## GeniusU Pte. Ltd.

## [2022] SGPDPCS 1

| **Case Number** | : | DP-2101-B7725 |
| --- | --- | --- |
| **Decision Date** | : | 21 April 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | GeniusU Pte. Ltd. |

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

1. On 12 January 2021, GeniusU Pte. Ltd. (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) of unauthorized access and exfiltration of a staging application database (the “**Database**”) holding personal data (the “**Incident**”).

2. The personal data of approximately 1.26 million users were affected. The datasets affected comprised first and last name, email address, location and last sign-in IP address.

3. The Organisation’s internal investigations revealed that the likely cause of the Incident was compromise of one of its developer’s password, either because the developer used a weak password for his GitHub account or the password for his GitHub account had been compromised. This allowed the threat actor to enter the Organisation’s GitHub environment. As the Organisation had stored the login credentials to the Database in the codebase in its GitHub environment, the threat actor was able to gain access to and exfiltrate personal data stored in the Database.

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

a. Rotated the credentials of the Database;

b. Removed all hard-coded credentials from the codebase;

c. Purged all existing website sessions;

d. Removed all personal data from non-production environment servers,

e. Implemented multi-factor authentication on all work-related accounts;

f. Implemented a standardised cyber security policy and related procedures for all staff; and

g. Notified users and the GDPR data authority (Ireland) of the Incident.

5. 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**”).

6. Based on its admissions, the Organisation had breached the Protection Obligation by:

a. Storing credentials for the Database in the codebase in its GitHub environment. This meant that once the threat actor was able to access the GitHub environment, he was able to discover the credentials to access personal data stored in the Database; and

b. Storing actual personal data in the Database that was in a non-production (testing) environment, which are usually not as secure as production environments. Actual personal data should not be stored in testing environments, which are known to be less secure.

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

8. Having considered the circumstances set out above and the factors listed at section 48J(6) of the PDPA and the circumstances of the case, 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 Organisation is given a notice to pay a financial penalty of $35,000.

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

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

## L’Oreal Singapore Pte. Ltd.

## [2019] SGPDPCS 9

| **Case Number** | : | Case No. DP-1812-B3091 |
| --- | --- | --- |
| **Decision Date** | : | 26 December 2019 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | L’Oreal Singapore Pte. Ltd. |

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

1. L’Oreal Singapore Pte Ltd (the “**Organisation**”) operated a website which had a login portal that enabled its customers to view their profile information, redeem vouchers and make enquiries about customer points (“**Customer Login Page**”). The customers’ profile information included their name, email address, postal address, mobile number and date of birth (the “**Personal Data**”). The development and maintenance of the website was carried out by a vendor engaged by the Organisation.

2. To improve the loading speed of the website, the Organisation instructed its vendor to make some changes to the website in November 2018. However, the Organisation failed to scope the User Acceptance Tests (“**UATs**”) to include the normal functioning of the website, in particular the login and caching functions of the Customer Login Page, after the code changes were introduced. As a result, when a customer (“**Customer A**”) logged into the Customer Login Page, his or her Personal Data would be cached. Customer A’s Personal Data would then be disclosed to customers who subsequently logged in to the Customer Login Page until the cache was refreshed. Similarly, the Personal Data of the second customer (“**Customer B**”), who logged in after the cache refresh, would be cached, leading to disclosure of Customer B’s Personal Data to the third customer who logs in next, and all subsequent customers until the next cache refresh. When the Organisation came to know of this, the Organisation disabled the Customer Login Page. The Organisation also engaged a consultant to assist in its investigations into the matter and to provide recommendations to prevent similar incidents in the future.

3. The Personal Data Protection Commission (“**Commission**”) found that Personal Data of 7 individuals had been exposed to the risk of unauthorised disclosure as a result of the Organisation’s failure to ensure appropriate testing of its website or make other security arrangements to protect the Personal Data. The Commission notes the Organisation’s representations that it had completed all necessary and appropriate UATs based upon the reasonably foreseeable impact of the requested changes to its website. However, as mentioned at [2] above, the scope of the UATs was inadequate because it did not simulate the normal operating environment of the website. In particular, the UATs only provided for a limited test case of a single user logging into the website, and failed to include the foreseeable scenario of multiple users logging in sequentially.

4. Having considered the representations and taking into account all the relevant circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 24 of the Personal Data Protection Act 2012 and decided to give a warning to the Organisation.

## BLS International Services Singapore Pte. Ltd.

## [2020] SGPDPCS 24

| **Case Number** | : | Case No. DP-2007-B6563 |
| --- | --- | --- |
| **Decision Date** | : | 30 November 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | BLS International Services Singapore Pte. Ltd. |

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

1. BLS International Services Singapore Pte. Ltd. (the “**Organisation**”) provides government-to-citizen services for the High Commission of India in Singapore, such as visa and consular services.

2. On 7 July 2020, the Personal Data Protection Commission (the “**Commission**”) received information that the URLs of the printable version of appointment booking confirmation webpages could be manipulated to access other individuals’ personal data (the “**Incident**”). The personal data comprised the individual’s name, passport number, contact number, email address, type of service request, booking date/time, appointment date/time, and number of booking applications.

3. 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**”).

4. Investigations revealed that on 8 June 2020, which was about a month prior to the Incident, the Organisation had implemented a new booking system for the High Commission of India. Under this new booking system, users who submitted a booking for an appointment at the High Commission of India would be provided with an URL, which led to a printable version of the booking confirmation. In designing the booking system, the Organisation had intended for the URLs to be encrypted. This would have made it more difficult for people to manipulate the URL. However, the encryption was not done properly due to a coding error. Although the Organisation had conducted some testing on the new booking system, the testing was not extensive enough to detect the error.

5. Upon realising the occurrence of the Incident from the Commission on 16 July 2020, the Organisation took immediate action to investigate and subsequently identified the coding error. On the same day, the Organisation made changes to the booking system. It stopped providing users with an URL to a printable version of their booking confirmation. Instead, the booking confirmation would be sent to the user’s email account.

6. The Organisation’s records showed that a total of 3,357 individuals used the new booking system from 8 June 2020 to 16 July 2020. This meant that the personal data of 3,357 individuals was at risk of exposure by URL manipulation.

7. The Deputy Commissioner for Personal Data Protection found that the Organisation was in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 for failing to conduct adequate testing of the booking system before it went “live”. Depending on how the URL encryption was implemented, URL encryption could had been a reasonable security measure for the personal data type the Organisation was collecting. However, because the Organisation had not conducted adequate testing of the booking system before it went “live”, the Organisation did not detect the coding error, thereby resulting in the Incident.

8. After considering the circumstances of the 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 Deputy Commissioner for Personal Data Protection directs that the Organisation pays a financial penalty of $5,000 for the breach.

9. The Organisation must make payment of the financial penalty 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 it is paid in full.

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

## Chan Brothers Travel Pte Ltd

## [2020] SGPDPCS 11

| **Case Number** | : | Case No. DP-1905-B3936 |
| --- | --- | --- |
| **Decision Date** | : | 21 July 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Chan Brothers Travel Pte Ltd |

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

1. On 23 May 2019, the Personal Data Protection Commission (the “**Commission**”) received a data breach notification from Chan Brothers Travel Pte Ltd (the “**Organisation**”) and a complaint from a member of the public. Both were in relation to personal data being at risk of unauthorised access through the Organisation’s website at [http://chanbrotherstravelclub.force.com](https://chanbrotherstravelclub.force.com/s/) (the “**Website**”) (the “**Incident**”).

2. In March 2017, the Organisation purchased Community Cloud, a product of Salesforce.com Singapore Pte Ltd (“**Salesforce**”), to host the Website. The Organisation managed the Website internally. In August 2018, the Organisation engaged Aodigy Asia Pacific Pte Ltd (“**Aodigy**”) as an outsource vendor to maintain and improve the Website.

3. The Website provided three online forms for enquiries and feedback. These were the “Enquiry Form”, Feedback Form” and “Post-Tour Feedback Form” (collectively the “**Forms**”). The Forms collected the users’ names, email addresses and mobile phone numbers.

4. In March 2018, there was a software update released by Salesforce for Community Cloud. This software update included an automated search engine optimisation feature (the “**SEO**”). As the Website’s access configuration was set to “Public”, the Forms automatically inherited the same setting for the purpose of the SEO feature. The result was that the personal data of an estimated 5,593 individuals collected by the Forms were indexed and cached, and made searchable, through online web search engines.

5. Organisations that employ IT systems or features are responsible for data security. Organisations must acquire knowledge of the security settings and be aware of security implications of software features of their IT system, and they must configure the security settings to enable effective protection of personal data stored in the IT system. This responsibility extends to new features introduced by subsequent software releases. Organisations that lack the IT knowledge to discharge this responsibility should engage qualified assistance.

6. The Organisation failed to consider the implication of the “Public” setting of the Website on the security of the data collected by the Forms. It also failed to understand the function and operation of the SEO feature. The combination of these acts of omission resulted in the security issues arising leaving the SEO feature enabled.

7. The Organisation claimed not to have received any notification from Salesforce of the SEO release. However, this is contradicted by the following. First, the notes of the software release was published on the website of Salesforce. Second, Aodigy had (in its role as vendor for another project) received information of the release. On balance, it is therefore unlikely that Salesforce would have omitted to notify the Organisation about the software release. In any event, the software release was in March 2018 when the Organisation was still maintaining the Website internally. The responsibility to assess the security implications of the software release laid squarely on its shoulders during that 5-month period before Aodigy was engaged.

8. Further, there is some uncertainty over whether Aodigy was instructed to review the security configuration of the Website (including the new software features) as part of its maintenance services when it was engaged. The Organisation did not give clear instructions to Aodigy to assess the security configuration of the IT system as part of the maintenance services.

9. In the circumstances, the Deputy Commissioner for Personal Data Protection therefore found the Organisation in breach of section 24 of the Personal Data Protection Act 2012 and took into account the following factors in deciding to issue a Warning to the Organisation:

a. The personal data at risk of disclosure was limited to names, email address and contact numbers, apart from an estimated 50 NRIC numbers.

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

c. Prompt co-operation in the course of the Commission’s investigations.

10. No directions are required as the Organisation took immediate steps to prevent the recurrence of the Incident.

## Horizon Fast Ferry Pte Ltd

## [2020] SGPDPCS 17

| **Case Number** | : | Case No. DP-1912-B5465 |
| --- | --- | --- |
| **Decision Date** | : | 27 August 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Horizon Fast Ferry Pte Ltd |

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

1. The Personal Data Protection Commission (“**Commission**”) investigated a complaint against Horizon Fast Ferry Pte. Ltd. (the “**Organisation**”) where the Organisation’s email account, singapore@horizonfastferry.com (the “**Email Account**”) had sent out phishing emails to its customers (the “**Incident**”).

