. Rebuilt its entire network and migrated to a cloud environment for its servers;

b. Enhanced security measures were implemented for the new network after consultations with the Cybersecurity Agency of Singapore (“**CSA**”) and the Ministry of Law Singapore; and

c. Notified all affected clients on 1 July 2024.

**Findings and Basis for Determination**

*Whether the Organisation had contravened the Protection Obligation*

12 Under section 24(a) of the PDPA, organisations must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks.

13 Taking into account the Organisation’s admission, and 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:

a. Failure to have reasonable access control. The volume and types of personal data in the possession and under the control of the Organisation required it to have adopted enhanced access controls. Given that the SA account granted privileged access to the Organisation’s moneylending system, adequate authorisation and authentication processes were required. This includes the implementation and enforcement of a strong password policy that includes a minimum level of password complexity, and a fixed period of password validity or regular change of passwords, the weak password used for the moneylending system during the Incident was an inadequate security arrangement to safeguard the personal data contained in the moneylending system.

b. Failure to conduct reasonable periodic security review. At the time of the incident, no network vulnerability assessments or penetration testing had been conducted. As stated in page 5 of the Commission’s Checklists to Guard Against Common Types of Data Breaches (the “**Checklists**”)[[note: 3]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/115802.xml&queryStr=(personal%20data%20protection%20act)#fn3), organisations should, as a basic practice, periodically conduct web application vulnerability scanning and assessments post deployment. The Organisation’s failure to conduct reasonable periodic security review amounted to a breach of section 24 of the PDPA.

14 For the above reasons, the Organisation was determined to have breached the Protection Obligation.

**The Deputy Commissioner’s Preliminary Decision**

*Financial Penalty*

15 In determining whether to impose a financial penalty on the Organisation under Section 48J of the PDPA, the Commission considered that a financial penalty was appropriate given the role of the Organisation as a SaaS provider that processes personal data entrusted to it by its client. As a SaaS provider, the Commission the Organisation should possess the necessary technical expertise to implement reasonable cybersecurity measures to address the evolving threats.

16 In deciding the appropriate financial penalty amount, the Commission first considered the impact of the personal data breach on the individuals affected and the nature of Organisation’s non-compliance with the PDPA. In addition, in order to ensure that the financial penalty imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with the PDPA, the Commission also considered the Organisation’s annual turnover.

17 The Commission also considered the following factors:

a. The Organisation was cooperative during the course of our investigations;

b. The Organisation voluntarily admitted to breach of the Protection Obligation under the EDP; and

c. This is the Organisation’s first instance of non-compliance with the PDPA.

18 Based on the foregoing, the Deputy Commissioner made a preliminary decision to impose a financial penalty of $17,500 on the Organisation for its breach of the Protection Obligation.

19 In addition, to ensure the Organisation’s compliance with the Protection Obligation, the Deputy Commissioner also directed the Organisation, under section 48I of the PDPA, to obtain CSA’s Cyber Trustmark Certification for its new IT network and report to the Commission on its completion.

**Representations Made by the Organisation**

20 The Organisation was notified of the preliminary decision by way of the Commission’s letter dated 2 December 2024 and was invited to make representations. On 3 December 2024, the Organisation made the following representations to the Commission seeking a waiver or reduction in the financial penalty:

a. The Organisation had expended significant financial commitment to investigate, mitigate the effects of the breach and fortifying its systems against future cybersecurity threats;

b. It had suffered significant operational disruptions and continued financial losses as a result of the Incident; and

c. It had maintained full transparency and cooperation with all regulatory bodies throughout the investigation.

21 After careful consideration, the Organisation’s representations were not accepted for the reasons outlined below:

a. The fact that the Organisation has expended significant financial commitment to implement remedial measures post-data breach does not warrant a further reduction, as it is a necessary part of its obligation to implement reasonable security arrangements under the Protection Obligation.

b. The operational disruptions and financial losses suffered by the Organisation were part of the vicissitudes of dealing with the aftermath of a serious data breach incident and its previous non-compliance with the Protection Obligation. Whilst the Organisation did provide some invoices showing that it had incurred expenses to implement remedial measures, these did not show that the Organisation is in such a dire financial situation that the imposition of a financial penalty of $17,500 would adversely impact its ability to continue its business; and

c. The Commission had already taken into account of the cooperativeness of the Organisation, in arriving at the preliminary decision.

**The Deputy Commissioner’s Decision**

22 Having considered all the relevant circumstances of this case, the Deputy Commissioner hereby requires the Organisation to pay a financial penalty of $17,500 within 30 days from the date of the relevant notice accompanying this decision, failing which interest at the rate specified in the Rules of Courts 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.

23 For completeness, the Organisation is also directed to:

a. Obtain CSA’s Cyber Trustmark Certification for its new IT network within 9 months from the date of this Decision; and

b. To report to the Commission within 14 days upon completion of the above action outlined above.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following section(s) of the Personal Data Protection Act 2012 had been cited in the above Summary of The Decision:

**Protection of personal data**

**24.** An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.

[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/115802.xml&queryStr=(personal%20data%20protection%20act)#fnref1) Credit Bureau (Singapore) Pte Ltd is the designated credit bureau by Ministry of Law Singapore to operate the MLCB platform.

[[note: 2]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/115802.xml&queryStr=(personal%20data%20protection%20act)#fnref2) The SA account login, short for *system administrator,* is one of the riskiest server-level principals in SQL Server. It’s automatically added as a member of the sysadmin fixed server role and, as such, has all permissions on that instance and can perform any activity.

[[note: 3]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/115802.xml&queryStr=(personal%20data%20protection%20act)#fnref3) https://www.pdpc.gov.sg/help-and-resources/2021/08/data-protection-practices-for-ict-systems

## Breach of the Protection Obligation HMI Institute of Health Science

## [2024] SGPDPCS 5

| **Case Number** | : | DP-2405-C2321 |
| --- | --- | --- |
| **Decision Date** | : | 08 October 2024 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | [Wong Huiwen Denise](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/result-page?p_p_id=legalresearchresultpage_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchresultpage_WAR_lawnet3legalresearchportlet_action=browseByCoramAuthorMP&typeOfBrowse=browseByCoram&filtering=Wong%20Huiwen%20Denise&searchFacetName=Coram) |
| **Counsel Name(s)** | : | — |
| **Parties** | : | HMI Institute of Health Science |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient administrative security arrangements* – *Failure to exercise reasonable oversight over vendor*

1 HMI Institute of Health Science Pte. Ltd. (the “**Organisation**”) is a healthcare training provider in Singapore. On 2 May 2024, the Organisation notified the Personal Data Protection Commission (the “**Commission**”) of a personal data breach incident after it received a complaint from an affected individual who found an Excel file containing the personal data of 761 individuals which the Organisation had inadvertently made publicly available on the Internet (the “**Incident**”).

2 The personal data disclosed included a combination of the name, address, email address, telephone number, NRIC number, date of birth, nationality, race, gender and educational qualification.

3 The Organisation requested, and the Commission agreed, for the investigation to proceed under the Expedited Decision Procedure. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision. It also admitted to a breach of the Protection Obligation under Section 24 of the Personal Data Protection Act 2012 (“**PDPA**”).

**Facts of the Case**

4 Investigations revealed that the affected individuals had provided their personal data to the Organisation via the Students’ Career Portal (the “**Portal**”), which was previously part of the Organisation’s website from 2017 to 2019. In December 2019, the Organisation decided to decommission the Portal. Investigations revealed that the Organisation did not follow up with the vendor to ensure that the Portal had been properly decommissioned, other than checking and confirming that the Portal was no longer accessible at its original URL address.

5 The Excel file continued to reside in the web directory of the Organisation’s website with no access control to prevent indexing by online search engines. This led to the Excel file being indexed and made publicly accessible via an online search using relevant keywords.

*Remedial Action*

6 Following the Incident, the Organisation promptly took the following remedial actions:

(a) Removed the Excel file in its web directory;

(b) Liaised with internet search engines to ensure that all web links to the Excel file had been removed;

(c) Implemented an internal checklist for all future commissioning, onboarding and decommissioning of IT solutions; and

(d) Established additional protocols to monitor its website content.

**Findings and Basis for Determination**

*Whether the Organisation had contravened the Protection Obligation*

7 Under section 24(a) of the PDPA, organisations must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks.

8 The Organisation admitted to a breach of section 24 of the PDPA as it did not have adequate policies and processes to exercise reasonable oversight over the vendor tasked with decommissioning the Portal. While the Organisation alluded to its own lack of technical expertise and reliance on the vendor to decommission the Portal, the Organisation’s lack of technical expertise is not an adequate defence to the Organisation’s failure to take the necessary steps in order to comply with its obligation under section 24 of the PDPA.

9 The Commission noted that in this case, the exercise of reasonable vendor oversight did not require technical expertise. The Organisation could have exercised reasonable oversight by verifying with its vendor that the personal data previously collected by the Organisation via the Portal had been properly deleted and was no longer accessible following the decommissioning of the Portal. However, the Organisation did not have the policies and processes in place to allow it to adequately supervise the work carried out by its vendor.

10 For the above reasons, the Organisation was determined to have breached the Protection Obligation.

**The Deputy Commissioner’s Decision**

*Financial Penalty*

11 In determining whether the Organisation should be required to pay a financial penalty under Section 48J of the PDPA, the Commission considered all relevant factors listed at Section 48J(6) of the PDPA, in particular, the impact of the personal data breach on the individuals affected, the duration of and the nature of the Organisation’s non-compliance with the PDPA.

12 The Commission also considered the fact this is the second contravention of the PDPA by the Organisation.

13 The Commission considered the following mitigating factors:

(a) The Organisation was cooperative during the course of our investigations; and

(b) The Organisation voluntarily admitted to breach of the Protection Obligation under the Commission’s Expedited Decision Procedure.

14 For the reasons above, the Commission hereby requires the Organisation to pay a financial penalty of $10,000 within 30 days from the date of the relevant notices 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.

*Directions*

15 In addition, to ensure the Organisation’s compliance with the Protection Obligation, the Organisation is directed to report to the Commission on the completion of the following remedial actions:

(a) Create and maintain a personal data asset inventory for tracking of its personal data assets;

(b) Put in place a well-documented vendor management policy and relevant processes for effective management and supervision of its IT vendors;

(c) Conduct a vulnerability assessment and/or penetration testing of its existing IT systems and to resolve any identified vulnerabilities; and

(d) Prepare and submit to the Commission a written report of the completion of the remediation actions directed above within 60 days from the date of the relevant notices accompanying this decision.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following section(s) of the Personal Data Protection Act 2012 had been cited in the above summary:

**Protection of personal data**

**24.** An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.

## Fortytwo Pte. Ltd.

## [2023] SGPDPCS 3

| **Case Number** | : | DP-2112-B9354 |
| --- | --- | --- |
| **Decision Date** | : | 07 March 2023 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Fortytwo Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Sensitivity of personal data* – *Unauthorised access to personal data* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements* – *Failure to patch third-party software*

*Data Protection* – *Protection obligation* –  *Incomplete, fictitious or pseudonymised data*

1. On 24 December 2021, Fortytwo Pte. Ltd. (the **“Organisation”**), an online furniture store, notified the Personal Data Protection Commission (the **“Commission”**) of malicious code injections on its website which led to the capturing of the email address and password of 6,241 individuals when they logged in to its website (the **“Incident”**). The name, credit card number, expiry date and CVV/CVN number of another 98 individuals’ were also affected.

2. The Organisation requested for the matter to be handled under the Commission’s expedited breach decision procedure. This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision; and admitted that it was in breach of section 24 of the Personal Data Protection Act (the “**PDPA**”).

3. An issue that arose in this case is whether fictitious names or pseudonymous personal particulars form part of the personal data under the possession or control of the Organisation. The importance of this lies in how it may potentially reduce the size of the dataset that was at risk. In their addendum to the Written Statement, the Organisation stated that it does not verify the names provided by the users, and suggested that the impact of the Incident might be more limited as some of the users’ names may be incomplete, fictitious or pseudonymous.

4. Section 2(1) of the PDPA defines “personal data” to be data, *whether true or not* (emphasis added), about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. The PDPA caters for the situation where not every record of personal data that is under the possession or control of an Organisation is verified. It takes a practical approach, as the accuracy of personal data records will change with the passage of time (e.g. information becomes outdated) or individuals may intentionally provide inaccurate information (e.g. users hiding their age or using fictitious residential addresses to bypass restriction of services by age or geolocation). What matters is that the Organisation, having collected the information, takes steps to comply with their obligations under the PDPA, such as to protect them and to ensure that they are used in accordance with the purpose of their collection.

5. The situation is different when the organisation, as a data security or data management measure, applies pseudonymisation or anonymisation techniques on personal data that is in their possession or under their control. In such circumstances, if the risk of reidentification is adequately addressed and managed, the resulting dataset may be treated as anonymised. The key difference is the intention of the organisation and its ability to direct and control the data processing activities required to achieve the resultant anonymised dataset.[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/111512.xml&queryStr=(personal%20data%20protection%20act)#fn1)

6. In this case, the Organisation was collecting data from its customers. Their customer database contained names, email addresses and additional details such as their shipping address, billing address, and date of birth. It also contained credit card details of 98 customers. Even if some customers had provided incomplete, fictitious or pseudonymous personal particulars or payment details, the Organisation had collected personal data. For the purpose of this investigations, it matters not that some of these customers may have provided inaccurate information. The Organisation’s obligations under the PDPA applies to the entire customer database.

7. The Organisation admitted that the Incident occurred because the threat actor had successfully exploited vulnerabilities present in the Magento open-source version 1.9.x.x which the Organisation had employed for its online store. These vulnerabilities were present because the Organisation failed to apply four Magento security patches released on 28 Nov 2017, 25 June 2019, 8 October 2019 and 28 April 2020 by Adobe.

8. Compounding the above, support for Magento version 1 had ended on 30 June 2020. The Organisation admitted that it should have upgraded to Magento open-source version 2.0 after Adobe ended the support for Magento 1 on 30 June 2020. The Organisation had planned to upgrade to Magento version 2 in early 2020, but its plans were disrupted by the COVID-19 pandemic. Having said that, Adobe had announced in November 2015 that it will end support for Magento 1.x in 36 months, i.e. by November 2018. In September 2018, Adobe then announced that it would extend the support to 30 June 2020. Given the ample notice given by Adobe to the Organisation of the need to upgrade the version of Magento Open Source which it was using in order to continue receiving support and security patches from Adobe, it is difficult to look past the Organisation’s prolonged failure to do the needful and perform the necessary upgrades.

9. The Commission had consistently advised organisations on the importance of applying software patches. In our Guide to Data Protection Practices for ICT Systems, the Commission had highlighted that organisations should perform system patching promptly to fix security vulnerabilities. If software patches are not updated as recommended by the software provider, they may not contain the latest cybersecurity updates and may compromise the organisation’s defence against cyber-attacks.

10. We note that the Organisation had considered and evaluated the four patches but decided to hold back on installing them. However, these four patches were released by Adobe to address several high severity risk issues and critical bugs, including the injection of malicious codes. The Organisation’s failure to patch had increased the risks of a malicious code injection capable of capturing users’ personal data.

11. In light of the above, the Organisation is found to have breached the Protection Obligation under section 24(a) of the PDPA.

12. The Commission notes that after the Incident, the Organisation took prompt remedial actions, including notifying affected individuals and various technical measures to improve its security. The Organisation is also taking steps to upgrade to Magento version 2.

13. In deciding the appropriate outcome in this case, the Commission considered the Organisation’s cooperation throughout the investigation, the voluntary admission of breach of the Protection Obligation, and the prompt remedial actions taken.

14. Following the issuance of the Commission’s preliminary decision, the Organisation represented that it was unfair to state that was a prolonged failure to perform the necessary upgrade. This is because there was a lead time of 6 months before the end of support when it made the decision to upgrade, before the COVID-19 pandemic disrupted its plans. The Organisation’s representation is not accepted as, notwithstanding the disruptions caused by the pandemic, the Organisation had been given ample notice of the impending end of support but took no action to perform the necessary upgrade from November 2015 to early 2020.

15. Having considered the circumstances set out above, the factors listed at section 48J(6) of the PDPA and the representations made by the Organisation, the Deputy Commissioner for Personal Data Protection hereby finds the Organisation in breach and directs the Organisation to pay a financial penalty of S$8,000 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.

16. The Organisation is also directed to:

a. Complete the upgrading of its website to a supported software version, including vulnerability assessment and penetration testing, within 6 months of the direction.

b. Inform the Commission with 14 days of the completion of the above.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following is the provision of the Personal Data Protection Act 2012 cited in the above summary:

**Protection of personal data**

**24.** An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.

[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/111512.xml&queryStr=(personal%20data%20protection%20act)#fnref1) See Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*, at paras 3.5, 3.8 and 3.13.

## Henry Park Primary School Parents’ Association

## [2020] SGPDPCS 3

| **Case Number** | : | Case No. DP-1903-B3531 |
| --- | --- | --- |
| **Decision Date** | : | 05 February 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Henry Park Primary School Parents’ Association |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements*

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

*Data Protection* – *Accountability obligation* – *Failure to appoint data protection officer*

1. Henry Park Primary School Parents’ Association (the “**Organisation**”) is a registered society whose membership comprised parent volunteers. To register as members of the Organisation, individuals provided to the Organisation their names, contact numbers, name of child and the child’s class in Henry Park Primary School (the “**Personal Data Set**”). The Organisation had a website at https://hppa.org.sg (the “**Website**”) where members could view their own account particulars upon logging in using their assigned user ID and password.

2. On 15 March 2019, the Personal Data Protection Commission (**“the Commission**”) received a complaint. The complainant informed that when she performed a Google search using her name, she found a search result of a webpage of the Website which disclosed her personal data (**the “Incident”**).

3. The Personal Data Sets of registered members were never intended to be disclosed online. The Website had been developed by a parent volunteer using the WordPress content management system.

4. The Organisation had conducted tests to verify that members who logged in to the Website could view their own account particulars. The Organisation also verified that account particulars could not be viewed when accessing the Website as a public user. Nevertheless, the Personal Data Set was crawled, indexed and searchable by Google. This points to a weakness in access control that had not been picked up by these rudimentary tests.

5. Security testing such as vulnerability scans would have identified the access control issue. The Organisation failed to conduct adequate security testing before launching the Website. On the above facts, the Commission found that the Organisation did not put in place reasonable security arrangements to protect the Personal Data Sets.

6. The Commission also found that the Organisation had not appointed a person to be responsible for ensuring its compliance with the Personal Data Protection Act 2012 (the “**PDPA**”). Further, the Organisation had not developed and implemented any policies and practices necessary for it to meet its obligations under the PDPA.

7. The Organisation had taken the Website offline after the Incident on 15 March 2019. On 14 November 2019, the Organisation had put online a new website that no longer allowed online access to the database of the Organisation’s members. The new website also included a data protection notice.

8. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of sections 11(3), 12 and 24 of the PDPA. In determining the directions, the Deputy Commissioner took into consideration that the Organisation was a volunteer organisation made up primarily of parents. The Organisation is directed to, within 60 days, (i) appoint one or more individuals to be responsible for ensuring that it complies with the PDPA, (ii) develop and implement internal data protection and training policies, and (iii) to put all volunteers handling personal data through data protection training.

## Barnacles Pte. Ltd.

## [2019] SGPDPCS 1

| **Case Number** | : | Case No. DP-1904-B3652 |
| --- | --- | --- |
| **Decision Date** | : | 26 September 2019 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Barnacles Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements*

*Data Protection* – *Retention limitation obligation* – *Purpose for which the personal data was collected is no longer served by retaining data* – *Retention is no longer necessary for legal or business purposes*

1. Barnacles Pte Ltd (the “**Organisation**”) operates a website which enables its customers to make reservations to dine at its restaurant. For this purpose, it collected certain personal data from its customers such as their name, contact number, email address and date and time of their reservation, amongst other information (the “**Personal Data**”). However, when the Organisation developed its website, the Organisation did not instruct the vendor it appointed to develop the website to implement security arrangements to protect the Personal Data. The Organisation also made no effort to verify whether any security arrangements had been put in place by its appointed vendor. As a result, the Personal Data was accessible over the Internet, for example, if a search was made on a customer’s name using an Internet search engine. The Organisation ceased operations in January 2019 but continued to retain the Personal Data until May 2019, even though it did not have any legal or business purpose to retain the Personal Data other than to fulfil or decline its customers’ reservations.

2. Following a complaint against the Organisation in April 2019, the Personal Data Protection Commission found that the Personal Data of 149 individuals had been exposed to the risk of unauthorised disclosure as a result of the Organisation’s failure to make security arrangements to protect the Personal Data and/or to cease to retain the Personal Data once it no longer had any legal or business purpose to retain it. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of sections 24 and 25 of the Personal Data Protection Act 2012 and decided to give a warning to the Organisation.

## Aman Group S.a.r.l and another

## [2022] SGPDPCS 7

| **Case Number** | : | DP-2012-B7506 |
| --- | --- | --- |
| **Decision Date** | : | 28 February 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Aman Group S.a.r.l; Amanresort International Pte Ltd |

*Data Protection* – *Protection obligation* – *No breach* – *No disclosure of personal data*

*Data Protection* – *Protection obligation* – *No breach* – *No possession or control of personal data*

1. On 5 December 2020, the Personal Data Protection Commission (the “**Commission**”) received a notification from SingCERT of a personal data breach involving Aman Group S.a.r.l (“**Aman Group**”) and Amanresort International Pte Ltd (“**Aman SG**”). 9 systems in London and 2 systems in Singapore were compromised and files containing personal data exfiltrated (the “**Incident**”).

2. As a result of the Incident, personal data of approximately 2,500 individuals which included their name, date of birth, address, email address, phone number and profession were affected.

3. The Aman Group engaged an external cybersecurity company, Ankura Consulting, to investigate the Incident. Its investigations found that the threat actor(s) had gained unauthorised access into 11 systems, which included 9 servers based in London and 2 servers based in Singapore.

4. While the investigations did not uncover any evidence of what the initial method and point of entry were, the most likely scenario is that the threat actor had initially entered via the London based systems. This is because the suspicious activities were first detected in the London systems. Thereafter, the threat actor subsequently gained access to the 2 Singapore based servers by creating administrator account credentials. There was no evidence that the firewalls in the Singapore based servers were breached.

5. Investigations could not conclusively exclude the possibility that data may have been exfiltrated from one of the Singapore based servers. However, analysis conducted by the Aman Group on four extracts obtained from the threat actor(s) failed to establish any conclusive links between the extracts and the current database in the affected Singapore based server.

6. Investigations further revealed that any exfiltrated data would have been encrypted and was in a proprietary format. Aman Group’s assessment was that the encryption and the proprietary format made it unlikely that the threat actor(s) would be able access and recreate the data in plaintext. Their assessment is that even if there had been exfiltration, there was no evidence that the exfiltrated data was in fact compromised. This is because the extracts obtained from the threat actor(s) do not resemble the current database in the affected Singapore based server.

7. Following the Incident, the Aman Group took prompt and extensive remedial actions to mitigate the effects of the Incident and enhance the robustness of its security measures.

8. Further, based on the facts as disclosed, Aman SG is a regional office. It did not hold the data protection role and was not in possession or control of the personal data in the 2 Singapore based servers. As such, Aman SG could not be held accountable for the Incident and cannot be said to be in breach of the Protection obligation under section 24 of the PDPA.

9. In view of the above, the Deputy Commissioner for Personal Data Protection is satisfied of the view that the Aman Group had met its Protection obligation under section 24 of the Personal Data Protection Act (“PDPA”) and that no enforcement action needs to be taken in relation to the Incident.

## MRI Diagnostics Pte Ltd and another

## [2020] SGPDPCS 14

| **Case Number** | : | Case No. DP-1811-B2975 |
| --- | --- | --- |
| **Decision Date** | : | 22 July 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | MRI Diagnostics Pte Ltd; Clarity Radiology Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Insufficient security arrangements*

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

*Data Protection* – *Accountability obligation* – *Failure to appoint data protection officer*

1. MRI Diagnostics Pte Ltd (“**NovenaMRI**”) operates a medical centre that provides magnetic resonance imaging and X-Ray services to patients. In the course of their business, NovenaMRI subscribed to an internet based teleradiology system (“**System**”) provided by Clarity Radiology Pte Ltd (“**Clarity**”). In-turn, Clarity engaged an overseas IT vendor (the “**IT Vendor**”) to maintain the System.

2. On 7 November 2018, a patient of NovenaMRI (“**Complainant**”) notified the Personal Data Protection Commission (the “**Commission**”) about an Excel Spreadsheet containing approximately 600 individual’s personal data (including the Complainant’s) that was accessible via the internet (the “**Incident**”).

3. During the course of investigations, the Commission found two additional Excel Spreadsheets containing similar information as the Excel Spreadsheet reported by the Complainant. A total of approximately 4,099 individuals were affected by the Incident (“**Affected Individuals**”). The Affected Individuals’ personal data that was exposed to unauthorised access included their names, NRIC numbers and the type of radiology scans performed (collectively, the “**Personal Data Sets**”).

4. The Commission’s investigations revealed that the Incident was caused by a lapse in the IT Vendor’s processes while carrying out maintenance work on the System. In particular, the IT Vendor had removed access restrictions to a network folder containing the Excel Spreadsheets for the purposes of patching the System, and omitted to reinstate the access restrictions after the patching was completed. Without access restrictions, the Excel Spreadsheets (containing the Personal Data Sets) were indexed by Google’s search engines and exposed to unauthorised access.

5. NovenaMRI was an organisation who had collected the Personal Data Sets from its patients, and had control of the Personal Data Sets at all material times.

6. Section 24 of the Personal Data Protection Act (“**PDPA**”) requires organisations like NovenaMRI 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 or similar risks (the “**Protection Obligation**”). In this regard, the Deputy Commissioner for Personal Data Protection (“**Deputy Commissioner**”) finds NovenaMRI in breach of the Protection Obligation because:

(a) When an organisation engages a vendor to supply, modify and/or maintain its IT system, it is required to provide the vendor with sufficient clarity and specifications on the requirements to protect personal data. This is because even if the vendor was not engaged to process personal data on the organisation’s behalf, it may nevertheless handle the personal data incidentally or make decisions that affect the security of the personal data in the course of providing its services. Depending on the circumstances of each case, the organisation should articulate its business requirements concerning the protection of personal data that the IT system will store. This will enable the vendor to assess and recommend the most appropriate and effective method to protect personal data. The organization will then be able to make a decision with access to the right information. Examples of measures include having clauses in written agreements setting out clearly the vendor’s obligations to protect personal data, providing operational guidance and verifying the data protection arrangements implemented by the vendor and/or exercising some form of supervision and oversight over the vendor’s activities;

(b) Given the nature of NovenaMRI’s business, which entailed being in possession and/or control of personal data of a sensitive nature (e.g. radiology scans and X-Rays), NovenaMRI should also have conducted a proper assessment of its vendor to satisfy itself that the vendor is well-placed to protect the personal data it hosts. For example, NovenaMRI could have obtained documentary evidence that the vendor had complied with industry standards with respect to information security (eg the ISO 27001 standard). However, in this case, there was no evidence that NovenaMRI had conducted proper due diligence of the security standards put in place by Clarity, prior to subscribing to the System that provided cloud-based services, including hosting the Personal Data Sets;

(c) Although NovenaMRI claimed that it had a written agreement with Clarity, it was unable to produce supporting evidence of this. NovenaMRI’s claim was also disputed by Clarity, who had admitted that there was no written agreement between the parties. In addition, even after NovenaMRI had engaged Clarity, NovenaMRI did not take any steps to verify if Clarity had implemented any data protection arrangements with respect to the System which hosted the Personal Data Sets.

7. As for Clarity, the contracted services from Clarity to NovenaMRI were to provide an archive for Dicom Images and a Web-based radiology information system with scheduling, registration, billing and client access modules. Essentially, Clarity was a “Software as a Service” provider (or what is commonly known as “SaaS-provider”) who had provided its cloud-based services to NovenaMRI. The provision of such technical solutions or deployment of software integrated into the clinical devices of NovenaMRI did not entail the processing of personal data. As such, Clarity was a vendor of NovenaMRI, and not a “data intermediary” of NovenaMRI. As a vendor, Clarity was not responsible for the protection of the Personal Data Sets under the PDPA in respect of the Incident.

8. However, during the course of investigations, Clarity admitted that it had failed to appoint a data protection officer and had not developed or put in place any data protection policies, as required under Sections 11(3) and 12 of the PDPA. Accordingly, Clarity is in breach of Sections 11(3) and 12 of the PDPA.

9. After considering the circumstances of the case, the Deputy Commissioner’s decisions are as follows:

(a) to issue a warning to NovenaMRI for its breach of the Protection Obligation. No further directions are necessary as NovenaMRI has ceased its business relationship with Clarity; and

(b) to direct that Clarity shall, within 30 days from the date of this decision:

i. Appoint a data protection officer;

ii. Develop and implement a data protection policy to comply with its obligations under the PDPA; and

iii. Inform the Commission within 7 days of the completion of each of the above directions.

## Nature Society (Singapore)

## [2021] SGPDPCS 15

| **Case Number** | : | DP-2011-B7351 |
| --- | --- | --- |
| **Decision Date** | : | 03 December 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Nature Society (Singapore) |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements*

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

*Data Protection* – *Accountability obligation* – *Failure to appoint data protection officer*

1. On 6 November 2020, the Personal Data Protection Commission (the “**Commission**”) received information of an online article reporting about hacked databases being made available for downloads on several hacking forums and Telegram channels. In the article, Nature Society (Singapore) (the "**Organisation**") was named as one of the affected Organisations (the “**Incident**”).

2. The personal data of 5,131 members and non-members who had created membership and user accounts on the Organisation’s website were affected in the Incident. The datasets affected comprised of names, usernames, passwords (encrypted), email addresses, telephone numbers, types of membership, gender, mailing addresses, dates of births, occupation, company and nationality.

3. Following the Incident, the Organisation engaged two IT professionals to carry out an investigation and analysis of the Organisation's website. The investigation and analysis revealed vulnerabilities in the Organisation's website and suspicious SQL injection activities prior to the Incident. The possible attack vector was identified as a SQL injection attack which led to personal data on the Organisation's website database being accessed and exfiltrated by unknown parties.

4. The Organisation took the following remedial measures after the Incident:

(a) Edited the website to stop all online membership sign-ups/renewals and logins to the website;

(b) Removed all members' and users' data from the website database;

(c) Backed up the website database and kept all personal data offline;

(d) Change all login passwords;

(e) Notified all affected individuals of the Incident via email;

(f) Appointed a Data Protection Officer ("**DPO**")

(g) Developed and implemented a personal data policy; and

(d) Engaging vendors to develop a new website to improve security.

5. In its representations to the Commission, the Organisation admitted to having breached the Accountability Obligation under sections 11(3) and 12(a) and the Protection Obligation under section 24 of the Personal Data Protection Act 2012 ("**PDPA**"), and requested for the matter to be dealt with in accordance with the Commission’s Expedited Decision Procedure.

*Breach of Section 11(3) of the PDPA*

6. First, the Organisation admitted it did not designate one or more individuals (typically referred to as a DPO) to be responsible for ensuring that the Organisation complies with the PDPA. The responsibilities of a DPO includes (a) ensuring compliance with the PDPA, (b) fostering a data protection culture, (c) handling and managing personal data queries and complaints, (d) alerting management to any risks with regard to personal data and (e) liaising with the Commission if necessary. From the foregoing, it is clear that the DPO plays a vital role in implementing and building a robust data protection framework to ensure an organisation’s compliance with its obligations under the PDPA.

*Breach of Section 12(a) of the PDPA*

7. Second, the Organisation admitted it did not develop and implement any personal data protection policy prior to the Incident. In this regard, it is important to reiterate that at the very basic level, an overarching personal data protection policy has to be developed and implemented to ensure a consistent minimum data protection standard across an organisation's practices, procedures and activities.

*Breach of Section 24 of the PDPA*

8. Third, the Organisation admitted that it did not make reasonable security arrangements to protect the personal data on its website database. After the Organisation's website was designed and developed by an external vendor in 2011, the Organisation did not have any contract/retainer agreement with the external vendor to maintain the website's security. As a result, the responsibility of protecting its website fell squarely on the Organisation. However, the Organisation failed to carry out any security measures e.g. conducting necessary security updates, patches and penetration tests, thus leaving its website vulnerable to attacks.

9. In the circumstances, the Organisation is found to have breached sections 11(3), 12(a) and 24 of the PDPA.

*Commission’s Decision*

10. After considering the factors listed at section 48J(6) of the PDPA and the circumstances of this case, including (i) the Organisation's upfront voluntary admission of liability which significantly reduced the time and resources required for investigations; (ii) the fact that the Organisation is a non-profit, registered society and (iii) the Organisation's prompt remedial actions, the Organisation is given notice to pay a financial penalty of $14,000.

11. The Organisation must make payment of the financial penalty 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.

12. In view of the remedial actions taken by the Organisation, the Commission will not issue any directions under section 48I of the PDPA.

## Autobahn Rent A Car Pte. Ltd.

## [2023] SGPDPCS 4

| **Case Number** | : | DP-2210-C0345 |
| --- | --- | --- |
| **Decision Date** | : | 09 June 2023 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Autobahn Rent A Car Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements* – *Failure to revoke unused administrator credentials*

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Lack of access controls* – *Failure to implement two-factor authentication / multi-factor authentication*

1. On 21 October 2022, Autobahn Rent A Car Pte. Ltd. (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) of a personal data breach (the “**Incident**”).

2. The Organisation operates a car-sharing service, Shariot, in Singapore. On 24 September 2022, the Organisation received customer feedback that a photograph on its mobile application had been replaced with a pornographic photograph. The Organisation discovered that the pornographic photograph had been uploaded through an unrevoked administrator account belonging to an ex-employee, who had left the Organisation in May 2022. The ex-employee received an email from an unknown sender on 10 September 2022 stating that his personal laptop had been hacked and demanding Bitcoins as ransom payment. The threat actor was able to log into the Shariot’s mobile application administrator portal through the administrator account belonging to the ex-employee, and used the export CSV function to download a copy of the Shariot’s users personal data.