2. Investigations revealed that the computer used to access the Email Account was infected with malware. This caused the Email Account to send phishng emails to three customers. Each email contained only the personal data that the customer himself had sent to the Email Account to book ferry tickets. Hence there was no disclosure of other customers’ personal data in the phishing email.

3. The Organisation informed the Commission that it had implemented various security measures prior to the Incident such as updating their anti-virus software regularly. However, investigations revealed that the password to access the Email Account was shared by 11 employees of the Organisation and had not been changed for almost 3 years. This poor management of passwords fell short of what is reasonably required to protect the personal data in the Email Account.

4. The Deputy Commissioner for Personal Data Protection therefore found that the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 for failing to implement reasonable security arrangements to protect the personal data in its possession or under its control. Upon consideration of the facts, a warning was issued to the Organisation.

## ERGO Insurance Pte. Ltd.

## [2019] SGPDPCS 2

| **Case Number** | : | Case No. DP-1810-B2869 |
| --- | --- | --- |
| **Decision Date** | : | 26 September 2019 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | ERGO Insurance Pte. Ltd. |

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

1. ERGO Insurance Pte Ltd (the “**Organisation**”) is a general insurer and operates an internet portal (the “**Portal**”) which enables its insurance intermediaries, who are not the Organisation’s employees, to request for documents of policyholders represented by the intermediaries. These documents contain the policyholders’ personal data such as their names, addresses, car registration numbers, genders, nationalities, NRIC numbers, dates of birth and contact numbers (the “**Personal Data**”).

2. The Organisation voluntarily informed the Personal Data Protection Commission on 15 October 2018 that it had earlier discovered, on 11 September 2018, that some of its insurance intermediaries had been incorrectly sent documents of policyholders who were represented by other insurance intermediaries (the “**Incident**”). The Incident arose when some insurance intermediaries (the “**Intermediaries**”) requested for documents of policyholders which they represent through the Portal. However, the Organisation’s application and printer servers had been shut down for a scheduled system downtime and when they were restarted, the Organisation’s employees had failed to follow the correct restart process. They were supposed to start both servers at the same time but this was not done as the starting of the printer server initially failed. This resulted in documents with duplicate document IDs being generated and hence the wrong documents being sent to the Intermediaries. As a result of the Incident, the Personal Data of 57 individuals were mistakenly disclosed to the Intermediaries.

3. The Personal Data Protection Commission found that the Organisation did not have in place a clearly defined process to restart its application and printer servers and a sufficiently robust document ID generation process (such as including a timestamp as part of the document ID) to prevent the duplication of document IDs. In the circumstances the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 24 of the Personal Data Protection Act 2012 and decided to give a warning to the Organisation. No directions are required as the Organisation implemented corrective measures that addressed the gap in its security arrangements.

## CampVision Ltd.

## [2019] SGPDPCS 5

| **Case Number** | : | Case No. DP-1808-B2508 |
| --- | --- | --- |
| **Decision Date** | : | 08 October 2019 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | CampVision Ltd. |

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

1. CampVision Ltd (the “**Organisation**”) engaged SHINE Children and Youth Services (“**SHINE**”) to collect evaluation feedback from youths participating in its programmes. For this purpose, SHINE collected information from the youths on the Organisation’s behalf, including their names, NRIC numbers, email addresses and schools (the “**Personal Data**”). SHINE did this using a platform provided by Typeform S.L. (“**Typeform**”), a company based in Spain, which provides online survey services. In June 2018, Typeform discovered that an unknown third party had gained access to its server and downloaded information provided by many Typeform users, including Personal Data collected by SHINE on behalf of the Organisation (the “**Incident**”).

2. The Personal Data Protection Commission (the “**Commission**”) found that Personal Data of 106 individuals collected by SHINE on behalf of the Organisation had been exposed to the risk of unauthorised access and disclosure in the Incident. The Commission’s investigations revealed that there was no written contract between the Organisation and SHINE setting out SHINE’s obligations with respect to the processing and protection of Personal Data, which it collected on the Organisation’s behalf. The Organisation also admitted that it had not conveyed any instructions to SHINE with respect to protection of the Personal Data. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 24 of the Personal Data Protection Act 2012 and decided to give a warning to the Organisation.

## Singapore Medical Association

## [2020] SGPDPCS 13

| **Case Number** | : | Case No. DP-2001- B5770 |
| --- | --- | --- |
| **Decision Date** | : | 21 July 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Singapore Medical Association |

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

1. On 31 January 2020, Singapore Medical Association (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) that the personal data of 68 individuals in 137 emails had been forwarded to an external email address without authorisation between 28 and 30 January 2020. The personal data comprised National Registration Identification Card numbers, dates of birth, indemnity coverage, period of coverage, educational information and financial transaction information.

2. The Organisation believed an unauthorised user (“**UU**”) gained entry into the affected Microsoft Office 365 email account by a brute force attack but did not have the system logs to confirm this. Regardless, the unauthorised entry enabled the UU to create an email rule to forward received emails to the external email address.

3. It was found that the Organisation failed to conduct periodic security reviews of its IT system. Consequently, it missed the opportunity to detect the following security issues that could have prevented the incident:

a. There was no periodic change to the passwords of email accounts. As an example, the password to the affected account had not been changed since first use in November 2013.

b. The Organisation collected financial information such as bank account details and swift codes and should have considered, as part of a security review, whether it needed to enhance security measures. For example, encryption of emails and/or attachments containing such sensitive personal data.

c. A reasonable security review would also have noted the absence of security arrangements against brute force attacks. Common examples of anti-brute force measures include limiting the number of failed login attempts and account lockouts. Without anti-brute force measures, a password-protected account could be subjected to unlimited and uninterrupted automated login attempts from the Internet. Given sufficient time, the attacker will succeed in arriving at the correct password.

4. 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. Upon consideration of the facts, a warning was issued to the Organisation. No directions are required as the Organisation had taken actions to address the gaps in its security arrangements

## Tan Tock Seng Hospital Pte. Ltd.

## [2019] SGPDPCS 3

| **Case Number** | : | Case No. DP-1902-B3372 |
| --- | --- | --- |
| **Decision Date** | : | 26 September 2019 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Tan Tock Seng Hospital Pte. Ltd. |

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

1. Tan Tock Seng Hospital Pte Ltd (the “**Organisation**”) voluntarily informed the Personal Data Protection Commission (the “**Commission**”) on 14 February 2019 that it had discovered on 12 February 2019 that letters sent to 85 patients (the “**Affected Individuals**”) to reschedule their appointments with the Organisation (the “**Letters**”) had been sent to the wrong addresses (the “**Incident**”). These Letters contained the names, NRIC numbers and appointment of the Affected Individuals (the “**Personal Data**”). Such letters were usually generated automatically. However, on 12 February the Letters were generated manually using the mail merge function in Microsoft Word to extract the Personal Data from a spreadsheet (the “**Spreadsheet**”) and insert the data in the letters. However, the staff that had been tasked to generate these letters only selected and sorted the address field in the Spreadsheet. As a result, the addresses in the Spreadsheet no longer corresponded to the correct patient information and when the staff ran the mail merge function, the incorrect addresses were inserted in the letters.

2. The Commission found that the Organisation did not conduct any checks on the generation and printing of the letters. A simple random sampling of the letters would have likely averted the Incident or greatly reduced the number of individuals affected. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 24 of the Personal Data Protection Act 2012 and decided to give a warning to the Organisation. No directions are required as the Organisation has implemented corrective measures that addressed the gap in its security arrangements.

## QCP Capital Pte Ltd

## [2022] SGPDPCS 16

| **Case Number** | : | DP-2108-B8816 |
| --- | --- | --- |
| **Decision Date** | : | 16 September 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | QCP Capital Pte Ltd |

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

1. On 30 August 2021, QCP Capital Pte Ltd (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) of a personal data breach that had occurred through an unauthorised access to employee accounts and exfiltration of customer personal data (the “**Incident**”).

2. As a result of the Incident, the personal data of 675 individuals was exfiltrated. The personal data affected includes name, NRIC number, date of birth, address, passport scan, passport number, photograph, email address, phone number, Telegram and WeChat ID, whitelisted address and trading records (which included the account balances, buy/sell/settlement activities).

3. The Organisation engaged an external cybersecurity company, Blackpanda Pte Ltd, to investigate the Incident. Its investigations found that the threat actor(s) had accessed two accounts, belonging to one employee, to gain unauthorised access to the Organisation systems and subsequently exfiltrated of personal data.

4. Investigations revealed that the Organisation had provided and made reasonable security arrangements to protect personal data in its possession and/or control in relation to the Incident. The Organisation also had an internal monitoring system in place which allowed the Organisation to detect, escalate the anomalous transaction, flag and suspend the trading account affected.

5. Following the Incident, the Organisation took prompt and extensive remedial action to mitigate the effects of the Incident and enhance the overall robustness of its security measures. This included notifying the affected individuals, layering access controls and introducing mandatory hardware key access authentication.

6. In view of the above, the Deputy Commissioner for Personal Data Protection is satisfied that the Organisation was in compliance with its Protection Obligation under section 24 of the PDPA and cannot be held liable for the unauthorised access by the threat actor(s) involved. No enforcement action therefore needs to be taken in relation to the Incident.

## FWD Singapore Pte Ltd

## [2020] SGPDPCS 5

| **Case Number** | : | Case No. DP-1907-B4352 |
| --- | --- | --- |
| **Decision Date** | : | 13 March 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | FWD Singapore Pte Ltd |

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

1. The Personal Data Protection Commission (the “**Commission**”) was notified on 26 July 2019 by FWD Singapore Pte Ltd (the “**Organisation**”) of the unintended disclosure of 71 individuals’ (the “**Affected Individuals**”) personal data contained in 42 payment advice letters sent to incorrect recipients between 20 June 2019 and 17 July 2019 (the “**Incident**”).

2. The Incident arose from the Organisation’s attempt to fix a logic error in the system that it used to generate payment advice letters. The error was introduced when a fix for an earlier logic error was deployed. The Commission found that the second logic error could have been detected if manual code review and unit testing had been conducted to a reasonable standard.

3. The second logic error caused the extraction of incorrect mailing addresses for payment advice letters in some circumstances. This resulted in the Affected Individuals’ names and identification numbers in payment advice letters being sent to incorrect addresses. The Organisation should have taken care in conducting its manual code review and unit testing to avoid another logic error. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of its Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”).

4. The Deputy Commissioner took into account the following factors in deciding to issue a warning to the Organisation:

a. The Organisation had managed to retrieve letters containing the personal data of 67 out of the 71 Affected Individuals.

b. The Organisation voluntarily notified the Commission of the Incident.

c. The second logic error resulted in the extraction of incorrect mailing addresses only in limited circumstances.