3. Subsequently, on 21 October 2022, a cybersecurity solutions provider alerted the Organisation of a cybercrime forum post offering the sale of a Shariot database containing personal data. The Commission commenced investigations to determine whether the Incident disclosed any breaches of the Personal Data Protection Act 2012 (“**PDPA”**) by the Organisation.

4. The Organisation requested, and the Commission agreed, for this matter to proceed under the Expedited Decision Breach Procedure. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision. It admitted to a breach of the Protection Obligation under Section 24 of the PDPA.

5. The Organisation’s internal investigations discovered that compromise of the dormant administrator account credentials enabled the unauthorised access to Shariot backend admin web portal, leading to the exfiltration of 53,000 personal data sets of Shariot users. The personal data that were affected in the Incident included names, email addresses, mobile phone numbers, NRIC numbers and general location data (e.g. Bishan, Toa Payoh or Orchard).

6. Following the Incident, the Organisation took the following remedial action:

(a) Immediately conducted an internal audit of its administrator accounts to ensure that any employee access that was not required was revoked;

(b) Enhanced its software code and admin panel user interface to mask displayed or exported NRIC numbers to show only the last 4 characters; and

(c) Conducted cyber hygiene and awareness training for all staff handling personal data.

7. The Organisation admitted that it had failed to ensure it had reasonable security arrangements in place to prevent the unauthorized access or disclosure of the personal data in its possession or control, as it failed to implement and ensure reasonable access control to its backend admin web portal. First, the Organisation failed to revoke the login credentials of an administrator account belonging to an ex-employee once the employment relationship came to an end in May 2022. As a result, the ex-employee’s administrator login credentials remained active, which – when compromised – enabled the malicious actor access into its network.

8. Second, the Organisation also admitted that the Incident would not have happened if it had implemented multi-factor authentication (“**MFA**”) as an additional access control for its administrator accounts that had access to its sizeable user database. In *Re Lovebonito [2022] SGPDPC 3*, the Commission had highlighted the need for organisations to strengthen access control, through the use of a one-time password (“OTP”) or 2FA/MFA, to such accounts. Indeed, regardless of whether an account is an administrative account, once an account is granted access rights to a database containing sensitive personal data records or a significant volume of personal data that would adversely impact the affected individuals in the event of a personal data breach, we would encourage organisations to consider implementing enhanced access controls to the account such as through the use of a OTP or 2FA/MFA to better safeguard the personal data.

9. For the above reasons, the Organisation was determined to have breached the Protection Obligation.

**The Deputy Commissioner’s Decision**

10. In determining whether the Organisation should be required to pay a financial penalty under Section 48J of the PDPA or if directions would suffice, I considered that a financial penalty was appropriate as the personal data breach was not insignificant. In deciding the appropriate financial penalty amount, I first considered all the relevant factors listed at Section 48J(6) of the PDPA, in particular, the impact of the personal data breach on the individuals affected and the nature of Organisation’s non-compliance with the PDPA. In this regard, while the NRIC numbers and general location data was affected, this is less serious than if the NRIC images and specific GPS location had been disclosed.

11. In deciding what would be the appropriate financial penalty amount, I also considered the organisation’s turnover to arrive at a figure that would, in my mind, be a proportionate and effective amount, to ensure compliance and deter non-compliance with the PDPA. On the facts of this particular case, the organisation’s turnover has been taken into consideration to arrive at a proportionate and effective financial penalty. I also considered the following mitigating factors, which led to a further reduction in the financial penalty:

(a) The Organisation was cooperative during the course of our investigations;

(b) The Organisation voluntarily admitted to breach of the Protection Obligation under the Commission’s Expedited Decision Procedure; and

(c) The Organisation took prompt remedial actions following discovery of the Incident.

12. For the reasons above, I hereby require the Organisation to pay a financial penalty of $3,000 within 30 days of the date of the relevant notices 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.

13. In addition to the financial penalty imposed, the Organisation is also directed to do the following:

(a) Implement processes for systems and applications revocation within a reasonable window of cessation of need for access by an employee;

(b) Strengthen access controls measures to administrator accounts with access to databases holding personal data;

(c) Conduct reasonable security review of technical and administrative arrangements for the protection of personal data in possession or under control of the Organisation within 60 days of the date of this Direction;

(d) Rectify any security gaps identified in the security review directed above; and

(e) Inform the Commission within 1 week of the completion on the steps directed above.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following are the provision of the Personal Data Protection Act 2012 cited in the above summary:

**Protection of personal data**

**24.** An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks and;

(b) the loss of any storage medium or device on which personal data is stored.

## Larsen & Toubro Infotech Limited, Singapore Branch

## [2021] SGPDPCS 5

| **Case Number** | : | Case No. DP-2011-B7464 |
| --- | --- | --- |
| **Decision Date** | : | 06 May 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Larsen & Toubro Infotech Limited, Singapore Branch |

*Data Protection* – *Consent obligation* – *Disclosure of personal data without consent*

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements*

1. On 29 November 2020, the Personal Data Protection Commission (the “**Commission**”) received a complaint against Larsen & Toubro Infotech Limited, Singapore Branch (“**LTI**”) from an LTI job applicant.

2. On 25 November 2020, an LTI employee had emailed the complainant a set of sample forms which contained the personal data of a past job applicant. The LTI employee had sent the complainant those sample forms to assist him in filling up his own forms correctly.

3. Subsequently, on 3 December 2020, another LTI employee sent an email reminder to the complainant and 53 other job applicants to complete their application process. The email contained all of the job applicants’ respective names, with their email addresses placed in the “To” field and thus visible to all recipients.

4. Once notified of the complaint by the Commission, LTI undertook a review of its employees’ emails for the period from 2016 to 2020, and uncovered 73 other instances where past job applicants’ personal data had been disclosed to other job applicants.

5. In total, 13 past job applicants’ forms were disclosed by 10 of LTI’s employees to 74 other job applicants. The personal data disclosed in the forms comprised:

a. Name;

b. Signature;

c. Email address;

d. National Identification/ passport numbers;

e. Date of Birth;

f. Address;

g. Contact number;

h. Medical health status;

i. Employment history;

j. Salary information; and

k. Criminal records disclosure.

6. The Deputy Commissioner for Personal Data Protection finds that LTI negligently contravened the Protection Obligation under section 24 of the Personal Data Protection Act 2012 by failing to provide adequate instructions to its employees dealing with recruitment matters on how to handle personal data. LTI also negligently contravened the Consent Obligation under section 13 of the Personal Data Protection Act 2012, by disclosing the names and email addresses of all job applicants in its email sent to the 54 job applicants on 3 December 2020, including the complainant.

7. While LTI claimed to have a general Corporate Privacy Policy and an Employee Privacy Notice which applied to all employees, the purpose of these documents was to provide notice to individuals and employees on how LTI used, processed, and protected personal data. Guidance to employees on how they should handle personal data in the course of work could only be found in LTI’s “Data Privacy Awareness” training materials. LTI had no targeted policies or standard operating procedures specifically for the employees handling recruitment matters, despite the type and volume of personal data handled by such employees. The fact that as many as 10 of LTI’s employees had engaged in the same conduct over a 4 year period, reinforced the finding that the existing instructions were inadequate.

8. LTI indicated that it would make all its employees aware of this incident, and that it would implement a new set of procedures for email communications to external job applicants. LTI notified all affected job applicants of the wrongful disclosure of their personal data to other job applicants, and informed the job applicants to delete the emails they had received containing the affected job applicants’ forms. Refresher training was also conducted for the employees who had sent the emails.

9. After considering the circumstances of the case and the factors listed at section 48J(6) of the Personal Data Protection Act 2012, including LTI’s cooperation with investigations, its proactive review to identify additional historical breaches, and its prompt remedial actions, the Deputy Commissioner for Personal Data Protection requires that LTI pay a financial penalty of $7,000 for the breach.

10. LTI must make payment of the financial penalty within 30 days from the date of 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 the financial penalty until it is paid in full.

11. No further directions are required as LTI had taken actions to address the gaps in its security arrangements.

## Chapel of Christ the Redeemer

## [2021] SGPDPCS 1

| **Case Number** | : | Case No. DP-2010-B7132 |
| --- | --- | --- |
| **Decision Date** | : | 29 January 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Chapel of Christ the Redeemer |

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

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements*

1. On 6 October 2020, Chapel of Christ the Redeemer (the “**Organisation**”) informed the Personal Data Protection Commission (the “**Commission**”) that a file (the “**File**”) containing personal data of 815 members’ name, NRIC, address, date of birth, marital status, email address, mobile and residential phone number was inadvertently disclosed online.

2. Investigations revealed that a staff had accidentally uploaded the File (which was supposed to be an internal document) onto the sub-directory on 24 November 2019. The Organisation only discovered the matter on 8 September 2020 when a member of the Organisation performed a Google search of another member’s name and found a Google search result of the File.

3. The Organisation admitted that there were no access controls to the sub-directory prior to the incident as the sub-directory was intended to be accessible to public. As a result, the File was indexed by search engines and showed up in online search results. The Organisation also admitted that at the time of the incident, the Organisation had not developed any internal policies and practices to ensure compliance with the Personal Data Protection Act 2012 (the “**PDPA**”). In particular, there was no system of checks for the uploading of files on the Organisation’s website.

4. Fortuitously, it appeared that the access to the File was minimal – based on Google Analytics Report, save for the Organisation’s member who discovered the File on the internet on 8 September 2020, there was only one other access to the File on 9 December 2019, and the access only lasted for approximately 1 minute.

5. Following the incident, the Organisation disabled the search engine indexing to the sub-directory, password-protected all files with members’ data, and implemented a weekly check of all files uploaded onto the website to detect any accidental uploading of incorrect files; and a policy to delete files that are on the website for more than three months. The Organisation has also informed the Commission that it intends to engage a consultant to conduct PDPA training for its staff, as well as to review the data protection processes within the Organisation to ensure compliance with the PDPA.

6. In view of the facts stated at [3] above, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 12 of the PDPA (the obligation to develop and implement data protection policies and practices), and section 24 of the PDPA (the obligation to protect personal data in an organisation’s possession or under its control by making reasonable security arrangements).

7. In determining the directions to be imposed on the Organisation under section 29 of the PDPA, the following factors were taken into account:

(a) The Organisations had voluntarily notified the Commission of the incident, fully cooperated with the Commission’s investigations and implemented prompt remedial measures to address the breach; and

(b) There was minimal access to the File and no evidence that the personal data had been misused.

8. In the circumstances, the Deputy Commissioner would not be imposing any financial penalty on the Organisation. However, in light of the Organisation’s lack of the necessary data protection policies and practices, the Deputy Commissioner hereby directs the Organisation to:

(a) Develop and implement internal data protection policies and practices to comply with the provisions of the Act within 90 days from the date of the direction, and

(b) Inform the Commission within 1 week of implementation of the above.

## Global Outsource Solutions Pte. Ltd.

## [2019] SGPDPCS 7

| **Case Number** | : | Case No. DP-1809-B2767 |
| --- | --- | --- |
| **Decision Date** | : | 12 November 2019 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Global Outsource Solutions Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised access to and disclosure of personal data* – *Insufficient security arrangements*

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

1. Global Outsource Solutions Pte. Ltd. (the “**Organisation**”) provided warranties for products purchased by its clients’ customers. To be eligible for this warranty, customers registered their purchases with the Organisation via the Organisation’s website at http://www.globaloutsourceasia.com (the “**Website**”). The Organisation collected various personal data from such customers for this purpose, including personal information such as their name, email address, mailing address and contact number, and details of the customers’ purchases such as the name of the product purchased, the purchase date, the name of the retailer and the location of the physical store where the product was purchased (collectively, the “**Personal Data**”).

2. The Personal Data Protection Commission (**“the Commission**”) received a complaint on 23 September 2018 that the complainant could access the Personal Data of another individual when viewing a warranty registration summary page on the Website (**the “Incident”**).

3. The Organisation admitted to the occurrence of the Incident but was unable to identify the cause of the Incident. The Commission found that the Organisation had not provided any security requirements to the vendor it had engaged sometime in 2013 to develop the Website. Consequently, it had not reviewed the Website’s security arrangements or conducted any security testing on the Website. In the circumstances, the Organisation had not implemented reasonable security arrangements to protect the personal data collected by the Website (including but not limited to the Personal Data disclosed in the Incident) and is therefore in breach of section 24 of the PDPA.

4. The Commission also found that the Organisation did not have any internal data protection policies for its employees in relation to the handling of personal data for the purposes of registering products through the Website. This failure to develop and implement such internal data protection policies is a breach of section 12 of the PDPA.

5. The Organisation has since removed the warranty registration section on its website and is in the process of revamping its Website to incorporate the necessary security arrangements. The Organisation is directed to develop and implement policies for data protection and staff training in data protection, and to put all employees handling personal data through data protection training.

## Worksmartly Pte. Ltd.

## [2020] SGPDPCS 19

| **Case Number** | : | Case No. DP-2004-B6162 |
| --- | --- | --- |
| **Decision Date** | : | 17 September 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Worksmartly Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Disclosure of personal data* – *Insufficient administrative security arrangements*

*Data Protection* – *Retention limitation obligation* – *Purpose for which the personal data was collected is no longer served by retaining the data* – *Retention is no longer necessary for legal or business purposes*

1. On 2 April 2020, Roche Singapore Pte Ltd (“**Roche**”) informed the Personal Data Protection Commission (the “**Commission**”) of a data security incident involving its former vendor, Worksmartly Pte. Ltd. (the “**Organisation**”). Roche had detected an unauthorised disclosure of their employees’ data on GitHub repository (“**GitHub**”) on 3 March 2020 (the “**Incident**”).

2. The Organisation subsequently requested for this matter to be handled under the Commission’s expedited decision procedure. In this regard, the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. It also admitted that it was in breach of sections 24 and 25 of the Personal Data Protection Act (the “**PDPA**”).

**Background**

3. The Organisation was engaged by Roche in 2017 to provide finance and payroll processing services. In order for the Organisation to provide the said services, Roche handed over its employees’ personal data to the Organisation. The contract between the parties was subsequently terminated, and the Organisation’s last day of service was 31 December 2018.

**The Incident**

4. On or around 28 February 2020, one of the Organisation’s employees uploaded a file on the Organisation’s GitHub account (the “**File**”). When doing so, the employee changed the setting of the GitHub account from “private” to “public” under the mistaken belief that the File would only be accessible to other members of the Organisation. In fact, the change in setting had resulted in the File being accessible to the public.

5. The File contained the personal data of 308 individuals, which comprised Roche’s current and former employees (the “**Employees**”), and their dependents (the “**Dependents**”). The personal data included:

a. For the Employees: name, NRIC/FIN/Passport number, address, date of birth, race, citizenship, employee ID, Roche email address, role title, employment commencement date, salary, bank account name and numbers and name of bank; and

b. For the Dependents: name, NRIC/FIN/Passport number, date of birth and contact number.

6. The File was used for data migration during the initial service engagement in 2017. The File was supposed to have been deleted—along with other files containing Roche’s employees’ data—before the Organisation’s last day of service, i.e. 31 December 2018. However, because the File was stored in a different folder from the other files, the Organisation had inadvertently omitted to delete the File. This led to the File being exposed to the public when the Organisation’s employee set the GitHub folder’s setting to “public” as stated at [4] above.

7. The File was exposed to the public for a period of five days from 28 February 2020 to 3 March 2020. Based on GitHub’s logs, the repository containing the File was accessed 23 times and downloaded 11 times during this time.

**The Contraventions**

8. The Organisation admitted that it lacked checks to manage the correct security settings of its GitHub account and had relied solely on employees to do the right thing. The Organisation also admitted that it had not conducted the necessary housekeeping and maintenance of files, which resulted in retaining the File when it was no longer required for business or legal purposes.

9. In the circumstances, the Deputy Commissioner for Personal Data Protection finds the Organisation in breach of the Protection Obligation under section 24 and Retention Obligation under section 25 of the PDPA.

10. Upon realising the Incident, the Organisation took the following remedial action:

a. Immediately set the GitHub access to “private” and deleted the File;

b. Reset the passwords for all the databases and servers;

c. Conducted housekeeping to ensure removal of obsolete files from GitHub;

d. Directed its GitHub account administrator to always set the repositories to “private” and introduced a disciplinary framework for the mishandling of its GitHub accounts.

**The Decision**

11. The Deputy Commissioner for Personal Data Protection notes that the Organisation had admitted to a breach of Protection and Retention Obligations under the PDPA, and had cooperated with the Commission’s investigation and taken prompt remedial action.

12. On account of the above, the Deputy Commissioner for Personal Data Protection directs the Organisation to pay a financial penalty of $5,000 within 30 days from the date of this direction (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).

13. In view of the remedial actions taken by the Organisation, the Commission will not be issuing any other directions.

## CPR Vision Management Pte Ltd and others

## [2022] SGPDPCS 17

| **Case Number** | : | DP-2207-B8974 |
| --- | --- | --- |
| **Decision Date** | : | 07 December 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | CPR Vision Management Pte Ltd — L’Oreal Singapore Pte Ltd — L’Occitane Singapore |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Failure to implement reasonable security arrangements*

*Data Protection* – *Retention limitation obligation* – *Purpose for which personal data was collected no longer served by retaining data* – *Retention no longer necessary for legal or business purposes*

1. The Personal Data Protection Commission (the “**Commission**”) received data breach notification reports from (i) L’Oreal Singapore Pte Ltd (“**L’Oreal**”) on 29 October 2021 and (ii) L’Occitane Singapore Pte Ltd (“**L’Occitane**”) on 1 November 2021 respectively of a ransomware attack on their customer relationship management (“**CRM**”) system vendor, CPR Vision Management Pte Ltd (the “**Organisation**”). The Organisation is a data intermediary that helped to process personal data collected by L’Oreal and L’Occitane.

2. The ransomware attack affected a server and three network attached storage (“**NAS**”) devices in the Organisation’s office (“**office network**”), and led to the encryption of the personal data belonging to 83,640 L’Occitane’s customers and 35,079 L’Oreal’s customers, which included their name, address, email address, mobile number, NRIC number, date of birth, age, gender, race, nationality, loyalty points and amount spent.

3. The Organisation requested, and the Commission agreed, for this matter to proceed under the Expedited Decision Breach Procedure. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision. It also admitted to a breach of the Protection Obligation under Section 24 and the Retention Limitation Obligation under Section 25 of the Personal Data Protection Act (the “**PDPA**”).

4. The Organisation’s internal investigations found the threat actor had first gained access to the office network via a compromised user account VPN connection on 13 October 2021 before executing the ransomware attack on or about 15 October 2021. However, due to the limited data logs available on the Organisation’s FortiGate firewall and VPN appliance, the Organisation was not able to determine how the threat actor gained access to the compromised user account VPN. As part of the immediate remediation efforts, the Organisation reset the credentials of the compromised user account VPN and the password credentials of all VPN accounts across the Organisation.

5. The Organisation admitted that its endpoint security solution would have been able to detect and block the unauthorised entry attempts to the office network affected in the Incident. However, the Organisation failed to extend the deployment of this protection solution to the affected office network. This could have been because the domain controller server within the affected office network had been earmarked to be decommissioned after the data was copied to MS365 Sharepoint. Another reason for the omission may have been the fact that the Organisation set up the affected office network for business continuity purposes, when it shifted to its new premises, sometime between 6 – 9 April 2020, on the eve of the nation-wide COVID-19 circuit breaker in Singapore.

6. The Commission finds the Organisation in breach of the Protection Obligation as it failed to have reasonable security arrangements in place to protect the personal data in its possession and control. As a CRM system vendor, the Organisation processes and processed a high volume of web traffic containing personal data on behalf of many e-commerce retailers, including L’Oreal and L’Occitane, and would ordinarily be held to a higher standard. The Organisation’s omission to deploy its endpoint security solution to the affected office network suggests that the Organisation failed to maintain an inventory of its data assets.

7. Even if there were extenuating circumstances in April 2020 which could have partly excused the Organisation’s omission to include the affected office network in its data inventory, it was inexcusable for the Organisation to let this state of affairs persist for more than one and-a-half years, from April 2020 until October 2021. We should add however, that as part of its remediation efforts, the Organisation has since ensured that its endpoint security solution was deployed to all office and end-user devices.

8. The Organisation also admitted to being in breach of the Retention Limitation Obligation. The Organisation admitted that the affected personal data in the Incident had been legacy content, which should have been deleted together with the domain controller server earmarked for decommissioning, and for which no business or legal purpose existed for retention. The Organisation highlighted however, that this lapse was not in accordance with its own data retention policy. Had the Organisation complied with the Retention Limitation Obligation and deleted the personal data in question, the Incident would not have amounted to a breach of the Retention Limitation Obligation under the PDPA.

9. In the course of our investigations, L’Oreal furnished documentary evidence which showed that L’Oreal had specifically instructed the Organisation, pursuant to its data retention policies, to delete the affected personal data on 26 March 2021. This was duly acknowledged by the Organisation, and the Organisation furnished a purported Certificate of Destruction dated 17 May 2021 stating that the personal data had been deleted on 6 May 2021.

10. Similarly, L’Occitane also raised its concerns that the Organisation failed to seek its prior written consent before duplicating the personal data to other non-production environments.

11. The Commission is satisfied that neither L’Oreal nor L’Occitane had any knowledge of the retention and storage of the legacy personal data by the Organisation on the affected NAS device; and neither had any control over the NAS device used by the Organisation to store the personal data affected by the ransomware attack. Both L’Oreal and L’Occitane had also adequately provided in their contracts with the Organisation to ensure compliance with the Protection and Retention Limitation Obligations under the PDPA. The Commission is therefore of the view that despite the personal data breach incident, L’Oreal and L’Occitane had acted consistently with and complied with the relevant obligations under the PDPA.

12. Having considered the circumstances set out above, including the Organisation’s upfront admission of liability, and the fact that data analysis conducted by the data security team of the Organisation’s parent company did not uncover any evidence to suggest that data exfiltration or modification had occurred, the Commission considered that it would be most appropriate in lieu of imposing a financial penalty, to direct the Organisation to comply with the following action:

a. Conduct a thorough security audit (with report) of its technical and administrative arrangements for the protection of personal data in its possession or control;

b. Rectify any security gaps identified in the security audit report;

c. Conduct a comprehensive review of all of the Organisation’s databases containing personal data to ensure full compliance with the Retention Limitation Obligation under Section 25 PDPA;

d. Review and update the personal data policies of the Organisation as applicable, including clarification of the roles of data intermediaries and vendors in complying with the Retention Limitation Obligation under section 25 of the PDPA, within 60 days from the date the security audit report is delivered to the Organisation; and

e. Inform the Commission within 1 week of the completion of the steps directed above.

The following are the provision of the Personal Data Protection Act 2012 cited in the above summary:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Protection of personal data**

**24.** An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks and;

(b) the loss of any storage medium or device on which personal data is stored.

**Retention of personal data**

**25.** An organisation must cease to retain its documents containing persona data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that –

(a) the purpose for which the personal data was collected is no longer being served by retention of the personal data; and

(b) retention is no longer necessary for legal or business purposes.

## Zero1 Pte Ltd and another

## [2020] SGPDPCS 9

| **Case Number** | : | Case No. DP-1903-B3630, DP-1908-B4431 |
| --- | --- | --- |
| **Decision Date** | : | 07 April 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Zero1 Pte Ltd; IP Tribe Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access to and disclosure of personal data* – *Insufficient security arrangements*

*Data Protection* – *Data intermediary* – *Obligations of data intermediary and organisation which engages a data intermediary*

1. On 22 March 2019, Zero1 Pte Ltd (the “**Organisation**”) voluntarily informed the Personal Data Protection Commission (the “**Commission**”) that invoices containing the personal data of their subscribers had been emailed to unintended recipients (the “**Incident**”). Each invoice contained the name, address, subscriber ID, mobile number, mobile charges, and the call details of any international calls made by a subscriber (the “**Personal Data**”). Each email contained a subscriber’s invoice which was unintendedly sent to another subscriber instead.

2. The Organisation was a licensed Mobile Virtual Network Operation that provided mobile services. It partnered Singtel Mobile Singapore Pte. Ltd. (“**Singtel**”), which appointed IP Tribe Pte Ltd (“**IPT**”) to develop and deploy a Mobile Virtual Network Enabler (the “**1st Platform**”) to manage subscriber accounts.

3. IPT ran the 1st Platform for the Organisation, including generating and sending monthly emails to subscribers. IPT then subcontracted the provision of the billing system within the 1st Platform to Openet Telecom Sales Limited (“**Openet**”). The 1st Platform was deployed in August 2018.

4. A replacement platform (the “**New Platform**”) was deployed in 2019. Openet subcontracted 6D Technologies (“**6D**”) to migrate subscriber data from the 1st Platform to the New Platform. In February 2019, 6D migrated the data of 12,000 to 15,000 subscribers.

5. The Incident was caused by Batch ID duplication. The Batch ID was a unique number that tagged each subscriber to his name and email address. The migration was staggered and some errors made it necessary to delete data migrated earlier. However, due to a coding error, not all previously migrated data had been deleted. The New Platform failed to recognise the Batch IDs that were not deleted and re-issued the same Batch IDs. As a result, 118 invoices belonging to subscribers with duplicated Batch IDs were affected. Since each Batch ID determined the email address to which an invoice was sent, Batch ID duplication resulted in the New Platform emailing the 118 invoices to the wrong addresses.

6. Before a new IT system or a change to an IT system goes live, pre-launch testing is important to determine that the system would run as expected. The Organisation, IPT and 6D jointly conducted pre-launch testing. The Organisation as the end user, and IPT as the Organisation’s data intermediary, should have scoped the pre-launch testing to include a simulation of expected scenarios. In particular, the scenario in which migration to the New Platform is staggered and a high volume of email addresses would have been assigned Batch IDs for the sending of emails to the right subscriber (“**Migration Scenario**”).

7. However, in the pre-launch testing, the Migration Scenario was not catered for. Only two test accounts were used to check that the New Platform could generate and email invoices to the right parties. This was insufficient to simulate expected usage. Consequently, the tests failed to surface this issue.

8. The proper scoping of pre-launching testing is important for the detection of functionality issues that may put personal data at risk. In failing to simulate the expected scenarios, in particular the Migration Scenario, the Organisation and IPT failed to meet the reasonable standard required to discharge the Protection Obligation.

9. Furthermore, the processes to ensure that the New Platform would issue unique Batch IDs were inadequate. A date/time stamp could have been included as part of each Batch ID to avoid duplication, which was implemented only after the Incident.

10. In deciding to find the Organisation and IPT respectively in breach of the Protection Obligation under the Personal Data Protection Act 2012 (the “**PDPA**”) and to issue a Warning to each party, the Deputy Commissioner for Personal Data Protection took into account the following:

a. Although the Organisation neither owned nor operated the New Platform, it remained a data controller in control of its subscribers’ Personal Data.

b. IPT was the Organisation’s data intermediary in developing the New Platform, which included migration of the personal data of subscribers. IPT relied on Openet as its subcontractor, and the Batch ID duplication occurred as a result of errors during the migration that was performed by 6D. Notwithstanding the representations made by IPT, it retained a key role, together with the Organisation, in scoping the pre-launch testing of the New Platform.

c. The tests proved to be inadequate and a reasonable opportunity to prevent the Incident was missed. For this, both the Organisation and IPT bore responsibility.

11. No directions are required as the Organisation and IPT had taken remedial actions to address the gaps in security arrangements respectively.

## Tanah Merah Country Club

## [2021] SGPDPCS 16

| **Case Number** | : | DP-2102-B7951 |
| --- | --- | --- |
| **Decision Date** | : | 20 December 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Tanah Merah Country Club |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data*  – *Insufficient security arrangements*

*Data Protection* – *Protection obligation* – *Failure to document password policy*

*Data Protection* – *Protection obligation* – *Failure to conduct staff training*

1. On 24 February 2021, Tanah Merah Country Club (the **“Organisation”**) notified the Personal Data Protection Commission (the **“Commission”**) that an employee’s (the **“Employee”**) email account had been compromised and 600 phishing emails had been sent to various individuals on 22 February 2021 (the **“Incident”**).

2. The Organisation subsequently requested for this matter to be handled under the Commission’s expedited breach decision procedure. This meant that the Organisation voluntarily and unequivocally admitted to the facts set out within this decision. It also admitted that it was in breach of section 24 of the Personal Data Protection Act (the “PDPA”).

3. The Organisation’s investigations revealed that it was likely that the Organisation’s email accounts had been subjected to password spraying attacks. Password spraying is a type of password attack where a threat actor uses a few commonly used or default passwords against many different accounts. In contrast to traditional brute-force attacks, where the targeted account may quickly get locked-out due to account-lockout policies that only allow for a limited number of failed attempts, password spraying attacks allow a threat actor to mount an attack against many accounts with a single commonly used password, while remaining undetected, before attempting the second password. At the time of the Incident, the Employee was using the password “XXX”, which the Employee had not changed for a period of nearly 5 years, since 2016 to the time of the Incident on 22 February 2021.

4. After gaining access to the Employee’s email account, the threat actor accessed the personal data of 467 individuals, including:

a. The email addresses of 155 club members and 284 members of public, which the threat actor had used to send phishing emails to.

b. The name, and/or NRIC number, and/or email addresses of a further 28 individuals contained within the emails.

5. Prior to the Incident, the Organisation had informed its employees via an email IT newsletter in August 2018 of the need to change their password once every 3 months, and to use passwords which are at least 8 characters, with a combination of uppercase letter, lowercase letter, special character, and number. In September 2019, the Organisation sent another email IT newsletter to inform its employees of the implementation of a domain password policy. This meant that the above-mentioned password requirements became system enforced.

6. Despite disseminating these email IT newsletters where it referred to its password requirements and the implementation of a system-enforced domain password policy, the Organisation failed to further develop its password requirements into a full-fledged password policy in writing and disseminate it in such a manner whereby all its employees, new and old, could easily take reference from the password policy and consult the password policy at any time. It was only on 23 February 2021, after the Incident had occurred, that the Organisation documented its password policy in writing.

7. We had previously emphasized the importance of organisations having a written personal data protection policy so as to guide its employees and staff in *Re Furnituremart.sg* [2017] SGPDPC 7. In that case, the Commission noted at [14] as follows:

“The lack of a written policy is a big drawback to the protection of personal data. Without having a policy in writing, employees and staff would not have a reference for the organisation’s policies and practices which they are to follow in order to protect personal data. Such policies and practices would be ineffective if passed on by word of mouth, and indeed, the Organisation may run the risk of the policies and practices being passed on incorrectly. Having a written policy is conducive to the conduct of internal training, which is a necessary component of an internal data protection programme”.

8. A properly documented password policy is therefore crucial for the protection of personal data. In this regard, the Organisation admitted that it had breached the Protection Obligation under section 24 of the PDPA as it failed to document its password policy in writing.

9. The Commission recently issued a “Guide to Data Protection Practices for ICT Systems” on 14 September 2021. In the Guide, we noted that in order to maintain good governance over its personal data and mitigate data breach risks throughout the data lifecycle, organisations should develop and implement ICT security policies for data protection. Key ICT policies would include a password policy.

10. Prior to the issuance of this Guide, the Commission had also released a Handbook on “How to Guard Against Common Types of Data Breaches”, which is complemented by the Checklists to Guard Against Common Types of Data Breaches. In the Handbook, the Commission identified poor management of accounts and passwords as one of the five common causes and types of data breaches. We noted that the use of default value, weak or easily guessable passwords result in accounts being particularly vulnerable to brute force or dictionary attacks. We therefore recommended that organisations adopt and implement a strong password policy, with the following good practices:

a. Enforcing a password history policy to ensure that employees do not reuse their previous passwords;

b. Encouraging users to use passphrases such as “Iwant2l@se10kg”, which may be long and complex, yet easy to remember; and

c. Discouraging users from using the same passwords across different systems.

11. In this regard, we observed that the Organisation’s email IT newsletters to its employees had cited “TMCC\_Password\_123” as an example of what amounts to a good password. Unfortunately, we are unable to endorse the Organisation’s choice of “TMCC\_Password\_123” as an example of what amounts to a good password. In *Re Chizzle Pte Ltd* [2020] SGPDPCR 1, the Commission highlighted that a password that complies with the recommended password complexity rules in form could still be a weak password easily guessable and vulnerable to password attacks if the password incorporates components such as the organisation’s name, which is not difficult to guess and crack. In this regard, we note that in the Organisation’s password policy, which it adopted on 23 February 2021, the Organisation now recommends that its employees refrain from the use of the Organisation’s name or abbreviations such as “TMCC”.

12. In addition, the Organisation also admitted that it had failed to provide structured and organised training for its staff on how to ensure compliance with the obligations under the PDPA and how personal data should be handled in the course of their work. Only ad-hoc and informal training had been provided. As a result, the Employee lacked the awareness of the need to change her password at more regular intervals and of the need to use a strong password. The Employee did not receive system prompts to change her password as the domain password policy was not pushed down to her system due to a domain controller disruption.

13. The Commission wishes to emphasize 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 under section 24 of the PDPA 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.

14. In light of the above, the Deputy Commissioner for Personal Data Protection finds the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the “PDPA”).

15. Following the incident, the Organisation engaged an IT forensic vendor for investigation. We note that the Organisation has since implemented the measures recommended by the vendor to improve its cybersecurity. The Organisation has also documented its password policy, implemented regular updates, conducted user awareness training, and other trainings on personal data protection.

16. The Organisation cooperated with the Commission’s investigations, admitted to its breach of the Protection Obligation, and took prompt remedial actions.

17. Having considered the circumstances set out above, the factors listed at section 48J(6) of the PDPA, and in particular, the Organisation’s voluntary admission to being in breach of section 24 of the PDPA under the Expedited Breach Decision Procedure, which is a significant mitigation factor, the Deputy Commissioner for Personal Data Protection requires the Organisation to pay a financial penalty of $4,000 within 30 days from the notice accompanying date 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.