5. No directions are required as the Organisation took steps to improve its development processes to prevent the recurrence of the Incident.

## Actstitude Pte Ltd

## [2020] SGPDPCS 8

| **Case Number** | : | Case No. DP-1910-B5129 |
| --- | --- | --- |
| **Decision Date** | : | 20 March 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Actstitude Pte Ltd |

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

1. Actstitude Pte Ltd (the “**Organisation**”) is a social media platform marketing agency. It has a webpage allowing individuals interested in joining the Organisation to upload their resumes. For each resume uploaded, a file was created with a Uniform Resource Locator (“**URL**”) and stored in a database. Between August 2018 to October 2019, over 160 individuals uploaded their resumes.

2. The Organisation, however, admitted that it did not put in place controls to restrict access to the resume files. The URLs generated by the Organisation could also be manipulated to access resume files uploaded by different individuals.

3. When the webpage was created on 5 July 2018, the Organisation did not conduct vulnerability scanning as part of pre-launch testing; neither did the Organisation conduct periodic security reviews. Such scans offer a reasonable chance of detecting both the lack of access controls and the vulnerability of the URLs to manipulation.

4. The result of this failure to put in place access controls or to conduct security testing was that Google indexed and disclosed the URLs when a search was made of the names in the uploaded resumes. The URLs could then be manipulated to access the resumes of other individuals. This led to a complaint to the Personal Data Protection Commission on 25 October 2019.

5. 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 disclosure. The Organisation was in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012. Upon consideration of the facts, a warning was issued to the Organisation. No directions are required as the Organisation had taken action to address the gaps in its security arrangements.

## NTUC Income Insurance Co-Operative Limited

## [2020] SGPDPCS 2

| **Case Number** | : | Case No. DP-1907-B4288 |
| --- | --- | --- |
| **Decision Date** | : | 28 January 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | NTUC Income Insurance Co-Operative Limited |

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

1. The Personal Data Protection Commission (the “**Commission**”) was notified on 17 July 2019 by NTUC Income Insurance Co-Operative Limited’s (the “**Organisation**”) of the unintended disclosure of personal data to users making enquiries through its website. The users received automated acknowledgement emails attached with files containing personal data of other individuals (the “**Incident**”).

2. On 10 July 2019, the Organisation enhanced the website’s online enquiry application to allow users to upload supporting documents together with their enquiry submissions. When a user A uploaded files, the application assigned a variable that served to identify the files for future retrieval by the same user or by the Organisation. However, due to a coding error, if the next user B did not upload files, the variable generated for the preceding user was applied to the B’s submission. As a result, the supporting documents uploaded by A were associated with B’s submission.

3. This coding error manifested in the sending of acknowledgement emails, which were intended to include supporting documents submitted by the user. When acknowledgement emails were generated for a user who did not upload files, the coding error caused the files uploaded by a preceding user to be attached. There were 17 users whose uploaded files were sent to 123 other users in this way. The files contained their personal data, such as names, policy numbers, premium amounts, sum assured and period of coverage, email and mailing addresses.

4. The Organisation admitted that the Incident was caused by poor quality codes. The Commission found that such errors should have been detected during the manual code review process that the Organisation had conducted. Further, before the enhancement went “live”, the Organisation’s tests did not simulate the various scenarios expected whereby some users would upload files while others did not.

5. The Organisation has since sought to improve checks on coding quality by replacing its manual code review process with tools such as Crucible and SonarQube. It also moved to ensure that test scenarios were adequate and that test plans and reviews were in place before changes in its IT applications and systems were allowed to be deployed.

6. In the circumstances, 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 and decided to give a warning to the Organisation. No directions are required as the Organisation has implemented corrective measures that addressed the gap in its security arrangements.

## Jean Yip Salon Pte Ltd

## [2020] SGPDPCS 6

| **Case Number** | : | Case No. DP-1907-B4281 |
| --- | --- | --- |
| **Decision Date** | : | 13 March 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Jean Yip Salon Pte Ltd |

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

1. The Personal Data Protection Commission (the “**Commission**”) received a complaint on 16 July 2019 about an employee system (the “**System**”) maintained by Jean Yip Salon Pte Ltd (the “**Organisation**”) that was publicly accessible via the internet. The personal data of 28 individuals disclosed via the System included their name, NRIC number, residence status, date of birth, nationality, gender, mobile number and job designation.

2. The Commission found that the Organisation did not adopt reasonable measures to protect personal data in its possession against risk of unauthorised access. First, the Organisation opened public access to a server without ascertaining what it hosted. As a result, while enabling public access to the Customer Online Appointment Booking System, it inadvertently also allowed access to the System (meant only for internal use), which was also hosted on the same server. Second, there were no processes in place to remove or deactivate unnecessary user accounts of the System. Finally, the Organisation did not enforce a password policy for the user accounts of the System. As such, the complainant was able to gain access to the System by simply using a well-known and weak default username and password pair.

3. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 24 of the Personal Data Protection Act 2012 and issued a warning to the Organisation. No directions were required as the Organisation had implemented corrective measures that addressed the gaps in its security arrangements.

## AXA Insurance Pte. Ltd.

## [2020] SGPDPCS 1

| **Case Number** | : | Case No. DP-1907-B4201 |
| --- | --- | --- |
| **Decision Date** | : | 13 January 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | AXA Insurance Pte. Ltd. |

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

1. The Personal Data Protection Commission (the **“Commission**”) received a complaint on 4 July 2019 against AXA Insurance Pte. Ltd. (the “**Organisation**”). The complaint was about an email (the “**Email**”) sent with a scanned document (the “**Attachment**”) containing personal data of 87 other policyholders (the“**Affected Individuals**”) to the Complainant on 28 June 2019 (the “**Incident**”).

2. The Attachment was an internal email correspondence of the Organisation that contained the names, NRIC numbers, insurance policy numbers and the details of the servicing agents of the Affected Individuals (the “**Personal Data**”). The Attachment was not meant for the Complainant.

3. The Organisation admitted that during scanning of documents by its employees, it did not have a process to segregate documents intended for internal record purposes from documents for customers.

4. The Organisation’s customer care specialist who retrieved the scanned document which formed the Attachment also failed to check the Attachment before sending out the Email.

5. The Commission found that these lapses in processes resulted in the Incident. The lapses pointed to a failure by the Organisation to make reasonable security arrangements to protect the personal data of its policyholders from inadvertent disclosure by its employees. The Organisation was therefore found in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012. The Commission has decided to issue a warning to the Organisation after considering the admission of liability by the Organisation, the impact of the breach and the corrective measures taken.

## ChampionTutor Inc. (Private Limited)

## [2021] SGPDPCS 12

| **Case Number** | : | Case No. DP-2103-B7984 |
| --- | --- | --- |
| **Decision Date** | : | 10 August 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | ChampionTutor Inc. (Private Limited) |

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

1. On 24 February 2021, the Personal Data Protection Commission (the “**Commission**”) received information that ChampionTutor Inc. (Private Limited)’s (the “**Organisation**”) database, containing personal data of individuals, was being sold on dark web (the “**Incident**”).

2. The Organisation was not aware of the Incident until it was notified by the Commission. The cause of the Incident was suspected to be SQL injection of the Organisation’s website. The Organisation knew about this SQL injection vulnerability when it conducted a penetration test in December 2020. The Organisation had instructed its developer, based in India, to fix the vulnerability. However, the developer did not act on the request and this vulnerability was left unfixed until the Incident happened.

3. As a result, the personal data of 4,625 students were affected. The personal data included name, email address, contact number and address.

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

a. Engaged a new team of developers to fix all the SQL injection vulnerabilities;

b. Parameterised SQL statements by disallowing data-directed context changes to prevent SQL injection attacks from resurfacing; and

c. Is in the process of revamping the entire website source codes to reduce possible vulnerabilities.

5. The Organisation admitted to having breached the Protection Obligation under section 24 of the Personal Data Protection Act (the “**PDPA**”), and requested for the matter to be dealt with in accordance with the Commission’s Expedited Decision Procedure.

6. The Organisation admitted it was aware of the SQL injection vulnerability in December 2020. Yet, the Organisation failed to take active steps to fix the vulnerability even when its developer was not responsive, purportedly due to the COVID-19 pandemic, and the Organisation left the vulnerability unresolved until the Incident happened.

7. In the circumstances, the Organisation is found to have breached section 24 of the PDPA.

8. On 14 July 2021, the Organisation was notified of the Commission’s intention to impose a financial penalty based on the Commission’s consideration of the factors listed under section 48J(6) of the PDPA, and the circumstances of this case, in particular (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 Organisation was invited to make representations.

9. Having considered the Organisation’s representations dated 28 July 2021, the Deputy Commissioner hereby directs the Organisation to pay a financial penalty of $10,000 in 12 instalments by the due dates as set out in the accompanying notice, failing which the full outstanding amount shall become due and payable immediately and 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.

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

## SSA Group International Pte Ltd

## [2020] SGPDPCS 4

| **Case Number** | : | Case No. DP-1909-B4729 |
| --- | --- | --- |
| **Decision Date** | : | 02 March 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | SSA Group International Pte Ltd |

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

1. The Personal Data Protection Commission (the “**Commission**”) received a complaint on 6 September 2019 that individuals’ course registration information were publicly accessible via a webpage (the “**Webpage**”) maintained by SSA Group International Pte Ltd (the “**Organisation**”). The Webpage contained 53 individuals’ names. Other information disclosed via the Webpage included course titles, sponsorship type, information on how the registrant knew about the Organisation and date of transaction.

2. The Commission found that the Organisation did not adopt reasonable steps to protect personal data in its possession or control against risk of unauthorised access. First, there were no authentication mechanisms in place to limit access to the Webpage. As such, the Webpage was indexed by search engines and made publicly searchable online. Second, there were no formal instructions provided to the developer of the Webpage to protect the contents during its creation in April 2018. Finally, there were no security reviews, including vulnerability scanning, conducted for the Webpage by the Organisation since its creation. As such, the fact that the Webpage was freely accessible from the Internet went undetected for more than a year.

3. On the facts above, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 24 of the Personal Data Protection Act 2012.

4. In deciding to issue a warning to the Organisation, the Deputy Commissioner also took into account the following considerations:

a) The Organisation’s representation that the Webpage had not been easy to locate was incorrect. An online search of the names of the 53 affected individuals produced the Webpage’s URL.

b) The remedial measures taken by the Organisation, the type of personal data at risk, the inadvertent nature of the breach and the absence of a previous breach, all mentioned by the Organisation in its representations, had also been duly considered.

c) The Commission’s previous decisions, including as Re Watami Food Service Pte Ltd [2018] SGPDPC [12] and Re Jade E-Services Singapore Pte Ltd [2018] SGPDPC 21 which had similar case facts.

5. No directions are required as the Organisation has implemented corrective measures that addressed the gaps in its security arrangements.

## Carousell Pte. Ltd.

## [2021] SGPDPCS 11

| **Case Number** | : | Case No. DP-2105-B8350 |
| --- | --- | --- |
| **Decision Date** | : | 03 August 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Carousell Pte. Ltd. |

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

1. On 14 May 2021, Carousell Pte. Ltd. (the “**Organisation**”) informed the Personal Data Protection Commission of an unauthorized access to their users’ accounts due to credential stuffing.

2. The Organisation was first alerted on 26 April 2021 when a user reported to the Organisation that his account had been hijacked and there were attempts to make unauthorised purchases. On 1 June 2021, the Organisation was alerted to another incident involving the same modus operandi where legitimate credentials were used to log in to users’ accounts and unauthorised purchases were made (collectively, the “**Incident**”).

3. The Organisation’s investigations indicated that the Incident was due to the threat actor(s) obtaining the login details and passwords of some of their users due to an exposure of the account details on another service provider’s platform. The threat actor(s) succeeded in certain cases where the user used the same login and password for their account with the Organisation and their compromised accounts with other provider’s platforms. After successfully logging into the account, the threat actor(s) was able to perform actions as an authorised user. The threat actor(s) would also have access to the data in an individual’s account and modify the account settings.

4. The Organisation’s investigations found that there was no known compromise or unauthorised access of information in other accounts that were stored in the same database. At the time of the Incident, the Organisation had in place security arrangements including, but not limited to, the following:

a. Users are informed when there is a change to the password, email or phone number linked to their account, or when a new device is used to log in;

b. Training of account takeover model to identify and investigate likely account takeovers;

c. Card transactions that meet a certain fraud score are blocked or reviewed;

d. One Time Password required to complete transactions for all card payments;

e. Regular review of policies and regular testing and review of risk rules based on fraud trends, seasonality, regulation and all related indicators;

f. Company-wide training and educational newsletters to increase staff awareness on security and data protection requirements; and

g. Conduct annual penetration security assessment.

5. I am of the view that the Organisation had adopted reasonable standards for protecting personal data in their customer accounts on an objective review of the measures that were implemented at the time of the Incident. Further, the Organisation took prompt action to mitigate the effects of the breach by suspending the compromised users accounts and force password resets for affected users. Emails were sent to alert affected users of suspicious login in their accounts. DBS Paylah! Express Checkout was disabled for affected users whose accounts were suspected to have been compromised.

6. The Organisation also reviewed the Incident, and took remedial measures to enhance the robustness of their security measures, including but not limited to the following:

a. Blocked suspicious IP addresses;

b. Added rules into third party fraud detection tool to prevent account takeovers;

c. Implemented a mandatory 2FA verification, via email, in the event there is a change detected in the user’s device ID across all platforms; and

d. Efforts to educate users and raise awareness to fight against phishing attempts were enhanced.

7. Having found that at the time of the Incident, the Organisation had implemented reasonable security arrangements to protect the personal data under its control, I conclude that the Organisation did not breach its Protection Obligation under the Personal Data Protection Act.

## Singapore Telecommunication Limited

## [2022] SGPDPCS 5

| **Case Number** | : | DP-2102-B7878 |
| --- | --- | --- |
| **Decision Date** | : | 10 December 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Singapore Telecommunication Limited |

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

1. On 10 February 2021, Singapore Telecommunication Limited (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) of a personal data breach that had occurred through the exploitation of zero-day vulnerabilities in a File Transfer Appliance (“**FTA**”) provided by a third party system (the “**Incident**”).

2. As a result of the Incident, 9,921 files containing personal data were exfiltrated. The personal data of 163,370 individuals which included their name, NRIC number, FIN, UIN, nationality, date of birth, address, email address, mobile number, photograph, staff, company pass or ID, bank account number, credit card information (with expiry date), billing information, and vehicle number were affected.

3. The Organisation engaged an external cybersecurity company, FireEye Mandiant, to investigate the Incident. Its investigations found that the threat actors had exploited two (2) zero-day vulnerabilities of the FTA to gain unauthorised access to the FTA’s MySQL database and subsequent file downloading.

4. Investigations revealed that the Organisation had a license to use the FTA with the FTA developer, Accellion Pte Ltd (“**Accellion**”). Accellion was the only party that had access to the proprietary source code to the FTA system. Accordingly, the discovery and rectification of the zero-day vulnerabilities within the FTA system fell within the sole responsibility and control of the developer. We are of the view that the Organisation could not have detected or prevented the incident as it had no control or visibility of the zero-day vulnerability of the FTA.

5. The Organisation had provided and made reasonable security arrangements to protect personal data in its possession and/or control in relation to the Incident. The Organisation maintained the practice of updating and patching the FTA within five (5) days of patch/update receipt.

6. 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 shutting down the FTA, conducting thorough review of processes and file sharing protocols to enhance information security posture, and offering identity monitoring service to the affected individuals.

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 and cannot be held liable for zero-day vulnerabilities on a third party system. No enforcement action therefore needs to be taken in relation to the Incident.

## Tanah Merah Country Club

## [2020] SGPDPCS 7

| **Case Number** | : | Case No. DP-1906-B4115 |
| --- | --- | --- |
| **Decision Date** | : | 20 March 2020 |
| **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*

[Editorial note: An application for reconsideration was filed against the decision in *Re Tanah Merah Country Club*. Pursuant to this application, the Commissioner has decided to reduce the financial penalty imposed on the Organisation from $8,000 to $4,000. As the application did not give rise to significant legal or factual issues, a separate decision on the application will not be published.]

1. On 19 June 2019, Tanah Merah Country Club (the “**Organisation**”) informed the Personal Data Protection Commission (the “**Commission**”) of unauthorised access to its electronic direct mail (“**EDM**”) system (the “**Incident**”). During the Incident, which occurred on 9 June 2019, the EDM system was used to send unauthorised spam emails.

2. The Organisation was unable to determine how unauthorised access was gained to the EDM system. During investigations, it was discovered that the common password for login to the EDM system was weak, as it comprised the initials of the Organisation and the year 2010 (which was the year that the EDM system was set up). The password was shared by at least 3 persons: 2 of the Organisation’s marketing staff and its technical support vendor. Further, it had not been changed since 2010. Investigations disclosed that there were no arrangements in place to ensure and enforce password strength, expiry and protection.

3. In the circumstances, although the means of unauthorised access to the EDM system was not determined, the evidence pointed to weak password control as the cause. The Deputy Commissioner for Personal Data Protection therefore found the Organisation in breach of section 24 of the Personal Data Protection Act 2012.

4. 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 will not issue any other directions.

5. The Organisation’s prompt co-operation in the course of the Commission’s investigation and its prompt actions taken to remediate the breach were taken into consideration in determining the quantum of the financial penalty.

## Singapore Telecommunications Limited

## [2021] SGPDPCS 7

| **Case Number** | : | Case No. DP-2007-B6607 |
| --- | --- | --- |
| **Decision Date** | : | 21 June 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Singapore Telecommunications Limited |

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

1. On 15 July 2020, Singapore Telecommunications Limited (the “**Organisation**”) informed the Personal Data Protection Commission of an incident which had occurred on or about 13 July 2020 (the “**Incident**”). In the Incident, a threat actor accessed the accounts of 17 of the Organisation’s telecommunications service subscribers to request for issuance of new SIM cards, forwarding of voice calls and/or cessation of mobile services[[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/107237.xml&queryStr=(personal%20data%20protection%20act)#fn1). Once these were issued, the affected subscribers were unable to access to their own accounts.

2. The Organisation investigations indicated that the Incident was due to threat actor(s) who gained access to its IT systems through coordinated social engineering tactics targeted at staff. The threat actor(s)’ aim was to use compromised staff accounts to gain control of subscriber accounts of the affected individuals to perform unauthorised activities.

3. The Organisation also made reports to IMDA under the Telecoms Act and the Singapore Police Force (“**SPF**”).

4. The Organisation’s investigations found no evidence that the integrity of its affected IT systems had been compromised or that any data had been exfiltrated from the systems at the time of the Incident, the Organisation had in place reasonable security arrangements that included the following:

a. Password requirements in security policies, standards and guidelines were aligned to industry best practices;

b. Systems and network enhancements were continually implemented to improve the security of applications and IT infrastructure;

c. Comprehensive and annual mandatory training was conducted for all staff in relation to the requirements under the PDPA; and

d. Reasonable security measures were in place for the work environment of all staffs based locally and overseas.

5. The Organisation took prompt action to mitigate the effects of the breach by suspending the compromised staff accounts and by password resets. Apart from exclusion from their account for a limited duration, no other loss or damage to any individual was reported from the Incident. Remedial action to prevent recurrence will remain confidential for security reasons.

6. The Deputy Commissioner for Personal Data Protection found that the Organisation had met its Protection Obligation in the circumstances. No enforcement action therefore needs to be taken in relation to the Incident.

[[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/107237.xml&queryStr=(personal%20data%20protection%20act)#fnref1) Singtel stated that the threat actor could have also accessed the records of an additional 15 subscribers.

## The Future of Cooking Pte. Ltd.

## [2020] SGPDPCS 23

| **Case Number** | : | Case No. DP-2001-B5620 |
| --- | --- | --- |
| **Decision Date** | : | 20 November 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | The Future of Cooking Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Disclosure of personal data* – *Failure to discharge obligations as data controller - Insufficient security arrangements*

1. The Future of Cooking Pte. Ltd. (the “**TFC**”) operates an e-commerce website at https://www.thermomix.com.sg (the “**Website**”), retailing kitchen appliances and accessories.

2. On 3 January 2020, the Personal Data Protection Commission (the “**Commission**”) received a complaint that a text file (the “**File**”) containing personal data was accessible via the URL: https://thermomix.com.sg/wp-content/uploads/2019/10/woocommerce-order-export-1.csv-1.txt. (the “**Incident**”).

3. The File contained the personal data of 178 unique individuals who had purchased items from the Website. The File was accessible via the URL from 1 October 2019 until 6 January 2020. It contained the following types of personal data (the “**Personal Data**”):

a. Name;

b. Email Address;

c. Billing Address;

d. Shipping Address;

e. Customer Notes (e.g. delivery instructions);

f. Order information (such as payment status, mode of payment, and transaction ID);

g. Product ID of items;

h. Quantity of items ordered; and

i. Telephone number.