18. Finally, in view of the remedial actions taken by the Organisation, no other directions are necessary.

## Webcada Pte Ltd

## [2021] SGPDPCS 6

| **Case Number** | : | Case No. DP-2009-B6931 |
| --- | --- | --- |
| **Decision Date** | : | 06 May 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Webcada Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access of personal data* – *Insufficient security arrangements*

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

1. On 4 September 2020, Webcada Pte Ltd (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) that three of its database servers had been subjected to a ransomware attack on 29 August 2020 (the “**Incident**”).

2. The personal data of 522,722 individuals were affected in the Incident. The datasets affected comprised of the individuals’ names, phone numbers, dates of birth, addresses and order histories.

3. Following the Incident, the Organisation engaged an independent third-party consultant to investigate, review and assist in the implementation of additional data protection measures.

4. Investigations revealed that the ransomware had been uploaded onto the affected servers via the Intelligent Platform Management Interface ("**IPMI**"). The IPMI is a set of computer interface specifications used for remote monitoring and management of servers. There was no evidence of data exfiltration, and all affected data was restored from available back-ups.

5. The Organisation took the following remedial measures after the Incident:

(a) IPMI was permanently disabled for all servers;

(b) The public IP address of all servers was removed and all remote management access to the servers was configured to allow only trusted IP addresses;

(c) End-point protection software with threat hunting capabilities was installed on all servers and computers within the Organisation; and

(d) A written data protection policy was developed and implemented to comply with the provisions of the Personal Data Protection Act 2012 (the "**PDPA**").

6. In its representations to the PDPC, the Organisation admitted to having breached the Accountability Obligation under section 12 and the Protection Obligation under section 24 of the PDPA, and requested for the matter to be dealt with in accordance with the PDPC’s Expedited Decision Procedure.

*Section 12 of the PDPA*

7. First, the Organisation admitted it did not have a written data protection policy prior to the Incident. In this regard, it is important to reiterate that an organisation must document its data protection policies and practices in writing as they serve to increase awareness and ensure accountability of the organisation's obligations under the PDPA. This requirement has been emphasized multiple times in previous decisions[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/107154.xml&queryStr=(personal%20data%20protection%20act)#fn1).

*Section 24 of the PDPA*

8. Second, the Organisation admitted that it did not configure its IPMI access settings correctly prior to the Incident. It enabled access to the IPMI from the public Internet when this was not necessary. Furthermore, in the monthly vulnerability scans carried out by the Organisation, it had omitted to scan the IPMI. Hence, it was not able to detect vulnerabilities in its IPMI, which were exploited to gain access to and upload the ransomware on the servers.

9. In the circumstances, the Organisation is found to have breached sections 12 and 24 of the PDPA.

10. After considering the factors listed at section 48J(6) of the PDPA and the circumstances of this case, including (i) the Organisation's upfront voluntary admission of liability which significantly reduced the time and resources required for investigations; and (ii) the Organisation's prompt remedial actions, the Organisation is given notice to pay a financial penalty of $25,000.

11. The Organisation must make payment of the financial penalty 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.

12. In view of the remedial actions taken by the Organisation, the Commission will not issue any directions under section 48I of the PDPA.

[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/107154.xml&queryStr=(personal%20data%20protection%20act)#fnref1) See *Re Aviva Ltd* [2017] SGPDC 14 at [32]; *Re Singapore Taekwondo Federation* [2018] SGPDC 17 at [39] to [42]; *Re AgcDesign Pte Ltd* [2019] SGPDC 23 at [4] to [5]; *Re (1)Everlast Projects Pte Ltd (2)Everlast Industries (S) Pte Ltd (3) ELG Specialist Pte Ltd* [2020] SGPDC 20 at [8] to [9]

## Crawfort Pte. Ltd.

## [2022] SGPDPCS 12

| **Case Number** | : | DP-2106-B8446 |
| --- | --- | --- |
| **Decision Date** | : | 07 June 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Crawfort Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements* – *Failure to implement reasonable access controls*

1. On 9 June 2021, Crawfort Pte. Ltd. (the “**Organisation**”) notified the Personal Data Protection Commission (the **“Commission”**) of the sale of the Organisation’s customer data on the dark web (the **“Incident”**).

2. The personal data of 5,421 customers were affected. The datasets affected comprised NRIC images (front and back), PDF copies of loan contract (containing all the information in the NRIC, age, email address, contact number and loan amount) and PDF copies of income document (payslip, CPF statements or IRAS Notice of Assessment).

3. The Organisation engaged external cyber security teams to investigate the Incident. The investigation identified an opened S3 server port in the Organisation’s AWS environment as the cause of the Incident.

4. The Organisation explained that it had opened the S3 server port for **one week** during a data migration exercise sometime on or about 15 April 2020 for business continuity purposes. On 3 April 2020, the Singapore government had announced that the country will enter into a Circuit Breaker to contain the spread of COVID-19. All non-essential workplaces, including the Organisation, had to be closed from 7 April 2020. In order to continue its business, the Organisation had to pivot its operations so as to allow its staff to work from home and its customers to make loan applications remotely. Within a very short period, the Organisation had to carry out the data migration exercise and as a result, overlooked conducting a risk assessment prior to conducting the data migration exercise.

5. The opened S3 server port connected directly to the S3 server hosting the S3 buckets, which contained the affected personal data. The open remote port enabled attempts to connect to the Organisation’s AWS environment from the internet. Furthermore, the S3 bucket containing the affected personal data was publicly accessible due to a misconfiguration of the S3 bucket. As a result, the threat actor was able to gain access to the publicly accessible S3 bucket **during the one-week period**.

6. The Organisation implemented the following remedial measures after the Incident:

(a) Reset and reconfigured all whitelisted IPs to AWS server;

(b) Reset and reconfigured all VPNs;

(c) Limited the whitelisted IP addresses to its web portal;

(d) Conducted a penetration test;

(e) Monitored the dark web to ensure that data was not circulated;

(f) Engaged independent cyber security consultant to carry out investigation, study the IT infrastructure and propose improvements to their systems; and

(g) Notified affected individuals.

7. The Commission accepted the Organisation’s request for this matter to be handled under the Commission’s expedited breach decision procedure. This meant that the Organisation had voluntarily provided and unequivocally admitted to the facts set out in this decision. The Organisation also admitted that it was in breach of section 24 of the Personal Data Protection Act (the “**PDPA**”).

8. The Organisation admitted that it failed to conduct a reasonable risk assessment before carrying out the data migration exercise. There was no access control to the S3 bucket containing the affected personal data during the week-long migration exercise. This, coupled with the open port, allowed the threat actor to gain access to the affected personal data.

9. In the circumstances, the Organisation is found to be in breach of section 24 of the PDPA.

10. Having considered the circumstances set out above and the factors listed in section 48J(6) of the PDPA, including (i) the Organisation’s upfront voluntary admission of liability which significantly reduced the time and resources required for investigations; and (ii) the prompt remedial actions undertaken by the Organisation, the Commission considered that it would be most appropriate in lieu of imposing a financial penalty, to direct the Organisation to comply with the following:

(a) To engage qualified security service provider to conduct a thorough security audit of its technical and administrative arrangements for the security and maintenance of its AWS S3 environment that contains personal data in the Organisation’s possession or control;

(b) Provide the full security audit report to the Commission, no later than 60 days from the date of the issue of this direction;

(c) Rectify any security gaps identified in the security audit report, review and update its personal data protection policies as applicable within 60 days from the date the security audit report is provided; and

(d) Inform the Commission within 1 week of completion of rectification and implementation in response to the security audit report.

## Vhive Pte Ltd

## [2022] SGPDPCS 8

| **Case Number** | : | DP-2013-B8138 |
| --- | --- | --- |
| **Decision Date** | : | 08 March 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Vhive Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Insufficient security arrangements*

*Data Protection* – *Protection obligation* – *No written agreement with IT vendor*

1. On 26 March 2021, Vhive Pte Ltd (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) of a ransomware attack that affected its customer database (the “**Incident**”). Approximately 186,281 individuals’ names, addresses, email addresses, telephone numbers, hashed passwords and customer IDs were affected.

2. The Organisation subsequently requested for this matter to be handled under the Commission’s expedited breach decision procedure. This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision, and admitted that it was in breach of section 24(a) of the Personal Data Protection Act (the “**PDPA**”).

3. The Organisation’s forensic investigation results revealed that the Organisation’s IT infrastructure had been outdated, with multiple vulnerabilities at the time of the Incident. The Organisation’s e-commerce server ran on an outdated webserver service. This, together with an unpatched firewall, allowed the threat actor to remotely execute unauthorised code on the e-commerce server, and gained backdoor access to the e-commerce server to carry out the ransomware attack.

4. The Organisation had engaged an IT vendor to host, manage and maintain the e-commerce server and all its other IT systems. However, our investigations revealed that despite the purported “engagement”, there was in fact no written contract between the Organisation and its IT vendor at the time of the Incident.

5. In *Spize Concepts Pte Ltd* [2019] SGPDPC 22 at [22], we had stated that section 4(2) of the PDPA imposes on organisations that engage data intermediaries to do so “pursuant to a contract which is evidenced or made in writing”. In that case, we also highlighted that one specific category of policies and practices under section 12(a) of the PDPA that an organisation should develop and implement is the contractual documentation relating to the scope of the data intermediary relationship, and failure to do so would amount to a breach. The raison d’etre is that the outsourcing of data processing activities must be clearly scoped, and the respective roles and responsibilities between the organization and the data intermediary clearly identified from the outset. In the absence of any written contract and the lack of evidence to show the scope, roles and responsibilities of the data processing outsourcing, the Organisation remained solely responsible for complying with the obligations under the PDPA, including the obligation to make reasonable security arrangements to protect the personal data in its possession or under its control under section 24 of the PDPA.

6. The Organisation’s outdated webserver was used to host the Organisation’s website and its online storefront. In this regard, the Commission had previously issued a Guide on Building Websites for SMEs in 2016, which was subsequently updated and revised in July 2018. In this Guide, the Commission emphasized the importance of ensuring the protection of personal data and the security of the website throughout the life cycle, including ensuring the clear delineation of responsibilities when an organization engages an IT vendor.

7. We wish to reiterate our observations in [4.2.1] of the Guide, where we highlighted the need to consider and properly document an IT vendor’s scope of work, and stated as follows:

Organisations should emphasise the need for personal data protection to their IT vendors, by making it part of their contractual terms. The contract should also state clearly the responsibilities of the IT vendor with respect to the PDPA. When discussing the scope of outsourced work, organisations should consider whether the IT vendor’s scope of work will include any of the following:

● Requiring that IT vendors consider how the personal data should be handled as part of the design and layout of the website.

● Planning and developing the website in a way that ensures that it does not contain any web application vulnerabilities that could expose the personal data of individuals collected, stored or accessed via the website through the Internet.

● Requiring that IT vendors who provide hosting for the website should ensure that the servers and networks are securely configured and adequately protected against unauthorised access.

● Requiring IT vendors to ensure that all work done is fully documented and that all documentation is handed over to the organisation at the completion of the project. Documents should capture the website’s requirements, design specifications, user test scripts, user test results, as well as server and network configurations.

● When engaging IT vendors to provide maintenance and/or administrative support for the website, requiring that any changes they make to the website do not contain vulnerabilities that could expose the personal data. Additionally, discussing whether they have technical and/or non-technical processes in place to prevent the personal data from being exposed accidentally or otherwise.

● Requiring that IT vendors providing maintenance and/or administrative support to ensure that all changes to the website are secure and documented, and that the document is kept up to date.

8. The Organisation admitted the weakness in its IT infrastructure and its failure to give due attention to the protection of the personal data of its customers had contributed to the Incident.

9. On the facts, the Organisation’s failure to ensure that there was a written contract with its IT vendor not only meant that there was a lack of clarity on the scope of work expected from the IT vendor, but also that the Organisation had failed to stipulate clear written security maintenance requirements and data protection requirements to its IT vendor to ensure the protection of personal data it was in control or in possession of. This ultimately resulted in a lack of system maintenance, including security maintenance by the Organisation.

10. Investigations further revealed that the Organisation did not have a security maintenance policy, which would have made up for the lack of specification of these requirements to its IT vendor, nor did the Organisation conduct any of its own scheduled security reviews, through which it could have detected any security inadequacy or vulnerabilities within its IT infrastructure.

11. In the above circumstances, the Organisation is found to have breached the Protection Obligation under section 24(a) of the PDPA.

12. Following the Incident, the Organisation decommissioned its e-commerce webserver and overhauled its IT infrastructure. Apart from deciding to conduct online sales solely through third party websites, the Organisation also rebuilt its ERP server in a secure environment with new set of firewalls, updated its operating systems and software, implemented the use of SSL-VPN for remote access, and engaged a new IT vendor with the data security and data protection provisions properly specified in a written contract. The Organisation also reviewed and updated all its internal policies relevant to the protection of personal data.

13. In deciding the appropriate outcome in this case, the Commission acknowledges the cooperation extended by the Organisation to the Commission throughout the course of our investigations. The Organisation had also voluntarily admitted to its breach of the Protection Obligation, and took prompt remediation actions to address its security gaps. The Organisation was able to restore fully the personal data affected without loss, thereby minimizing any disruptions to its operations.

14. Having considered the circumstances set out above and the factors listed at section 48J(6) of the PDPA, the Commissioner for Personal Data Protection hereby finds the Organisation in breach and requires the Organisation to pay a financial penalty of $22,000 within 30 days from the notice accompanying date 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.

15. In view of the remedial action by the Organisation, no directions under section 48I are necessary.

## Audio House Marketing Pte Ltd

## [2022] SGPDPCS 11

| **Case Number** | : | DP-2106-B8421 |
| --- | --- | --- |
| **Decision Date** | : | 27 May 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Audio House Marketing Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Insufficient security arrangements* – *Failure to conduct reasonable periodic security review*

*Data Protection* – *Protection obligation* – *No written agreement with IT vendor*

1. On 1 June 2021, Audio House Marketing Pte Ltd (the “**Organisation**”) notified the Personal Data Protection Commission (the **“Commission”**) of a ransomware affecting its customer database (the **“Incident”**). Approximately 98,000 individuals’ names, addresses, email addresses and telephone numbers, in the nature of contact information, were affected.

2. The Organisation subsequently requested for this matter to be handled under the Commission’s expedited breach decision procedure. This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision; and admitted that it was in breach of section 24 of the Personal Data Protection Act (the “**PDPA**”).

3. The Organisation’s internal investigations revealed that PHP files used to develop a web application on the Organisation’s website contained vulnerabilities that allowed the threat actor to carry out a SQL injection attack. The Organisation admitted that it is possible that the vulnerabilities in the PHP files had existed since April 2017, when its website was first launched. Further, even though the Organisation had conducted pre-launch tests prior to the launch of its website, the Organisation admitted that it failed to identify and detect the existing vulnerabilities in the PHP files.

4. SQL injection attacks are well-known vulnerabilities: see “Top Ten” list of the Open Web Application Security Project (OWASP). The Commission has consistently advised organisations to take the necessary precautions to guard against the risk of injection attacks (see para. 15.3 of the Commission’s Guide to Securing Personal Data in Electronic Medium, published on 8 May 2015, and revised on 20 January 2017). We note that apart from conducting functionality testing of features such as the shopping cart and payment on its website, the Organisation did not conduct any vulnerability scanning and assessment that would have provided a reasonable opportunity to discover the vulnerabilities in the PHP files that were eventually exploited in the Incident.

5. Compounding the above, the Organisation also did not conduct reasonable periodic security review. A reasonable periodic security review would include vulnerability scanning and assessments, which would have offered the Organisation the opportunity to detect any vulnerabilities that were not detected during the pre-launch tests, or any vulnerabilities that may have arisen since.

6. Periodic security reviews is also a practice that the Commission has consistently advised organisations to adopt. In our Checklists to Guard against Common Types of Data Breaches, the Commission highlighted that conducting a periodic security review is a basic practice that all organisations ought to embrace. This is also reiterated in para. 6.1(a) of the Commission’s Guide to Securing Personal Data in Electronic Medium where we stated that it was a good practice for organisations to “conduct regular ICT security audits, scans and tests to detect vulnerabilities and non-compliance with organizational standards”, and Table 13(f) of the same Guide where we encouraged organisations to perform web application scanning and source code analysis to help detect common web vulnerabilities, in particular, those identified in the “Top Ten” list of the OWASP, which includes SQL injection attacks.

7. With the use of IT comes the responsibility for data security in IT systems. We urge organisations who may be unable to conduct such security reviews on their own to engage the necessary expertise from the professionals.

8. Having said that, we note that the Organisation’s website was built by a company, which the Organisation’s main IT vendor had engaged on the Organisation’s behalf. The Organisation did not have any contract with the company that developed the website. As a result, the Organisation failed to stipulate clear job specifications or any data protection requirements on the company that developed its website. There was also an absence of any data protection requirements in the Organisation’s contract with its main IT vendor, who it relied upon to manage and maintain its IT systems. The Commission’s published decisions[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/109384.xml&queryStr=(personal%20data%20protection%20act)#fn1) have emphasized that organisations engaging IT vendors should – a) stipulate personal data protection requirements on the vendors, b) make clear the job specifications, especially where they include security maintenance and software updates, and, last but not least, c) exercise reasonable oversight over the vendor responsible for the technical capabilities of the organisation so as to offer adequate protection to the types of personal data that may be affected by the engagement of the vendor. In cases where sub-contracting is contemplated, the Organisation should have identified requirements in its main contract that it requires its main IT vendor to impose similar obligations on and exercise adequate oversight over its sub-contractor.

9. In light of the above, the Organisation is found to have breached the Protection Obligation under section 24(a) of the PDPA.

10. In deciding the appropriate outcome in this case, the Commission considered the Organisation’s cooperation throughout the investigation, the Organisation’s voluntary admission of breach of the Protection Obligation, and the prompt remediation actions taken. This included disabling the use of its website on the same day of the Incident, reformatting of its webserver, adding security against SQL injections and the implementation of vulnerable assessment and penetration testing. We note that the Organisation managed to restore all the personal data affected without loss, thereby minimizing any disruptions to its operations.

11. Having considered the circumstances set out above and the factors listed at section 48J(6) of the PDPA, the Deputy Commissioner for Personal Data Protection hereby finds the Organisation in breach and directs the Organisation to pay a financial penalty of S$10,000 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.

12. In view of the remedial actions taken by the Organisation, no directions under section 48I are necessary.

[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/109384.xml&queryStr=(personal%20data%20protection%20act)#fnref1) See *Jigyasa* [2020] SGPDPC 9 and *Civil Service Club* [2020] SGPDPC 15

## Century Evergreen Private Limited

## [2023] SGPDPCS 5

| **Case Number** | : | DP-2212-C0526 |
| --- | --- | --- |
| **Decision Date** | : | 26 July 2023 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Century Evergreen Private Limited |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements* – *Failure to specify adequate data protection requirements in vendor’s contract*

1. On 11 December 2022, the Personal Data Protection Commission (the **“Commission”**) received a complaint against Century Evergreen Private Limited (the “**Organisation**”) that images of identification documents (which includes the National Registration Identity Card) submitted by jobseekers to the Organisation were publicly accessible on the Organisation’s website (“**Incident**”). The Organisation is a manpower contracting services company and required jobseekers to submit their identification documents to verify the identity of and suitability of the jobseeker in question.

2. Following the complaint received, the Commission commenced investigations to determine the Organisation’s compliance with the Personal Data Protection Act 2012 (“**PDPA**”). The Organisation requested that the investigation be handled under the Commission’s Expedited Decision Procedure (“**EDP**”). This means that the Organisation voluntarily provided and admitted to the facts set out in this decision. The Organisation also admitted that it failed to implement reasonable security arrangements to protect the personal data in its possession and control, and was in breach of section 24(a) of the PDPA.

3. The Organisation admitted that the Insecure Direct Object References (“**IDOR**”) vulnerability on its website, which allowed the complainant to manipulate the URL had existed from the time the website was launched on 9 November 2015. As a result of this vulnerability, 96,889 images of identification documents belonging to 23,940 individuals were downloaded from the Organisation’s website from 10 to 12 December 2022.

4. The Organisation admitted that it was in breach of section 24(a) of the PDPA as it failed to include any security requirements to protect personal data in its contract with the vendor who first developed and subsequently maintained the website. In this regard, even though the Organisation had engaged an IT vendor from the time the website was developed and launched, the Organisation remained solely responsible for protecting the personal data in its possession and control at all material times.

5. What is expected from organisations who engage professional services to build their websites and other online portals is explained in the Commission’s Guide on Building Websites for SMEs (revised 10 July 2018) (the “**Guide**”). The Commission had consistently advised organisations of the need to emphasise the protection of personal data to their IT vendors, by making it part of their contractual terms.[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/112353.xml&queryStr=(personal%20data%20protection%20act)#fn1) The contract should clearly state the responsibilities of the IT vendor with respect to the PDPA. In this regard, the Commission noted that there was a glaring omission of clauses to protect personal data in the Organisation’s contract with its IT vendor.

6. The Organisation also admitted that apart from conducting functionality testing when the website was first launched, the Organisation had no arrangements with its IT vendor to conduct any security tests prior to the launch of the website, or thereafter. The Organisation had also failed to impose any security requirements on the IT vendor to protect personal data, via contract.

7. In view of the above, the Deputy Commissioner found that the Organisation had contravened section 24(a) of the PDPA.

8. In deciding the appropriate outcome in this case, the Commission considered that a financial penalty ought to be imposed as the personal data affected included not just the identification numbers, but the images of the identification documents. Furthermore, there was a long period of non-compliance. The vulnerability was not addressed since 2015.

9. In deciding on the appropriate amount of financial penalty, the circumstances set out above and the factors listed at section 48J(6) of the PDPA were considered, specifically the impact of the personal data breach on the individuals affected and the nature of the Organisation’s non-compliance with the PDPA. In the circumstances, this was not an insignificant breach given the number of individuals affected (ie 23,940) and the nature of personal data exfiltrated: 96,889 images of identification documents.

10. The Organisation’s non-compliance with the PDPA was also not simply one of mere negligence but that of gross negligence. There was a long period of non-compliance on the facts of this case. As set out above, the Commission had issued the Guide to assist SMEs, and consistently cautioned the need for organisations to ensure compliance with the PDPA even when they engage an IT vendor in our previous decisions.[[note: 2]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/112353.xml&queryStr=(personal%20data%20protection%20act)#fn2)

11. In deciding on the appropriate amount of the financial penalty, the following factors were considered – the Organisation’s turnover and profitability, its cooperation throughout the investigation, its voluntary admission of breach of the Protection Obligation under the EDP, and the prompt remedial actions taken after the Organisation became aware of the IDOR vulnerability. This included rectifying the IDOR vulnerability, making server configuration changes to improve security, implementing vulnerability scans, migrating its backup server to an encrypted remote server, deploying additional security software and subscription to security services, and securing a new contract with its vendor to manage the security of its website. In addition to its prompt remedial actions, its poor performance in the most recent financial year was also taken into consideration. Finally, the organisation had admitted to its culpability at an early stage and elected to proceed under the EDP.

12. For the reasons above, the Deputy Commissioner for Personal Data Protection hereby finds the Organisation in breach and directs the Organisation to pay a financial penalty of S$9,000 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following section of the Personal Data Protection Act 2012 had been cited in the above summary:

**Protection of personal data**

**24.** An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.

[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/112353.xml&queryStr=(personal%20data%20protection%20act)#fnref1) See Guide on Building Websites for SMEs (revised 10 July 2018) at [4.2.1] and Re EU Holidays Pte Ltd [2019] SGPDPC 38.

[[note: 2]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/112353.xml&queryStr=(personal%20data%20protection%20act)#fnref2) Re EU Holidays Pte Ltd [2019] SGPDPC 38 and Re Vhive Pte Ltd (Case No. DP-2013-B8138).

## Kingsforce Management Services Pte Ltd

## [2023] SGPDPCS 1

| **Case Number** | : | DP-2202-B9480 |
| --- | --- | --- |
| **Decision Date** | : | 10 March 2023 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Kingsforce Management Services Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements* – *Failure to correctly scope and conduct reasonable periodic security review*

1. On 31 January 2022, the Personal Data Protection Commission (the **“Commission”**) was notified by Kingsforce Management Services Pte Ltd (the **“Organisation”**) of the sale on RaidForums, on or about 27 December 2021, of data from its jobseeker database (the “**Incident**”).

2. The affected database held approximately 54,900 jobseeker datasets, comprising name, address, email address, telephone number, date of birth, job qualifications, last and expected salary, highest qualification and other data related to job searches.

3. External cyber security investigators identified outdated website coding technology, with critical vulnerabilities, as the cause of the Incident.

4. The Commission accepted the Organisation’s request for handling under the Commission’s expedited breach decision procedure. The Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision, and to breach of section 24 of the Personal Data Protection Act (“the **PDPA**”).

5. The Organisation admitted work had not been completed on the website at launch owing to contractual disputes with the developer. The Organisation subsequently engaged IT maintenance vendors in an effort to ensure the security of the website. However, maintenance had been ad-hoc and limited to troubleshooting functionality issues from bugs, glitches and/or when a page failed to load.

6. In breach of the Protection Obligation, the Organisation failed to provide sufficient clarity and specifications to its vendors on how to protect its database and personal data. In *Re Civil Service Club*, the Commission had pointed out that organisations that engage IT vendors can provide clarity and emphasize the need for personal data protection to their IT vendors by a) making it part of their contractual terms, and b) reviewing the requirements specifications to ensure that personal data protection is reflected in the design of the end-product.[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/111511.xml&queryStr=(personal%20data%20protection%20act)#fn1) Further, post-execution of the contract, an organization is also expected to exercise reasonable oversight over its vendor during the course of the engagement to ensure that the vendor is protecting the personal data by adhering to the stipulated requirements.[[note: 2]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/111511.xml&queryStr=(personal%20data%20protection%20act)#fn2)

7. Another breach of the Protection Obligation by the Organisation was failure to conduct reasonable periodic security reviews, including vulnerability scans, since the launch of its website. The requirement for and scope of reasonable periodic security reviews had long been established in the published decisions of the Commission.[[note: 3]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/111511.xml&queryStr=(personal%20data%20protection%20act)#fn3) The PDPC’s Guide to Data Protection Practices for ICT Systems also emphasized the need to periodically conduct web application vulnerability scanning and assessments, post deployment, as a basic practice to ensure compliance with the Protection Obligation under the PDPA.[[note: 4]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/111511.xml&queryStr=(personal%20data%20protection%20act)#fn4)

8. The Organisation is therefore found to have breached the Protection Obligation under section 24(a) of the PDPA.

9. In deciding the enforcement action in this case, the Commission considered the Organisation’s efforts towards website security, cooperation throughout the investigation, voluntary admission of breach of the Protection Obligation and the prompt remediation taken. The last included immediate suspension of its website, and the engagement of a new developer to develop a new and enhance web application. The Commission also notes that the affected personal data was no longer or accessible following the shutdown of RaidForums. In the circumstances, the Commission directs the Organisation to do the following:

a. To submit to the Commission, within twenty-one (**21**) days from the date of issue of this Direction, a plan to ensure regular patching, updates and upgrades for all software and firmware supporting its website(s) and applications through which personal data in its possession may be accessed.

b. To state whether it intends to implement the plan by engagement of qualified external services or by relying on its own resources, and if by engagement of qualified external services, to state in detail the job specifications for software and firmware patching, updates, and upgrades to be stipulated to the vendor.

c. To outline each implementation step with deadlines to ensure that the entire implementation is completed within sixty (**60**) days from the date of issue of this Direction.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following is the provision of the Personal Data Protection Act 2012 cited in the above summary:

**Protection of personal data**

**24**. An organisation shall protect personal data in is possession or under its control by making reasonable security arrangements to prevent-

(a) unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.

[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/111511.xml&queryStr=(personal%20data%20protection%20act)#fnref1) Re *Civil Service Club* [2020] SGPDPC 15.

[[note: 2]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/111511.xml&queryStr=(personal%20data%20protection%20act)#fnref2) *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317 at [16] and [17].

[[note: 3]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/111511.xml&queryStr=(personal%20data%20protection%20act)#fnref3) See, *eg*, *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317; *Re Bud Cosmetics Pte Ltd* [2019] PDP Digest 351; and *Re Watami Food Service Singapore Pte Ltd* [2019] PDP Digest 221.

[[note: 4]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/111511.xml&queryStr=(personal%20data%20protection%20act)#fnref4) Pages 21 and 22 of the Guide to Data Protection Practices for ICT Systems.

## Ngian Wen Hao Dennis and others

## [2022] SGPDPCS 9

| **Case Number** | : | DP-2109-B8857 |
| --- | --- | --- |
| **Decision Date** | : | 08 March 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Ngian Wen Hao Dennis; Chan Puay Hwa Melissa; Winarto; Aviva Financial Advisers Pte Ltd |

*Data Protection* – *Consent obligation* – *Disclosure of personal data without consent*

*Data Protection* – *Notification obligation* – *Disclosure of personal data without notification of purpose*

1. On 7 September 2021, the Personal Data Protection Commission (the “**Commission**”) was notified of two incidents involving unauthorised disclosure and collection of personal data by three individuals.

2. Ngian Wen Hao Dennis (“**Dennis**”) was an Aviva Financial Advisers Pte Ltd (“**AFA**”) representative between December 2017 and February 2019. In March 2019 and August 2020, Dennis approached two insurance financial advisers, Chua Puay Hwa Melissa (“**Melissa**”) and Winarto, to offer them a list of client leads, stating that he was leaving the insurance industry and looking for a reliable agent to take over his clientele. Melissa and Winarto each said they paid $1,000 to Dennis for the list (the “**Incidents**”).

3. The list contained approximately 1,000 clients’ names, mailing addresses, contact numbers and the names of organisations underwriting the hospitalisation plans bought by the clients (“**Personal Data Sets**”).

4. The PDPA defines “organisations” to include individuals. As held in *Re Sharon Assya Qadriyah Tang*[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/109232.xml&queryStr=(personal%20data%20protection%20act)#fn1), individuals who collect, use or disclose personal data otherwise than in a personal or domestic capacity will be treated as organisations within the meaning of the Act, and are obliged to comply with the Data Protection Provisions. In this case, we are of the view that it is clear that Dennis, Melissa and Winarto can be regarded as an “organisation” as defined under the PDPA for a number of reasons. First, the trio had bought and sold the client leads for work and business purposes, with the aim of generating an income or profit, and cannot be said to have been acting in a personal or domestic capacity.

5. Second, Dennis, Melissa and Winarto were not employees. In *Re Ang Rui Song*[[note: 2]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/109232.xml&queryStr=(personal%20data%20protection%20act)#fn2)*,* the Commission found that the respondent, a financial consultant with Prudential Assurance Company (Pte) Ltd, had been engaged on such terms that he was in effect an independent contractor rather than an employee of Prudential. The same applies to the trio. The Representative Agreement between AFA and Dennis expressly provides that “nothing in [the] Agreement shall constitute, or be construed, or deemed to constitute, any employment…between [Dennis] and [AFA]”.

*Dennis*

6. Having found that the PDPA applies, we now turn to consider the data protection obligations applicable to the different parties concerned. Dennis conceded that he approached Melissa and Winarto to transfer his list of client leads to them. Our investigations revealed that Dennis’ claim that he had obtained the necessary consent and duly notified the clients on the list regarding the disclosure of their personal data to other insurance financial advisers could not be corroborated. None of the clients verified Dennis’ claim that he had contacted them to seek their consent or notified them of the disclosure of their personal data to other insurance financial advisers. We are therefore of the view that Dennis has breached the Consent and Notification Obligation under the PDPA in that he did not obtain his clients’ consent before disclosure of their personal data.

*Melissa and Winarto*

7. Both Melissa and Winarto admitted to the collection (purchase) of the client list from Dennis. They claimed to have relied on the verbal assurances provided by Dennis that he had informed the clients about the change in their insurance financial adviser. In *Re Amicus Solutions Pte Ltd and Ivan Chua Lye Kiat* [2019] SGPDPC 33(at [49]), we stated that a reasonable person should undertake proper due diligence, such as obtaining from the seller a sample of the written notifications and consent. In our view, Melissa and Winarto have failed to take reasonable steps to verify from Dennis that there had been proper notification to and consent obtained from the clients for the disclosure of their personal data. In collecting (i.e. buying) the client list, we find that Melissa and Winarto are in breach of the Notification and Consent Obligations under the PDPA.

*AFA*

8. The Commission found no evidence of breach of the PDPA by AFA in the Incidents. As stated in [5], Dennis was not an employee of AFA for whose acts AFA may be liable through section 53(1) of the PDPA. Dennis claimed that the Personal Data Sets were not retrieved from AFA’s systems and that he had compiled the list on his own accord to keep track of his clientele during his time as an independent financial adviser with AFA. This was consistent with AFA’s own investigations. Our investigations also revealed that AFA had reasonable policies and security measures in place for personal data protection. These included data leak prevention controls and monitoring of AFA corporate network to prevent representatives from exporting clients’ data from its systems. Contractual terms were also in place to require representatives to comply with the PDPA. AFA issued a letter to Dennis, upon the termination of the relationship between them, referring to the need to return “all policies, rate books, receipts, manuals, literature, lists and personal information of Customers”.

**The Commission’s Decision**

9. The sale of personal data by organisations without obtaining the consent of the individuals involved is a serious breach of the PDPA. In *Re Sharon Assya Qadriyah Tang* at [30], we had stated as follows:

**There are strong policy reasons for taking a hard stance against the unauthorised sale of personal data**. Amongst these policy reasons are **the need to protect the interests of the individual and safeguard against any harm to the individual, such as identity theft or nuisance calls**. Additionally, there is a need to **prevent abuse by organisations in profiting from the sale of the individual’s personal data at the individual’s expense**. It is indeed such cases of potential misuse or abuse by organisations of the individual’s personal data which the PDPA seeks to safeguard against. In this regard, the Commissioner is prepared to take such stern action against organisations for the unauthorised sale of personal data.