**The Commission’s Findings**

***No breach by Hachi as a Data Intermediary***

4. TFC had engaged Hachi Web Solutions Pte. Ltd. (“**Hachi**”) to re-design the Website and also perform data backup and migration. Insofar as the data backup and migration activities are concerned, Hachi was TFC’s data intermediary. The cause of the breach, however, did not relate to the data processing activities but to the Website re-design. Therefore, Hachi was not in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the “**PDPA**”) by virtue of its role as a data intermediary.

***TFC in breach of the Protection Obligation***

5. The cause of the data breach may be traced to a WordPress plugin (the “**Plugin**”) which was installed on the Website. The Plugin contained a bug which caused the File to be generated and uploaded on the Website’s directory folder. Although this was a temporary file, it was accessible to the public via the URL.

6. TFC had used the Website to collect the personal data of individuals. At the time of the Incident, TFC’s database contained personal data of approximately 3,500 individuals. To discharge its Protection Obligation under section 24 of the PDPA, TFC needed to have put in place reasonable security arrangements to protect the personal data collected.

7. In this case, investigations revealed that TFC had failed to discharge its obligations as data controller when engaging Hachi to undertake data processing activities. First, TFC did not specify any requirements for Hachi to implement any data protection measures to be implemented in the Website, whether in its contract with Hachi or other project documentation. Second, TFC did not conduct any pre-launch security testing (such as vulnerability assessments) on the Website. Had security testing been conducted, TFC would have been able to detect the presence of the publicly accessible temporary file, even if it was unaware of the bug in the Plugin that caused it.

8. Once it knew about the Incident, TFC and Hachi removed the Plugin and disabled the public’s access to the relevant directory folder. Hachi also contacted the developers of the Plugin, who acknowledged the existence of the bug and fixed the bug in an updated version. TFC subsequently engaged a vendor to perform penetration testing and other measures to enhance the security of the Website.

9. The Deputy Commissioner found TFC in breach of the Protection Obligation under section 24 of the PDPA. After considering the circumstances of the Incident, including according mitigatory weight to TFC’s cooperation with the Commission during investigations and the remedial action taken by TFC after the Incident, the Deputy Commissioner directs TFC to pay a financial penalty of $9,000 for its breach.

10. TFC must make payment of the financial penalty 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 it is paid in full.

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

## Interauct! Pte Ltd

## [2020] SGPDPCS 16

| **Case Number** | : | Case No. DP-1911-B5268 |
| --- | --- | --- |
| **Decision Date** | : | 03 August 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Interauct! Pte Ltd |

*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. Interauct! Pte Ltd (the “**Organisation**”) operated an online mobile number auction (the “**Auction**”) for a telecommunications provider (the “**Telco**”). This arrangement started in the year 2000 and ended in 2018.

2. In November 2019, the Commission was informed that the Telco’s cybersecurity team had located an internet sub-domain containing files with the personal data of individuals who had participated in the Auction (the “**Files**”). The Files contained the following types of personal data:

a. Name;

b. ID (such as passport or NRIC number);

c. Mobile number;

d. Address;

e. Date of birth; and

f. Email address.

3. The Commission’s investigations revealed the following:

a. The Organisation had engaged a vendor to provide web hosting services for the Auction. In 2012 and 2016, the vendor conducted server migration exercises. On both occasions, the Organisation created backups of the Files prior to server migration exercises and uploaded them on the vendor’s servers. The Organisation did not delete the Files after the server migration were completed;

b. In April 2019, the vendor misconfigured its servers. As a result, the Files became accessible on the internet sub-domain. However, to access this sub-domain requires an individual to key in either one of two URLs exactly. Both URLs were complex and lengthy. It was therefore difficult for an individual to determine the URLs exactly to enter the sub-domain. Indeed, an examination of server logs found that only the Telco had accessed the sub-domain;

c. The Files contained a mix of individuals’ personal data, as well as dummy data used for testing purposes. An analysis of the Files showed that there were approximately 8,750 individuals’ personal data contained in them. The Telco compared the data with its customer records, and via a reconciliation process, was able to identify 3,380 individuals as its customers. In this regard, the Telco informed that it would have been very difficult for a third party, without access to the Telco’s customer records, to carry out such a reconciliation exercise. This means that even if an individual had accessed the Files, it would have been difficult to him to identify the individuals from the personal data in the Files;

d. The Organisation deleted the Files within three hours of the Telco notifying the Organisation of their discovery of the internet sub-domain. The Organisation had also ensured that the vendor fixed the misconfiguration of the servers, which was done within six hours of the discovery of the internet sub-domain.

4. The Deputy Commissioner for Personal Data Protection (the “**Deputy Commissioner**”) finds that the Organisation had put in place, via the vendor, reasonable security arrangements to protect the personal data. In particular, the security arrangements in place would have prevented direct access by unauthorised third-parties to the Files hosted on the server. This had greatly reduced the potential adverse impact of the incident.

5. However, the Organisation admitted that there was no reason to retain the Files after the migration exercises were completed. If the Files had been duly deleted, the personal data in the Files would not have been compromised in the first place. The Deputy Commissioner therefore finds the Organisation in breach of the Retention Limitation Obligation under section 25 of the Personal Data Protection Act 2012.

6. After considering the facts and circumstances of the incident, including the fact that the personal data in the Files was ultimately not exposed, the Deputy Commissioner has decided to issue a warning to the Organisation for the breach of the Retention Limitation Obligation. No other direction is required as the breach has been remedied.

## North London Collegiate School (Singapore) Pte. Ltd.

## [2021] SGPDPCS 14

| **Case Number** | : | DP-2107-B8562 |
| --- | --- | --- |
| **Decision Date** | : | 01 December 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | North London Collegiate School (Singapore) Pte. Ltd. |

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

1. On 2 July 2021, North London Collegiate School (Singapore) Pte. Ltd. (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) that a parent of a student was able to view and access a student report by the Organisation by performing searches using internet search engines. (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 Data Protection Act (the “**PDPA**”).

3. Investigations revealed that, from December 2019 to July 2021, parents of prospective students could submit documents for admission applications via the Organisation’s website (https://nlcssingapore.sg/). All submitted documents were stored in a directory/ folder of the website. However, the website directory/ folder was not adequately secured from automatic indexing by web crawlers. As a result, the submitted documents were indexed by search engines and could show up in online search results.

4. The table below summarises[[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/108719.xml&queryStr=(personal%20data%20protection%20act)#fn1) the number of affected individuals for each type of document accessible in the directory/ folder (the “**Compromised Documents**”):

| **S/N** | **Type of Document (Scanned or Electronic Copies)** | **Number of Individuals Affected** |
| --- | --- | --- |
| 1 | Passport | 1,742 |
| 2 | Identity cards (i.e NRICs) | 1,714 |
| 3 | Digital Photographs of applicants | 720 |
| 4 | Birth Certificates | 709 |
| 5 | Academic Reports | 676 |
| 6 | Immunization Records | 670 |

5. The documents above contained the following types of personal data (the “**Personal Data Sets”)** at risk of unauthorised access in the Incident - Name, Address, NRIC number, Passport Number, Photograph, Date of Birth, immunization details and academic details.

6. The Organisation admitted that it had only relied on a Robots.txt file deployed on its Website to instruct search engines to refrain from indexing the documents in the website directory folder. However, it is well established that the robots exclusion protocol is not mandatory, in the sense that it relies on compliance of web crawlers without an enforcement mechanism. Therefore, Organisations storing personal data in website directory/ folders should instead implement proper folder or directory permissions and access controls to prevent unintended access by web crawlers.

7. In addition, the Organisation had stated that it relied on a related group company to setup and manage its website, including to make the necessary security arrangements to protect any personal data collected. However, in this case, there were no clear business requirements (e.g. contractual stipulations) specifying that the Organisation was relying on the sister company to recommend and/or implement security arrangements to protect personal data that resides in the website directory/ folder.

8. *Everlast Projects Pte Ltd & Others* [2020] SGPDPC 20 stated the arrangements to be made when organisations in a group used IT services provided by a group member. An organisation receiving IT services from another organisation of the group should ensure that the latter is bound by either written agreements or group rules to protect personal data in the course of provision of the services. Absent clear written personal data protection requirements of the group member managing the Organisation’s website, the responsibility to make reasonable security arrangements to protect the Affected Personal Data in the directory/ folder of the website remained squarely with the Organisation.

9. 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**”).

10. Following the incident, the Organisation ceased the collection of documents via its website and would now be utilizing a specialized school admission software to manage the application process and the personal data submitted. Additionally, the Organisation would be implementing appropriate binding corporate rules to govern the centralization of corporate functions and the handling of data protection and cybersecurity within its corporate group.

11. The Organisation cooperated with the Commission’s investigations, admitted to its breach of the Protection Obligation and took prompt remedial actions to address its inadequacies in its processes. There were also no indications that that the personal data affected in the Incident had been misused in any form. However, personal data of minors were at risk of unauthorised access.

12. 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 requires the Organisation to pay a financial penalty of $10,000 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.

13. In view of the remedial actions taken by the Organisation, no other directions 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/108719.xml&queryStr=(personal%20data%20protection%20act)#fnref1) This table sets out the documents at risk of unauthorised access in the Incident. Not all of these types of documents were affected for each Affected Individual, and the documents affected for each Affected Individual varies. A unique Affected Individual could have multiple type of documents affected.

## Thomson Medical Pte. Ltd.

## [2022] SGPDPCS 15

| **Case Number** | : | DP-2010-B7246 |
| --- | --- | --- |
| **Decision Date** | : | 29 December 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Thomson Medical Pte. Ltd. |

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

1. On 26 October 2020, the Personal Data Protection Commission (the **“Commission”**) was notified that the Thomson Medical Pte. Ltd. (the **“Organisation”**) Health Declaration Portal was not secure, enabling public access to the personal data of visitors (the “**Incident**”) stored in a **CSV** (comma separated values) file.

2. Visitor data collected on the Organisation’s Health Declaration Portal had been stored concurrently in a publicly-accessible CSV file as well as a secured database from 16 April 2020, when the health declaration portal was first used by the Organisation to 8 September 2020, when the storage of the visitor data was changed to only the secured database instead of the CSV file. The CSV file was hosted on the Organisation’s web server.

3. The Organisation admitted that, contrary to the instructions given to the employee to switch the data storage from the CSV file to secured database exclusively, and the organisation’s protocols, its in-house developer had omitted to remove a software code, causing the visitor data to be stored in the CSV file and the same in-house developer had omitted to change the default web server configuration, thereby allowing public access to the hosted CSV file. The switch to storage in a secured database would have ensured access controls by requiring user login ID and secure password protection, as well as encryption of data transfers using SSL certificates. The access controls would ensure that only authorized users would be able to access the data.