[Emphasis added.]

10. To curb this form of abuse of personal data, the amount of profit made by the organisation from the sale may be factored in determining the financial penalty that the organisation may be required to pay. Indeed, had the sale taken place after the 2020 amendments to the PDPA, this would have been a specific consideration under section 48J(6)(c): “whether the organisation or person (as the case may be), as a result of the non‑compliance, gained any financial benefit”.

11. In determining the enforcement action in response to the breach by Dennis, the Commission took into account the cooperation extended to the investigation, and the full refund made by Dennis of the proceeds he made from the sale. The Commission also considered that Dennis is in poor health, has been unemployed since 2018, has little savings in his bank account, and is dependent on his aged father for financial support. Having considered the state of Dennis’ health and financial status, the Commission is of the view that a financial penalty would impose a crushing burden on him and his family, resulting in undue hardship. Accordingly, taking into account all relevant factors, the Commission has decided to administer a warning in respect of the breach by Dennis of the Consent and Notification Obligations. The Commission wishes to emphasize that this assessment that undue hardship may occur following the imposition of a financial penalty is not a finding that the Commission will make easily and will be reserved only for the most deserving and exceptional cases. Individuals who seek to misuse personal data for profit and are found to be in breach of the PDPA must expect to pay a heavy financial penalty.

12. Turning to Melissa and Winarto, the Commission has decided to administer warnings to Melissa and Winarto in respect of their breaches of the Consent and Notification Obligations. In so deciding, the Commission considered that both of them did not sell the personal data for profit and had been cooperative throughout the investigations. More importantly, neither of them used the personal data they obtained without consent from the individuals involved.

[[note: 1]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/109232.xml&queryStr=(personal%20data%20protection%20act)#fnref1) [2018] SGPDPC 1

[[note: 2]](https://www-lawnet-sg.libproxy.smu.edu.sg/lawnet/group/lawnet/page-content?p_p_id=legalresearchpagecontent_WAR_lawnet3legalresearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_legalresearchpagecontent_WAR_lawnet3legalresearchportlet_action=openContentPage&contentDocID=/Decision/109232.xml&queryStr=(personal%20data%20protection%20act)#fnref2) [2017] SGPDPC 13.

## Cognita Asia Holdings Pte Ltd

## [2022] SGPDPCS 14

| **Case Number** | : | DP-2106-B8484 |
| --- | --- | --- |
| **Decision Date** | : | 09 June 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Cognita Asia Holdings Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access of personal data* – *Unauthorised modification of personal data* – *Insufficient security arrangements* – *Failure to implement reasonable access controls* – *Failure to conduct staff training*

1. On 16 June 2021, Cognita Asia Holdings Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the “**Commission**”) of a ransomware attack on 13 June 2021. The ransomware incident (the "**Incident**") affected the servers of three schools run by the Organisation.

2. The ransomware encrypted the personal data of 1,260 individuals, of which 1,195 are students. The personal data included copies of identification/passport page, salaries of the affected employees and the bank account details necessary for the crediting of salaries.

3. The Organisation’s internal investigations found that the threat actor gained initial entry to one of the school's network in April 2021 through a VPN session. The VPN logs showed no brute-force entry attempts, suggesting the use of compromised administrator account credentials. Investigations disclosed that between 8 and 12 June 2021, the threat actor gained broad network access and deployed the encrypting ransomware.

4. The Organisation requested that this matter proceed via the Expedited Decision Breach Procedure, which the Commission acceded to. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision. It also admitted to a breach of section 24 of the Personal Data Protection Act (the "**PDPA**"), also referred to as the Protection Obligation.

5. At the time of the Incident, even though the Organisation employed VPN, the Organisation’s existing configuration of VPN required merely a username and password for authentication. However, the personal data collected and processed by the Organisation included copies of the photographic identification documents of students as well as salary and bank account information of employees. In view of the nature of personal data that it holds, the Organisation needed a higher level of security and stronger access control for its administrator accounts, such as multi-factor authentication for VPN connection to its administrator accounts to protect such personal data.

6. The Organisation also failed to have reasonable password policies or ensure compliance with their existing password policies. The Organisation did not enforce their password policies in the following areas:

(i) Although the Organisation's password policy specified a minimum requirement of 10 characters, in practice the requirement that was enforced by their IT systems was only 8 characters; and

(ii) Its password policy of requiring the default password to be changed after the first usage was not enforced.

7. The Commission's Handbook on "*How to Guard Against Common Types of Data Breaches*", which is complemented by the "*Checklists to Guard Against Common Type of Data Breaches*", has identified poor management of accounts and passwords as one of the five common causes and types of data breaches. Organisations must adopt, implement, and enforce a strong password policy as a necessary measure of data protection.

8. Finally, the Organisation also failed to ensure that personal data protection training was conducted for its staff. In this regard, the Commission wishes to reiterate that staff training in personal data protection is an important and necessary component of the Protection Obligation of an organisation.

9. In light of the above, the Organisation is found to have breached section 24 of the PDPA.

10. The Commission acknowledged that, the Organisation informed the relevant stakeholders of the Incident and implemented real time threat monitoring and Deep and Dark Web monitoring for potentially exposed personal data.

11. The Organisation also undertook remedial actions to mitigate the effects of the Incident and improve the robustness of its security measures. This included the engagement of a cybersecurity expert to investigate the cause of the Incident and working together with the said expert to enact a Remediation Plan.

12. The Remediation Plan included measures such as, enforcing multi-factor authentication of all staff accounts, enhancing the password requirements for administrator accounts, and increasing the frequency of security reviews and cyber security trainings for its staff.

13. The Organisation also conducted security awareness webinars and offered a 12 months’ personal identity monitoring services to all the staff and parents (who can sign up on behalf of the affected students) of these three schools.

14. The Commission’s decision to require payment of a financial penalty, and on the quantum of the penalty, took into account sections 48J(1) and 48J(6) of the PDPA, and all the relevant circumstances of the case. This included the Organisation's admission of breach of the Protection Obligation, which the Commission considers is a significant mitigating factor. Having considered all the facts of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of S$26,000.

15. The Organisation must make payment of the financial penalty 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.

16. In view of the remedial actions taken by the Organisation, the Commission will not issue any directions under section 48I of the PDPA.

## Vimalakirti Buddhist Centre

## [2020] SGPDPCS 18

| **Case Number** | : | Case No. DP-2004-B6193 |
| --- | --- | --- |
| **Decision Date** | : | 04 September 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Vimalakirti Buddhist Centre |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Insufficient security arrangements*

1. On 14 April 2020, Vimalakirti Buddhist Centre (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) of a ransomware infection that had rendered its data management system inaccessible by the Organisation (the “**Incident**”).

2. The Organisation subsequently requested for this matter to be handled under the Commission’s expedited breach decision procedure. In this regard, the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. It also admitted that it was in breach of section 24 of the Personal Dara Protection Act (the “**PDPA**”).

3. The Incident occurred on or about 31 March 2020. Personal data of approximately 4,500 members and 4,000 non-members (total 8,500 individuals) were encrypted by the ransomware. The personal data encrypted included the name, address, contact number, NRIC number, date of birth and donation details of the individuals.

4. The Organisation admitted it did not give due attention to personal data protection, and had neglected to implement both procedural and technical security arrangements to protect the personal data in its possession and control. Consequently, it did not have the relevant security software and/or protocols in place to prevent the ransomware from entering its data management system.

5. In the circumstances, the Deputy Commissioner for Personal Data Protection finds the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”).

6. Following the incident, the Organisation set up a new server with backup from 21 October 2019. For the data collected by the Organisation from 22 October 2019 to the Incident, the Organisation had retrieved the data from physical file records and restored them in the new server. It also installed a firewall to filter network traffic to and from the new server, and cleaned, restored and reinstalled all computers connected to its data management system. Additionally, the Organisation committed to engage consultants to help produce a data protection manual and train its staff in cyber hygiene and incident response.

7. The Deputy Commissioner for Personal Data Protection notes that the Organisation had admitted to a breach of Protection Obligation under the PDPA, cooperated with the Commission’s investigation and taken prompt remedial action. There was no evidence that the personal data affected in the Incident had been misused in any form. In addition, the Organisation had a backup copy of the encrypted data and did not lose any data as a result of the Incident. Accordingly, the practice of having data backup(s) should be encouraged to prevent organisations from losing data in the event of ransomware.

8. On account of the above, the Deputy Commissioner for Personal Data Protection directs the Organisation to pay a financial penalty of $5,000 within 30 days from the date of this direction (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).

9. In view of the remedial actions taken by the Organisation, the Commission will not be issuing any other directions.

## Seriously Keto Pte. Ltd.

## [2021] SGPDPCS 8

| **Case Number** | : | Case No. DP-2006-B6449 |
| --- | --- | --- |
| **Decision Date** | : | 14 July 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Seriously Keto Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Insufficient security arrangements*

1. On 16 June 2020, Seriously Keto Pte Ltd (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) of a ransomware infection that occurred on or about 15 June 2020 (the “**Incident**”). The affected personal data comprised approximately 3,073 individuals’ names, addresses, email addresses and telephone numbers (“**the Affected Personal Data**”).

2. The Organisation requested that the Commission investigate the Incident under its Expedited Decision Procedure. In this regard, the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. It also admitted that it was in breach of the Protection Obligation under section 24 of the Personal Data Protection Act (the “**PDPA**”).

3. Investigations revealed the presence of an unprotected file in the Organisation’s network infrastructure which contained unencrypted login credentials to access the server containing the Affected Personal Data. The unprotected file could be located by infrastructure scanning, and this provided a channel for unauthorised access to the server. Server logs retrieved by the Organisation after the Incident indicated that there had been unauthorised access to the file.

4. The Organisation admitted that it had failed to conduct any periodic security reviews prior to the Incident which could have revealed the existence of the unprotected file within its network infrastructure.

5. The Organisation had engaged a vendor to develop its e-commerce and membership website and claimed to have relied on the vendor to make the necessary security arrangements to protect the Affected Personal Data. However, in this case, there were no clear business requirements (e.g. contractual stipulations) specifying that the Organisation was relying on the vendor to recommend and/or implement security arrangements to protect personal data hosted in the e-commerce and membership website that the vendor was engaged to develop. Protection of personal data in the possession or under the control lies primarily with the Organisation, although it may contract the operations to a vendor who is more knowledgeable and with expertise. To do so, the Organisation has to be clear about the scope of outsourcing and the vendor has to also agree to do so. In the absence of clear outsourcing, the responsibility to implement reasonable security arrangements to protect the Affected Personal Data remained squarely with the Organisation.

6. Overall, the Organisation admitted that it had failed to give due attention to personal data protection prior to the Incident and had neglected to implement reasonable security arrangements to protect the Affected Personal Data.

7. In the above circumstances, the Deputy Commissioner for Personal Data Protection finds that the Organisation negligently contravened the Protection Obligation under section 24 of the PDPA.

8. Following the Incident, the Organisation underwent a full security audit and remedied vulnerabilities identified. The Organisation also set up a new website with a more robust internal security infrastructure, implemented a mandatory password change for all users of its new website, and activated a firewall to safeguard access to the new website. It also engaged a cybersecurity vendor to develop further measures and policies to strengthen its internal IT infrastructure. Additionally, the Organisation committed to engaging consultants to improve its data protection policies and outsource data protection functions.

9. The Organisation cooperated with the Commission’s investigation, admitted to its breach of the Protection Obligation, and took prompt remedial action. There was no evidence of exfiltration of the Affected Personal Data, and the Organisation was able to restore the Affected Personal Data from a backup and did not lose any data as a result of the Incident. The practice of having regular and separately located data backup(s) is to be encouraged to prevent organisations from losing data to ransomware.

10. Having considered the above circumstances and the factors listed at section 48J(6) of the PDPA, the Deputy Commissioner for Personal Data Protection requires the Organisation to pay a financial penalty of $8,000 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.

11. In view of the remedial actions taken by the Organisation, no other directions are necessary.

## Giordano Originals (s) Pte Ltd

## [2021] SGPDPCS 13

| **Case Number** | : | Case No. DP-2011-B7387 |
| --- | --- | --- |
| **Decision Date** | : | 15 October 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Giordano Originals (s) Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *No breach* – *Reasonable security arrangements implemented*

1. On 3 December 2020, the Personal Data Protection Commission (the “**Commission**”) was notified by Giordano Originals (S) Pte Ltd (the “**Organisation**”) of an unauthorized network entry and ransomware infection at the OS and server level that occurred on or about 12 July 2020 (the “**Incident**”).

2. As a result of the Incident, two of the Organisation’s systems, one which stores the personal data of its employees and second, the personal data of its members were affected.

3. The Organisation’s own and independent investigation conducted found no sign of suspicious activity in the Singapore network, and no impact beyond the Singapore network. The unauthorised entry had most likely occurred through the use of compromised credentials obtained through phishing.

4. Personal data of 790,000 members and 184 employees in encrypted form were affected. The personal data of members comprised names (20% of the members), contact number and partial date of birth (without birth year). The personal data of employees comprised name, NRIC, address, gender, age, contact number, email address, educational and salary information.

5. Investigations revealed that the Organisation had in place reasonable security measures that are consistent with the recommendations that the Personal Data Protection Commission had made in our recent Handbook on “How to Guard Against Common Types of Data Breaches” on how to prevent malware or phishing attacks. The Organisation had installed and deployed various endpoint security solutions, which was complemented with real-time system monitoring for any Internet traffic abnormalities. Even before the Incident, the Organisation also conducted regular periodic system maintenance, reviews and updates (such as vulnerability scanning and patching).

6. More importantly, the Organisation had also ensured that its data was regularly and automatically backed-up, which was a key recommendation that the Commission made in our Handbook.

7. In addition, the Organisation had also taken steps to better protect the personal data affected by encrypting the personal data using current industry-standard RSA algorithm and passphrase. As a result, the personal data affected by the ransomware was not legible without decryption.

8. The Commission endorses the proper use of industry-standard encryption to protect personal data, and will give due weight to Organisations which have implemented the recommendations we made in our Handbook in determining whether an organisation has complied with its Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”), or as a strong mitigation factor in the event of the Commission finds that there has been a breach of section 24 of the PDPA.

9. Following the Incident, the Organisation took prompt and extensive remedial both to mitigate the effects of the Incident and enhance the robustness of its security measures. This included increased frequency of staff phishing simulation trainings and security reviews as well as additional monitoring measures. There was no evidence of exfiltration of the personal data or decryption of the personal data. The Organisation was also able to fully restore the personal data from its backups.

10. In light of the reasons discussed above, the Deputy Commissioner for Personal Data Protection is satisfied that the Organisation had met its Protection Obligation under section 24 of the PDPA. In light of our findings, we will not be issuing any directions or taking any further enforcement action against the Organisation in relation to the Incident.

## Flying Cape Pte Ltd and another

## [2021] SGPDPCS 4

| **Case Number** | : | Case No. DP-2011-B7385 |
| --- | --- | --- |
| **Decision Date** | : | 17 March 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Flying Cape Pte Ltd; ACCA Singapore Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements*

1. Sometime between 25 September 2020 to 5 October 2020, the personal data of 191 users (the “**Affected Individuals**”) of [www.accapdhub.com](https://www.accapdhub.com/) (the “**Website**”) was exfiltrated by an unauthorised party (the “**Incident**”).The exfiltrated personal data comprised of the names, email addresses and contact numbers of the Affected Individuals (“**the Exfiltrated Data**”).

2. The Website was owned by ACCA Singapore Pte Ltd (“**ACCA**”), but hosted, managed, and operated by Flying Cape Pte Ltd (“**FCPL**”) as ACCA’s data intermediary. FCPL notified the Personal Data Protection Commission (the “**Commission**”) of the Incident on 12 November 2020, after having received a ransom demand in respect of the Exfiltrated Data.

3. Sometime in early September 2020, as part of its management of the Website, FCPL extracted the personal data of the Affected Individuals from the database of the Website into an excel file. An FCPL employee who was assigned to work with the excel file failed to protect the file with a password or encrypt it as required by FCPL’s IT policy. Moreover, the employee incorrectly stored the excel file in a publicly accessible online storage bucket, as opposed to the correct, secured storage bucket. These lapses were believed to have led to the Incident.

4. Pursuant to section 53(1) of the PDPA, FCPL is liable for acts done by employees. The question therefore becomes whether FCPL had taken reasonable steps to prevent or detect mistakes such as the one made by the employee. The investigations did not surface any arrangements to supervise or verify its employees’ compliance with its internal policies or detect non-compliance. The Deputy Commissioner for Personal Data Protection therefore found that FCPL had breached the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”) in respect of the Exfiltrated Data.

5. As the data controller and owner of the Website, ACCA owed the Protection Obligation in respect of the Exfiltrated Data as well. The Deputy Commissioner is satisfied that ACCA discharged this obligation by (i) carrying out a due diligence assessment of FCPL’s data protection policies and practices before their engagement, and (ii) by stipulating data protection requirements in its contract when engaging with FCPL.