4. The Commission’s investigations revealed that the affected CSV file contained the personal data of 44,679 of the Organisation’s visitors, including the date and time of visit, temperature, type of visitor (purpose of visit), name of visitor, name of newborn, contact number, NRIC/FIN/passport number, doctor/clinic name or room visiting, and answers to a health declaration questionnaire (which included a declaration by the visitor that he/she did not have any symptoms or recent exposure to the Covid-19 virus).

5. The Organisation accepted that it was in breach of the Protection Obligation under section 24 of the Personal Data Protection Act (“PDPA”). The Commission finds that the Organisation had breached section 24 of the PDPA for two reasons.

6. First, even though the Organisation’s existing policies required the visitor data collected to be stored in a secured database, the Organisation failed to ensure that there were processes in place to ensure these policies and instructions would be complied with. The Organisation stated that the in-house developer had been the only staff in its IT department familiar with the programming language used for the health declaration form. This, however, should not have prevented the Organisation, as an example, from requiring the in-house developer to demonstrate to another staff member, and for that staff member to verify that the storage instructions had been complied with. As noted in *Re Aviva Ltd* [2017] SPDPC 14, relying solely on individual employees to perform their tasks diligently, with no oversight or supervision, is not a reasonable security arrangement.

7. Second, the Organisation failed to conduct reasonable pre-launch testing before the Health Declaration Portal went live. While acceptance testing and some technical tests were conducted, there had been no security testing to verify that there were access controls to the visitor data collected.

8. Having said that, it is a mitigating fact that the Organisation’s in-house developer sought to comply with the Organisation’s policies and swiftly rectified the software code on 8 September 2020, when he first discovered the coding error whilst updating the health declaration questionnaire.

9. The forensic investigator engaged by the Organisation did not uncover any evidence that the disclosed data had been exported and posted online, including on the Dark Web. The Organisation’s server logs also revealed that the CSV file was only accessed 4 times from 3 different local IP addresses. Given the timing of the access instances, it is probable that these instances were made by the complainant and by the Commission when investigating this matter, which suggests that the impact of this Incident was limited.

10. The Commission noted a parallel between the facts of this case and *Re Spear Security Force Pte. Ltd.*  [2016] SGPDPC 12, in that both cases arose from a single complaint about a potential breach of the PDPA, with no other evidence suggesting that the personal data had actually been exposed to unauthorised third parties due to the lapses by the Organisation.

11. The personal data exposed here included the clinic or room that the individual intended to visit, and the reason for the visit. This could be to seek treatment, accompany a patient, or a business visit made by a sales representative of a pharmaceutical or medical device company. While the personal data exposed included some health-related information, this had essentially been health declaration information for the purpose of containment of the pandemic. The information did not in fact reveal any potentially sensitive information such as whether the visitor was Covid-19 positive.[[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/110546.xml&queryStr=(personal%20data%20protection%20act)#fn1)

12. The personal data disclosed is also not on par with *Re Singapore Health Services Pte. Ltd.& Ors.* [2019] SGPDPC 3 (“Singhealth”). In the Singhealth case, we recognised the sensitivity involved in the exposure of the affected individuals’ personal data in their “clinical episode information, clinical documentation, patient diagnosis and health issues and Dispensed Medication Records” as the information and personal data affected may allow one to deduce the condition for which a patient had sought treatment, and may lead to the unintended disclosure of serious or socially embarrassing illnesses.[[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/110546.xml&queryStr=(personal%20data%20protection%20act)#fn2) While there is some personal data in the present case which may reveal the clinic which an affected individual had sought treatment, this is of a much more limited scope as compared to the Singhealth case.

13. The Commission accepted that the Organisation took prompt remedial action to contain the exposure. This include removing the affected CSV file and changing all the passwords to the database, even though it was not affected by the Incident. To prevent a recurrence of a similar incident, the Organisation also reviewed its application deployment process to take into consideration data security, and rectified all potential gaps discovered during a vulnerability scan.

14. Given the lack of evidence suggesting that personal data had actually been exposed to unauthorised third parties due to the lapses by the Organisation and the limited impact of the Incident, the Commission considered that it would be most appropriate in lieu of imposing a financial penalty, to impose directions.

15. Another factor which prompted the Commission to impose directions in lieu of a financial penalty was the fact that at the material time, such health declaration information was widely collected across the island. There was also a corresponding acceptance and support from members of the public of the need for the collection of such health declaration information in order for the relevant authorities to effectively respond to and control the potential spread of COVID-19.

16. Given the above, the Commission directs the Organisation to carry out the following within 60 days:

a. In relation to the Organisation’s remedial action of reviewing its application deployment process to take into consideration data security,

i. The Organisation shall ensure that the intended measures include arrangements for reasonable pre-launch security testing to be conducted before the launch of any new website, application, portal or other online feature for the processing of personal data; and

ii. The Organisation shall ensure that the intended measures include the development and implementation of a data retention policy to meet the Retention Limitation Obligation under section 25 of the PDPA.

b. In relation to the Organisation’s remedial action of scanning the Dark Web for evidence of exfiltration of the personal data,

i. The Organisation shall conduct a scan of the Clear/Surface Web, as well as a renewed scan of the Dark Web to confirm that there is no evidence of publication of the affected personal data online.

c. By no later than 14 days after the above actions have been carried out, the Organisation shall submit to the Commission a written update providing details of the actions taken.

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

**Protection Obligation**

**24(a)** Failure to 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

[[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/110546.xml&queryStr=(personal%20data%20protection%20act)#fnref1) Cf *Re Terra Systems Pte Ltd* [2021] SGPDPC 7.

[[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/110546.xml&queryStr=(personal%20data%20protection%20act)#fnref2) See *Re Singapore Health Services Pte. Ltd.& Ors.* [2019] SGPDPC 3, at [139].

## Novelship Pte. Ltd.

## [2020] SGPDPCS 15

| **Case Number** | : | Case No. DP-1905-B3820 |
| --- | --- | --- |
| **Decision Date** | : | 22 July 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Novelship Pte. Ltd. |

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

1. Novelship Pte. Ltd. (the “**Organisation**”) operates an e-commerce website for individuals to sell or buy luxury brands of streetwear (the “**Website**”). To create a buyer or seller account on the Website, individuals would have to provide their personal data to the Organisation. The Organisation does not, in usual course, reveal the personal data it had collected to any buyer or seller transacting on the Website. Instead, the Organisation, together with an external payment processor, facilitates transaction payments on behalf of the parties.

2. On 1 May 2019, the Personal Data Protection Commission (the “**Commission**”) received information that a registered seller (“**User**”) was able to gain unauthorised access to the personal data of other sellers by employing software tools and manipulating the public URLs of active listings (“the “**Incident**”).

3. The User had accessed the personal data of six unique sellers who had active listings at the time of the Incident. The personal data concerned included: (i) first and last names; (ii) email addresses; (iii) shipping addresses; (iv) hashed account passwords; and (v) the name of bank and bank account numbers (“**Personal Data Sets**”). No buyer data was accessed in the Incident.

4. Investigations revealed that the Organisation had not conducted adequate security testing before the launch of the Website. The testing it had conducted was limited to design and functionality issues, such as verifying the password hashing and password requirement functions. **Critically, the Organisation should have—but had not—conducted vulnerability scanning**. Vulnerability scanning that is reasonably and competently conducted should include scanning for OWASP Top Ten, i.e. the top 10 security vulnerabilities listed by the Open Web Application Security Project (“**OWASP**”). The vulnerability of URLs to manipulation is within the OWASP Top 10, and would have been detected if the Organisation had conducted adequate vulnerability testing.

5. The Commission understands that not every organisation is equipped with adequate knowledge of cyber security risks or the ability to conduct security testing. However, the obligation of organisations to protect the personal data they collect and process online cannot depend on their subjective familiarity with the security risks or ability to prevent them. Organisations are expected to engage qualified competent parties, where reasonably needed, to assist them to discharge their obligation to protect personal data. When doing so, organisations can refer on the technical advice and expertise of their service provider, but remain ultimately responsible for articulating the business risks they wish to avoid and business outcomes that they seek to achieve.

6. Similarly, the Commission recognises that organisations may face financial, manpower and technical limitations. These limitations are relevant in establishing the reasonableness of decisions they have taken, but cannot allow an organisation to justify providing a level of protection that is below what is reasonable for the type of personal data it collects and processes.

7. Accordingly, 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.

8. Having considered the representations made by the Organisation and the material factors, in particular:

(a) the sellers’ personal data would have been at risk of unauthorised access for a period of eight months (from the time the sellers were first allowed to sell on the Website, to the date remedial actions were taken);

(b) there was actual unauthorised access of the Personal Data Sets of six individuals by the User;

(c) the remedial measures taken by the Organisation upon being made aware of the Incident; which included fixing the vulnerability to ensure that the sellers’ personal data would no longer be accessible to unauthorised persons, redacting all user information relating to bank information, and the Organisation committing to developing a new website; and

(d) the adverse impact the COVID-19 pandemic had on the Organisation’s business;

the Deputy Commissioner for Personal Data Protection directs that the Organisation pays a financial penalty of S$4,000 for the contravention. The Organisation must make payment of the financial penalty 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 it is paid in full. No other directions are required as the Organisation had implemented the necessary remedial measures.

## Budgetcars Pte. Ltd.

## [2022] SGPDPCS 13

| **Case Number** | : | DP-2108-B8798 |
| --- | --- | --- |
| **Decision Date** | : | 06 July 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Budgetcars Pte. Ltd. |

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

1. On 25 August 2021, the Personal Data Protection Commission (the “**Commission**”) received a complaint that the delivery tracking function (the “**Tracking Function Page**”) on the website of Budgetcars Pte Ltd (the “**Organisation**”) could be used to gain access to the personal data belonging to another individual. By changing a few digits of a Tracking ID, the complainant could access the personal data of another individual (the “**Incident**”).

2. The Organisation is a logistics company delivering parcels to customers (“**Customers**”) on behalf of retailers (“**Retailers**”).

3. The personal data of 44,357 individuals had been at risk of unauthorised access. The datasets comprised name, address, contact number and photographs of their signatures.

4. The Tracking Function Page was set up in December 2020 to allow Retailers and Customers to (i) keep track of the delivery status of their parcels; and (ii) confirm the identity of individuals to collect parcels on their behalf (where applicable). The Tracking IDs were generated by Retailers and comprised either sequential or non-sequential numbers. Although generated by Retailers, the Organisation adopted the Tracking IDs for use on its own Tracking Function Page that allowed their customers to track their deliveries, which would disclose personal data listed above. The Protection Obligation therefore required the Organisation to ensure that there were reasonable access controls in its use of the Tracking IDs for giving access to an individual’s personal data.

5. The risk of unauthorised access to personal data from altering numerical references, both sequential and non-sequential, have featured in the published decisions of the Commission in *Re Fu Kwee Kitchen Catering Services* [2016] SGPDPC 14, and more recently, in *Re* *Ninja Logistics Pte. Ltd.* [2019] SGPDPC 39. Insecure direct object reference has long been a well-known security risk to personal data. The Organisation failed to have reasonable access control to the affected individuals’ personal data when it simply adopted Tracking IDs generated by the Retailers without factoring in this risk.

6. The Organisation also admitted that it did not have in place a process to protect personal data through proper safeguards by archiving personal data relating to a completed delivery order after a reasonable period of time has lapsed. To reduce the risk of access to personal data through frontend applications, they should be removed and archived within a reasonable time. The Organisation’s failure to do so resulted in more personal data at risk in the Incident than should have been the case.

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

8. Upon being notified by the Commission of the Incident, the Organisation took the following remedial measures after the Incident:

a. Removed all personal data from the Tracking Function Page;

b. Engaged its IT solutions provider to re-examine management of the Tracking Function Page;

c. Post-delivery expiry of Tracking ID after 14 days; and

d. Implemented checks to prevent sequential Tracking IDs from being uploaded onto the Tracking Function Page.

9. 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 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**”).

10. In *Re Ninja Logistics Pte. Ltd.* cited above, the organisation had been aware of the risk from manipulation of Tracking IDs. However, a counter-measure which the organisation initially introduced was abandoned due to operational issues and was not replaced. This resulted in a significantly larger dataset (>1.2 million) that was exposed to the risk of unauthorised access over a period of close to 2 years. In comparison, the number of affected individuals in the present case was lower as the Organisation was only handling deliveries for a few Retailers at the time of the Incident.

11. 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; and (ii) the prompt remedial action undertaken by the Organisation, the Commission considered that it would be appropriate not to require the payment of a financial penalty but to direct the Organisation to do the following:

a. To put in place the appropriate contractual provisions to set out the obligations and responsibilities of both the data controller and data intermediary to protect the Organisation’s personal data, and the parties’ respective roles in protecting the personal data;

b. 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 website that contains personal data in the Organisation’s possession or control;

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

d. 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

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

## Hello Travel Pte. Ltd.

## [2020] SGPDPCS 20

| **Case Number** | : | Case No. DP-2004-B6189 |
| --- | --- | --- |
| **Decision Date** | : | 30 October 2020 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Hello Travel Pte. Ltd. |

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

1. On 8 April 2020, the Personal Data Protection Commission (the “**Commission**”) received information that a database belonging to Hello Travel Pte Ltd (the “**Organisation**”) was posted on an internet forum and was thus made publicly available (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 compromised database contained the personal data of approximately 71,002 users who had created accounts at the Organisation’s website ([www.havehalalwilltravel.com](https://www.havehalalwilltravel.com/)) from February 2015 to July 2018. The disclosed personal data included their name, email address, date of birth, nationality and phone number. The table below summarises the number of affected individuals for each corresponding type of personal data disclosed:

| **S/N** | **Type of Personal Data** | **Number of Individuals Affected** |
| --- | --- | --- |
| 1 | Name | 71,002 |
| 2 | Email Address | 57,693 |
| 3 | Phone Number | 453 |
| 4 | Date of Birth | 946 |
| 5 | Nationality | 20,754 |

4. The Organisation’s internal investigations pointed to a possible hack as the cause of the Incident. Sometime in year 2018, the server instance which hosted the Organisation’s website and the database became corrupted and unusable after the installation of a free open source wordpress plugin. The Organisation believed that unknown parties could have exploited vulnerabilities of the installed plugin at that time and exfiltrated the database.

5. The Organisation admitted that it did not give due attention to personal data protection and had neglected to put in place basic procedural and technical security arrangements to protect the personal data in its possession and control. As examples, it did not have the relevant policies and/or protocols in place to perform regular system patching or to conduct security assessment and/or testing when making changes to its ICT systems.

6. 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**”).

7. Following the incident, the Organisation implemented technical measures to secure its systems from potential vulnerabilities. The personal data of its members were also encrypted immediately. Additionally, the Organisation had engaged relevant parties to take down the compromised database and informed the affected individuals of the Incident.

8. In determining the directions, if any, to be imposed on the Organisation. The Deputy Commissioner took into account the following factors:

Aggravating factors

(a) The high number of individuals affected;

(b) The fact that personal data was exfiltrated and posted online; and

(c) The Organisation did not put in place basic procedural and technical security arrangements.

Mitigating factors

(a) The Organisation had cooperated with the investigation;

(b) The Organisation’s upfront voluntary admission of liability to a breach of the Protection Obligation under the PDPA;

(c) The Organisation’s prompt remedial actions at [7] to address the inadequacies in its procedures and processes; and

(d) There was no evidence that the personal data affected in the Incident had been misused in any form.

9. In the course of settling this decision, the Organisation made representation on the amount of financial penalty which the Commission intends to impose and requested that the financial penalty to be paid in instalments. The Organisation raised the following factors for the Commission’s consideration:

(a) The Organisation had been suffering substantial loss due to the impact to the travel industry by the Covid-19 pandemic; and

(b) The Organisation had already spent quite a substantial amount of money to fix the security breach.

10. Having carefully considered the representations, the Deputy Commissioner has decided to reduce the financial penalty to the amount set out in [11a] and is agreeable for the financial penalty to be payable in instalments. The quantum of financial penalty has been calibrated after due consideration of the Organisation’s financial circumstances due to the unprecedented challenges faced by businesses amid the current Covid-19 pandemic, bearing in mind that financial penalties imposed should not be crushing or cause undue hardship on organisations. Although a lower financial penalty has been imposed in this case, the quantum of financial penalty should be treated as exceptional and should not be taken as setting any precedent for future cases.

11. Taking into account all relevant facts and circumstances, the Deputy Commissioner hereby directs the Organisation to:

(a) Pay a financial penalty of $8,000 in 10 instalments by the due dates as set out below, failing which, the full outstanding amount shall become due and payable immediately and 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:

i. 1st instalment of $800 on 1 January 2021;

ii. 2nd instalment of $800 on 1 February 2021;

iii. 3rd instalment of $800 on 1 March 2021;

iv. 4th instalment of $800 on 1 April 2021;

v. 5th instalment of $800 on 1 May 2021;

vi. 6th instalment of $800 on 1 June 2021;

vii. 7th instalment of $800 on 1 July 2021;

viii. 8th instalment of $800 on 1 August 2021;

ix. 9th instalment of $800 on 1 September 2021; and

x. 10th instalment of $800 on 1 October 2021

12. In view of the remedial actions taken by the Organisation, the Deputy Commissioner will not be issuing any other directions.

## Trinity Christian Centre Limited

## [2022] SGPDPCS 3

| **Case Number** | : | DP-2009-B7057 |
| --- | --- | --- |
| **Decision Date** | : | 21 April 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Trinity Christian Centre Limited |

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

1. On 11 March 2021, Trinity Christian Centre Limited (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) that its database servers containing personal data were infected with ransomware on or around 17 February 2021 (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 Data Protection Act (the “**PDPA**”).

**The Incident**

3. The Organisation runs Trinity Christian Church in Singapore.

4. At the time of the Incident, the database servers contained 72,285 individuals’ data. The types of data affected for each individual varied, and included at times an individual’s name, full identification number, residential address, contact number, email address, photograph, date of birth, age, marital status, education level, and/or description of medical condition (if applicable).

5. Investigations by the Organisation revealed that the Organisation maintained an open and publicly exposed remote desktop protocol port. This allowed a threat actor with access to compromised administrator account credentials to enter the Organisation’s network and database servers to execute ransomware attack on 17 February 2021, rendering the databases inaccessible.

6. The Organisation managed to restore the affected databases from its back-up copies. Based on the Organisation’s investigations, there was no evidence to suggest that the threat actor exfiltrated the Organisation’s databases.

**The Organisation’s Admission**

7. The Organisation admitted that it had breached the Protection Obligation under section 24 of the PDPA as:

a. It could have implemented separate access controls (i.e. separate logins) to protect the databases containing personal data; and

b. The initial unauthorised entry to the Organisation’s network was through an administrator account that the Organisation had assigned to an IT vendor it had engaged to develop and test applications. The Organisation conceded that it failed to stipulate data protection requirements on its vendor.

**Remediation**

8. Following the Incident, the Organisation notified its church members on 8 April 2021. The Organisation changed all user and administrator passwords, closed all unused and open ports used for remote access and restricted logon access with domain administrator privileges to servers and workstations. A security review was also conducted and the Organisation implemented real time threat monitoring, detection, and response measures.

**The Commission’s Decision**

9. As noted earlier, the Organisation admitted that it was in breach of section 24 of the PDPA as it could have implemented separate access controls to protect the databases containing personal data. In our view, the number and type of personal data sets in the possession or under the control of the Organisation created a security need for stronger access control beyond reliance on frontend password protection. Indeed, with increasingly sophisticated phishing and social engineering techniques, adding another layer of protection to protect backend database servers, and manage the risks that frontend login credentials may be compromised was a reasonable security measure, which the Organisation also accepted.

10. The Commission had also previously emphasised in our 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/109079.xml&queryStr=(personal%20data%20protection%20act)#fn1) and in the Commission’s Guide to Managing Data Intermediaries that organisations that engage IT vendors should ensure that their IT vendors are aware of the need for personal data protection by making it part of their contractual terms.

11. The Organisation admitted that its contract with its IT vendor only contained a general confidentiality clause not to disclose information obtained without the Organisation’s prior written consent. Even though the Organisation was well aware that its IT vendor would process personal data, the Organisation failed to stipulate within the contract any requirements on the vendor to protect the church members’ personal data, thereby breaching section 24 of the PDPA.

12. In determining the directions to be imposed on the Organisation for the breach, the Commissioner took into account the following factors:

**Aggravating**

(a) The high number of affected individuals of 72,285 which included approximately 8,300 minors;

(b) The nature of the affected data. In particular, the affected databases contained descriptions of medical conditions provided by individuals counselling services and overseas mission applications. Individuals would expect a high level of confidence when they convey such information to the Organisation for handling;

**Mitigating**

(c) The Organisation’s upfront admission of breach of the Protection Obligation, and the prompt remedial actions to mitigate the effects and prevent recurrence of the Incident; and

(d) There was no evidence of exfiltration of the Organisation’s databases.

13. On account of the above, the Organisation is directed to pay a financial penalty of $20,000 within 30 days from the date of this direction. In view of the remedial action of the Organisation, the Commission will not be issuing any other directions.

[[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/109079.xml&queryStr=(personal%20data%20protection%20act)#fnref1) See examples – Jigyasa [2020] SGPDPC 9, MDIS Corporation Pte Ltd [2020] SGPDPC 11 and Civil Service Club [2020] SGPDPC 15.