6. Taking into account the circumstances of the case, and in particular the factors below, the Deputy Commissioner for Personal Data Protection found ACCA not in breach of the PDPA and decided to issue a Warning to FCPL:

a. The number of the Affected Individuals was low;

b. The Exfiltrated Data was of a low sensitivity;

c. FCPL took immediate remedial actions to prevent the occurrence of a similar incident; and

d. FCPL voluntary notified the Commission of the Incident.

7. In view of the remedial actions taken by FCPL, no directions were issued.

## Security Masters Pte Ltd

## [2020] SGPDPCS 12

| **Case Number** | : | Case No. DP-2002- B5875 |
| --- | --- | --- |
| **Decision Date** | : | 21 July 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Security Masters Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Insufficient security arrangements*

1. On 17 February 2020, Security Masters Pte Ltd (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) that a security employee had used the mobile phone numbers of eight building visitors to contact them to request their return of visitor passes and send them Chinese New Year greetings.

2. Investigation found that the Organisation did not put in place any standard operating procedure or guidelines for the retrieval and use of visitors’ personal data prior to the incident. This gap in security arrangements allowed the incident to occur.

3. The Deputy Commissioner for Personal Data Protection therefore found that the Organisation did not adopt reasonable steps to protect personal data in its possession or under its control against risk of unauthorised access. The Organisation was in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012.

4. Following the incident, the Organisation restricted access to personal data to senior personnel and required all security personnel to sign an undertaking not to contact visitors in their personal capacity. However, structured training is needed to help its security personnel understand the importance of protecting the personal data they handled daily in their duties, such as National Registration Identification Card numbers, photographs and closed-circuit television footage.

5. On the above consideration, the Deputy Commissioner for Personal Data Protection hereby directs the Organisation to:

(a) Within 60 days from the date of the direction, revise its training curriculum to ensure that its security personnel understand

i. the rationale for personal data protection;

ii. the importance of consent and authorisation in the handling of personal data; and

iii. the circumstances in which it would be appropriate to use and disclose personal data on social media platforms for work-related purposes; and

(b) Inform the Commission within 1 week of implementation of the above.

## Singapore Accountancy Commission

## [2020] SGPDPCS 10

| **Case Number** | : | Case No. DP-1911-B5296 |
| --- | --- | --- |
| **Decision Date** | : | 22 June 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Singapore Accountancy Commission |

*Data Protection* – *Protection obligation* – *Unauthorised access to and disclosure of personal data* – *Insufficient security arrangements*

1. On 18 November 2019, Singapore Accountancy Commission (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) that a folder containing personal data of 6,541 Singapore Chartered Accountant Qualification programme personnel and candidates was mistakenly enclosed in emails sent to 41 unintended recipients between 12 June 2019 and 22 October 2019. The folder comprised information such as names, National Registration Identification Card numbers, dates of birth, contact details, education and employment information and Singapore Chartered Accountant Qualification examination results. Following the incident, 41 unintended recipients confirmed deletion of the email and folder they each received.

2. The Organisation admitted to a lack of robust processes to protect personal data when sending emails. The staff involved in the sending of the emails were not informed of the Organisation’s personal data policies as part of their induction training. The Organisation’s data protection policies and procedures were not translated into security arrangements for protection of personal data. There were, for example, no second-tier or supervisory checks or technical measures to reduce the risk of sending content with personal data to unintended parties at the time of the incident.

3. Following the incident, the Organisation undertook remediation. This included training sessions on cybersecurity and personal data protection for all employees and revision of policies and procedures on handling of personal data.

4. In the circumstances, the Deputy Commissioner for Personal Data Protection found that the Organisation did not adopt reasonable steps to protect personal data in its possession or under its control against unauthorised access. The Organisation was in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”).

5. The Organisation had made an admission of breach of the Protection Obligation under the PDPA, cooperated with the Commission’s investigation and taken prompt remedial actions.

6. On account of the above, the Organisation is directed to pay a financial penalty of $5,000 within 30 days from the date of this direction, 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. In view of the remedial actions taken by the Organisation, the Commission will not issue any other directions.

## Specialized Asia Pacific Pte Ltd

## [2021] SGPDPCS 10

| **Case Number** | : | Case No. DP-2101-B7826 |
| --- | --- | --- |
| **Decision Date** | : | 30 July 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Specialized Asia Pacific Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Insufficient technical security arrangements*

1. On 29 January 2021, Specialized Asia Pacific Pte Ltd. (the “**Organisation**”) informed the Personal Data Protection Commission of a data security incident involving the Specialized Cadence application (the “**Application**”) that it developed, operated and maintained.

2. The Organisation’s developing staff did not realize that the online development tool, which was used to develop the Application, had a default privacy setting that made all data created by users or developers “visible”, even though this had been stated in the tool’s privacy rules. This default setting allowed the Application’s network traffic to be intercepted and accessed using third-party security testing software that can be acquired online. A member of the public had therefore been able to intercept and access the personal data of the Application’s users by using a free version of such software (the “**Incident**”). However, the risk of unauthorised access had been limited to parties who knew how to use such security testing software to obtain access. This factored in the enforcement outcome below (see paragraph 6 below).

3. The undetected default privacy setting of “visible” put the personal data of 2,445 individuals at risk of unauthorised access. The data affected included names, addresses, dates of birth, telephone numbers, email addresses and gender.

4. Remediation by the Organisation encompassed turning off all access and use of the Application by all external parties, including users, and changing the privacy setting from “visible” to “hidden”. The Organisation also engaged a third-party IT security firm to test and address any security and privacy issues relating to the Application, commenced discussions with its IT application designers and employees involved to adopt ‘privacy-by-design’ in future applications development.

5. The Protection Obligation in section 24 of the Personal Data Protection Act 2012 requires that organisations understand the privacy policies and security features of all online tools or software they choose to employ. This was established in published cases such as *Re GMM Technoworld Pte. Ltd.* [2016] SGDPDPC 18. Organisations employing online tools or other online software must set or reconfigure privacy policies and security features to protect the personal data of application or website users. It would not be a discharge of the Protection Obligation for an organisation to simply adopt, vis-à-vis users, the same default privacy policies of online tools or software that do not protect the personal data of users.

6. The Deputy Commissioner for Personal Data Protection therefore found the Organisation in breach of the Protection Obligation under Section 24 of the Personal Data Protection Act 2012. Upon consideration of the facts, including the limited exposure of the affected data to those who knew how to use the above-mentioned third party software to access such information via the default privacy setting, and the Organisation’s commitment to improve its processes, a Warning was issued to the Organisation.

## Honestbee Pte Ltd

## [2019] SGPDPCS 8

| **Case Number** | : | Case No. DP-1905-B3827 |
| --- | --- | --- |
| **Decision Date** | : | 21 November 2019 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Honestbee Pte Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised access to personal data* – *Lack of access control*

1. Honestbee Pte Ltd (the “**Organisation**”) is an online food and grocery delivery service. Third party merchants, which either engaged or were planning to engage the Organisation for delivery services, provided it with personal data of their customers in order to test its logistics service delivery platform. The Organisation stored this personal data in its Amazon Web Services (“**AWS**”) file repository. The personal data (the “**Personal Data**”) included names, email addresses, residential addresses and mobile numbers.

2. The Personal Data Protection Commission (the “**Commission**”) was informed on 2 May 2019 that the Personal Data was accessible to the public. The number of individuals whose personal data was accessible was about 8,000. The Organisation admitted that it had mistakenly placed the Personal Data in a ‘bucket’ (which is similar to a file folder) without access restrictions. This allowed anyone with knowledge of AWS’s command line to gain access to the Personal Data.

3. The Commission found that the Organisation omitted to put in place the most rudimentary security measures necessary to protect the Personal Data. For example, the Organisation could have implemented a requirement to conduct checks to confirm that any personal data used in testing was stored in a ‘bucket’ with the appropriate access restrictions. In the circumstances, the Organisation had not implemented reasonable security arrangements to protect the Personal Data and is therefore in breach of section 24 of the Personal Data Protection Act 2012.

4. The Organisation has since blocked public access to the Personal Data by modifying the relevant access settings and circulated a report to its engineering team to ensure that similar mistakes would not be repeated in code reviews. The Organisation is also in discussions with cybersecurity companies to perform regular security audits on its systems.

5. The Organisation is directed to pay a financial penalty of $8,000 within 30 days from the date of this direction, 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 the financial penalty until the financial penalty is paid in full. In view of the remedial measures taken by the Organisation, the Commission has not imposed any other directions.

6. The Organisation’s prompt co-operation in the course of the Commission’s investigation, its prompt actions taken to remediate the breach and the limited unauthorized disclosure of the Personal Data were mitigating factors taken into consideration in determining the quantum of the financial penalty.

## Water + Plants Lab Pte. Ltd.

## [2020] SGPDPCS 22

| **Case Number** | : | Case No. DP-2004-B6182 |
| --- | --- | --- |
| **Decision Date** | : | 18 November 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Water + Plants Lab Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised modification or access to personal data* – *Insufficient security arrangements*

1. On 9 April 2020, Water + Plants Lab Pte. Ltd. (the “**Organisation**”) informed the Personal Data Protection Commission of a ransomware infection that rendered the Organisation’s server (the “**Server**”) inaccessible to the Organisation (the “**Incident**”).

2. The Incident occurred on or around 30 March 2020. Personal data of 28 employees were encrypted by the ransomware. The personal data affected included the employees’ name, NRIC/FIN/Work Permit number, address, date of birth, mobile number and photograph.

3. Investigations revealed that an employee from the Organisation had downloaded and opened an email attachment that contained ransomware. At the time of the Incident, the Organisation had some security measures in place, for example, it had anti-virus protection, and access rights and password control for the Server. It also had a good practice of performing regular backup of its Server, and most of the data was successfully restored from an external backup. The Organisation therefore suffered minimal data loss as a result of the Incident.

4. However, as admitted by the Organisation, it had not carried out any patching and security scanning of the Server in the 12 months preceding the Incident. Patching and regular security scanning are important security measures to prevent vulnerabilities in an organisation’s ICT systems which a hacker may exploit in compromising personal data. For this reason, the Deputy Commissioner for Personal Data Protection found that the Organisation had failed to protect the personal data in its possession or under its control, in breach of section 24 of the Personal Data Protection Act 2012.

5. Following the Incident, the Organisation installed a firewall with greater capabilities to protect the Organisation against external threats, for example, possessing deeper content inspection capabilities to identify malware. The Organisation had also conducted staff training on personal data protection and on how to identify security threats.

6. Upon consideration of the facts, including the impact from the breach, the remediation action taken by the Organisation and that there was no evidence of exfiltration of the data in the Server, the Deputy Commissioner issued a warning to the Organisation.

## Sembcorp Marine Ltd

## [2023] SGPDPCS 2

| **Case Number** | : | DP-2206-B9934 |
| --- | --- | --- |
| **Decision Date** | : | 07 February 2023 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Sembcorp Marine Ltd |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *No breach* – *Reasonable security arrangements implemented*

1. On 25 July 2022, Sembcorp Marine Ltd (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) of a personal data breach that had occurred through the exploitation of the Log4J zero-day vulnerability (the “**Incident**”).

2. As a result of the Incident, the personal data of 25,925 individuals was exfiltrated. The personal data affected included their name, address, email address, NRIC number, telephone number, passport number, photograph, date of birth, bank account details, salary, and medical screening results.

3. The Organisation engaged an external cybersecurity company, Sygnia, to investigate the Incident. Its investigations found that the threat actor had exploited three Log4J vulnerabilities present in an application (the “**Application**”) to gain unauthorised access to a server as early as on 4 January 2022. The threat actor also deployed the “Cobalt Strike” beacon, conducted reconnaissance, and made lateral movements across several machines, before exfiltrating data between 10 and 23 June 2022, and deploying a ransomware on 28 June 2022.

4. Threat intelligence research revealed that the ransomware campaign which affected the Organisation began targeting users of the Application in January 2022. Given that reports of the Log4J vulnerability were first made in December 2021, it would have been difficult for the Organisation to detect and prevent the infiltration when it was one of the early targets, having been infiltrated as early as 4 January 2022.

5. After finding out about the Log4J vulnerability, the Organisation took prompt actions to identify instances of Log4J vulnerabilities across all the software application it was using. The Organisation started identifying instances of Log4J vulnerabilities across its systems on 14 December 2021. It applied the security patches immediately when they were made available by the respective software vendors. The Organisation also implemented workarounds recommended by the vendors, for systems which patches were not available or had not been released. Additional measures such as blocking incoming and outgoing Log4J traffic were also taken.

6. We are satisfied that the Organisation had made reasonable security arrangements to protect personal data in its possession and/or control in relation to the Incident. The Organisation had in fact adopted good practices in relation to its Information and Communications Technology (ICT) systems. This included a cybersecurity testing programme, regular vulnerability assessment and penetration testing, and cyber security monitoring.

7. In view of the above, the Deputy Commissioner for Personal Data Protection is satisfied that the Organisation had met its Protection Obligation under section 24 of the PDPA. No enforcement action therefore needs to be taken in relation to the Incident.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following provision(s) of the Personal Data Protection Act 2012 had been cited in the above summary:

**Protection of personal data**

**24.** An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.

## St. Joseph’s Institution International Ltd.

## [2021] SGPDPCS 2

| **Case Number** | : | Case No. DP-2010-B7196 |
| --- | --- | --- |
| **Decision Date** | : | 12 March 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | St. Joseph’s Institution International Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *Insufficient security arrangements*

1. On 16 October 2020, St Joseph’s Institution International Ltd. (the “**Organisation**”) informed the Personal Data Protection Commission that a file listing the personal data of 3155 parents and students (“**the File**”) was found on a website called VirusTotal (the “**Incident**”).

2. The Incident occurred on or around 13 October 2020 when a staff of the Organisation downloaded and deployed a Google Chrome browser extension developed by VirusTotal for additional security scanning. Unknown to the staff, apart from security scanning, the extension also forwarded scanned samples to premium members of VirusTotal (the “**3rd Parties**”) for security analysis and research. This use of samples was made known in VirusTotal’s privacy policy covering the use of the extension.

3. As a result of the Incident, the personal data of 3155 individuals including both parents and students were put at risk of unauthorised access. The personal data affected included the names of parents and students, parents’ email addresses, students’ date of birth, students’ classes, students’ year and grades.

4. Users of the VirusTotal Chrome extension would have to agree to VirusTotal’s Privacy Policy, which provides that once files are uploaded to the VirusTotal website for scanning, copies of these files will be kept by VirusTotal and shared with their subscribers for research purposes. The risk of such file sharing and in turn disclosure of personal data to 3rd Parties ought to have been known to the said staff of the Organisation, but was overlooked due to oversight. Such oversight could have been prevented if the Organisation had sufficiently robust processes for assessing such risks prior to deploying downloaded software, including Chrome Extensions. However, the Organisation lacked such processes.

5. Nevertheless, the Organisation took prompt action to mitigate the effects of the breach by contacting VirusTotal immediately to remove the File and notified all affected individuals. While personal data was disclosed, it was limited to premium members of VirusTotal for research purposes only.

6. On the facts, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012. However, in consideration of the limited risk of personal data being disclosed, and the Organisation’s commitment to improve its processes, a Warning was issued to the Organisation.

7. The Commission reminds all organisations that they must have sufficiently robust processes to obtain a functional understanding of software to be deployed, in order to assess the security risks to personal data in their possession or control. Failure to do so would be breach of the Protection Obligation.

## R.I.S.E Aerospace Pte. Ltd.

## [2020] SGPDPCS 21

| **Case Number** | : | Case No. DP-2007-B6832 |
| --- | --- | --- |
| **Decision Date** | : | 13 November 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | R.I.S.E Aerospace Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised modification or access to personal data* – *Insufficient security arrangements*

1. On 25 August 2020, R.I.S.E Aerospace Pte Ltd (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) of a ransomware infection that had rendered its network storage server inaccessible to the Organisation (the “**Incident**”).

2. The Incident occurred on or about 23 August 2020. Personal data of 21 employees were encrypted by the ransomware. The personal data encrypted included the name, address, contact number, NRIC number, Work Permit details, passport details. redacted bank account numbers, and child’s date of birth.

3. Investigations revealed that the Organisation had not implemented adequate technical security arrangements to protect the personal data in its possession or control, in particular, the Organisation did not carry out any security scans or perform updates to the server firmware despite being prompted to do so by the device manufacturer. In addition, the Organisation did not put in place any documented form of IT Security policies such as its password policy, policies for patching and updating of the company server etc. These failings had resulted in a system that had vulnerabilities which a hacker could exploit by injecting ransomware into the server.

4. Following the Incident, the Organisation had since discontinued the use of its network storage server and to opt for cloud storage instead. Additionally, the Organisation also decided to encrypt all its sensitive data and only store them on offline devices.

5. In the circumstances, the Deputy Commissioner for Personal Data Protection finds the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”) and took into account the following factors in deciding to issue a Warning to the Organisation.

a. The low number of affected individuals;

b. There was no evidence that the personal data affected in the Incident had been misused in any form;

c. The Organisation had a backup copy of the encrypted personal data and did not lose any personal data as a result of the Incident; and

d. The Organisation voluntary notified the Commission of the Incident.

6. In view of the remedial actions taken by the Organisation, the Commission will not be issuing any other directions.