## Breach of the Top Mobile Gallery (BR)

## [2024] SGPDPCS 1

| **Case Number** | : | DP-2208-C0053 |
| --- | --- | --- |
| **Decision Date** | : | 01 March 2024 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Tok Leng Leng (trading as Top Mobile Gallery (BR)) |

*Data Protection* – *Protection obligation* – *Unauthorised use of and access to personal data* – *Insufficient administrative security arrangements and lack of access controls*

**Introduction**

1. Between the period December 2020 to April 2021, the Personal Data Protection Commission (“the **Commission**”) received 435 Do Not Call (“**DNC**”) complaints relating to property messages, despite their numbers being registered with the DNC Register. The complaints were traced to 44 M1 pre-paid SIM cards sold by Tok Leng Leng (trading as Top Mobile Gallery (BR)) (“**Organisation**”), located in a foreign worker dormitory at 2 Seletar North Link.

2. The Commission commenced investigations into the Organisation for suspected breaches under the Personal Data Protection Act 2012 (“**PDPA**”).

**Facts of the Case**

3. The 44 M1 pre-paid SIM cards were registered under 33 unique individuals who were foreign workers. Investigations confirmed that these foreign workers lived in the dormitory at 2 Seletar North Link, and had purchased pre-paid SIM cards from the Organisation. Additional pre-paid SIM cards were registered under their names even though they had not in fact purchased these SIM cards (the **“illicit SIM cards**”).

4. As a retailer of M1 SIM cards, the Organisation used a terminal device issued by M1 for the purposes of SIM card registration. The SIM card registration process with the M1 terminal device was as follows:

a. First, the customer’s identity document (e.g. identity card, passport, work pass etc.) would be scanned using the terminal device, which is connected directly to M1’s registration system. The system would capture the customer’s particulars, and whether the customer had reached the limit of 3 pre-paid SIM cards.

b. Next, the barcode of the SIM card(s) would be scanned so that they could be tagged to the registered customer.

c. Finally, the retailer would use a mobile application to load credit value to the prepaid SIM card(s) to activate them for usage. This was done in the Organisation’s premises. M1’s policy was for each prepaid M1 SIM card to have a zero-initial balance, and for retailers to load some or all the money paid by the customer.

5. At a certain point in time, the Organisation started registering M1 pre-paid SIM cards via a M1 mobile application on a mobile phone.

6. As the Organisation registered M1 pre-paid SIM cards by scanning the front and back of the affected individuals’ work permits, the following types of personal data was affected:

a. Name;

b. Sex;

c. FIN / work permit number;

d. Date of Birth;

e. Nationality; and

f. Name of employer.

**Findings and Basis for Determination**

7. Section 2(1) of the PDPA defines an “*organisation”* to include “*any individual, company, association or body of persons, corporate or unincorporated*”. The Organisation is a sole proprietorship and has no separate legal personality from Tok Leng Leng (“**TLL**”). Accordingly, TLL (trading as Top Mobile Gallery (BR)) is an organisation for the purposes of the PDPA.

8. Based on the circumstances set out above, the Commission’s investigation centered on whether the Organisation had breached the Protection Obligation under section 24 of the PDPA.

*The Protection Obligation under section 24 of the PDPA*

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 (the “**Protection Obligation**”).

10. During investigations, the Organisation admitted to a breach of section 24 of the PDPA. TLL, the sole proprietor of Top Mobile Gallery (BR), accepted that she failed to have security arrangements in place to protect against the unauthorised use of and access to customers’ personal data for registration of M1 pre-paid SIM cards:

a. First, TLL admitted that she could have but failed to maintain an inventory of M1 pre-paid SIM cards. TLL explained that in contrast to the SIM cards sold by other retailers such as Singtel or Starhub which came with a pre-paid balance, M1 pre-paid SIM cards came with zero initial-balance. This contributed to her omission to maintain an inventory. Furthermore, the M1 salesperson did not have a fixed schedule for delivering the pre-paid SIM cards to the Organisation and would deliver more pre-paid SIM cards to the Organisation sporadically, which her employees would then acknowledge receipt.

b. Second, TLL admitted that she failed to have processes in place that would require the employees to account for each M1 pre-paid SIM card sold and to whom the pre-paid SIM card was registered. TLL admitted that all her employees had equal access to the M1 pre-paid SIM cards. The Deputy Commissioner notes that the Organisation could have maintained a record of the name of the employee who sold each pre-paid SIM card, the date, time and place of registration, and sufficient particulars of the individual to whom the SIM card was sold and registered to.

c. Third, TLL alluded in her statements of how her employees enjoyed the same “access” to register the pre-paid SIM cards. This was corroborated by an employee, who stated that the login credentials to the M1 application used for registration of pre-paid SIM cards was shared amongst the employees, and that the employees would login to the M1 application on their personal mobile devices if the Organisation’s mobile device was not readily available. In the Deputy Commission’s view, the Organisation’s failure to implement access control restrictions and to prohibit the sharing, amongst its employees, of the login credentials to the M1 mobile application used to register pre-paid SIM cards made it much easier for the employees to turn rogue, as it became harder to detect the errant employee.

d. TLL also admitted that there was little or no supervision over the Organisation’s employees regarding how they used or accessed the customers’ personal data. She was often not at the shop and left the shop to be managed by her employees. While there was CCTV footage installed at the Organisation, she did not review the CCTV footage often.

11. For the reasons set out above, the Deputy Commissioner finds the Organisation in breach of the Protection Obligation under section 24 of the PDPA as there has been a complete failure to adopt any security arrangements to protect the customers’ personal data from misuse.

**The Deputy Commissioner’s Preliminary Decision**

12. In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and the amount of any such financial penalty, the matters set out at section 48J(1) and the factors listed at section 48J(6) of the PDPA were taken into account.

13. In addition, the Deputy Commissioner also considered the following factors which would justify an increase or decrease in the financial penalty:

Factors that justify an increase in the financial penalty

a. The Organisation’s breaches of the PDPA had caused inconvenience to other innocent parties. The illicit SIM cards sold by the Organisation were used to send unsolicited messages to phone numbers that were registered with the DNC Register.

b. Even though TLL denied knowledge of any wrongdoing on the part of her employees, TLL has been the registered sole-proprietor of Top Mobile since 2014. She ought to have been aware of the practice of registering illicit SIM cards. The Organisation’s lackadaisical attitude towards preventing the potential misuse of individuals’ personal data and failure to introduce reasonable safeguards displayed a higher level of culpability.

Factors that justify a decrease in the financial penalty

c. The Organisation admitted to its contravention to the PDPA and co-operated fully with the investigation process.

d. This is the first incident of a personal data breach by the Organisation.

14. Having considered the above factors and circumstances, the Commission preliminarily determined that a financial penalty of $7,000 would be imposed in respect of the Organisation’s contravention of the Protection Obligation. On 23 November 2023, the Organisation was notified of the Commission’s preliminary decision, including the full findings set out above, and given 14 days to make written representations.

**Representations Made by the Organisation**

15. While the Organisation did not challenge the findings and bases of the contravention, the Organisation made representations to the Commission seeking that a financial penalty not be imposed, summarised as follows:

a. TLL, as the sole proprietor of Top Mobile Gallery (BR), admitted that as the boss it was her fault in failing to realise that her staff had misappropriated the information provided by the customers in time;

b. The Organisation had been in business since 2014 and had always complied with applicable laws and regulations. Effectively, this is the Organisation’s first contravention of the PDPA;

c. The financial penalty of $7,000 is a hefty amount for the Organisation.

16. The Commission considered the representations made carefully but was unable to accept them for the following reasons:

a. The Commission had already taken into account the first two factors raised by the Organisation, in arriving at the preliminary decision;

b. The Organisation had not substantiated to the Commission that it is experiencing financial difficulties and would be unable to continue with its usual business activities following the imposition of the financial penalty.

17. Having considered all the relevant circumstances of this case, the Commission hereby requires the Organisation to pay a financial penalty of $7,000 within 30 days from the date of the relevant notice accompanying this decision.

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

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(a).** An organisation 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.

## Royal Caribbean Cruises (Asia) Pte. Ltd.

## [2022] SGPDPCS 4

| **Case Number** | : | DP-1804-B1931 |
| --- | --- | --- |
| **Decision Date** | : | 13 August 2019 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Royal Caribbean Cruises (Asia) Pte. Ltd. |

*Data Protection* – *Protection obligation* – *Unauthorised disclosure of personal data* – *No breach* – *Coding error not within organisation’s operations or business functions*

1. On 5 April 2018, the Personal Data Protection Commission (“**Commission**”) commenced investigation against Royal Caribbean Cruises (Asia) Pte Ltd (the “**Organisation**”) after receiving a complaint from a member of the public (the “**Complaint**”). The complainant stated that she had received the personal data of unrelated individuals in an email payment reminder sent by the Organisation.

2. Investigations revealed that, from 8 February 2018 to 4 April 2018, the personal data of 526 individuals were inadvertently disclosed to other unrelated members of the public via unintended email payment reminders (the “**Data Breach Incident**”). The personal data disclosed included booking IDs, ship codes, sailing dates, names, net amounts due, amounts paid, balance due and the balance due date (the “**Affected Personal Data**”).

3. The Organisation is part of the Royal Caribbean Group, and is the wholly owned subsidiary and data intermediary of the USA-based Royal Caribbean Cruises Ltd (Liberia) (“**RCL**”). It is responsible for the following business functions on behalf of RCL:

(a) Conducting sales and marketing activities on behalf of the cruise ship operators of the Royal Caribbean Group, including RCL;

(b) Taking cruise bookings from Singapore-based customers of RCL;

(c) Administering a loyalty membership programme on behalf of RCL; and

(d) Collecting payments from Singapore-based customers of RCL who made their bookings via walk-in, roadshows and online bookings at the Royal Caribbean Group’s Singapore website.

4. RCL’s branch office in the Philippines (“**RCL Philippines**”) provides IT support to entities within the Royal Caribbean Group, and does not have a separate legal identity from RCL. On 1 January 2017, the Organisation entered into an operative intercompany agreement with RCL Philippines for the provision of IT support and customer services support. Such services included providing technical support for the business software applications and services used by the Organisation.

5. As part of its business functions, the Organisation would send its Singapore customers email payment reminders prior to the commencement of their cruises. On 8 February 2020, the Organisation automated this business function through a business software enterprise operated by RCL Philippines (the “**Hyperion System**”), which would generate pre-programmed emails to individual customers to remind them of outstanding bill amounts (the “**Direct Payment Reminder**”). Concurrently, a collated list of the customers (together with other personal data) who received the Direct Payment Reminder would be generated and sent via email to the Organisation (“**Collated Payment Reminder**”). Both the Direct Payment Reminder and Collated Payment Reminder were automatically generated on a scheduled frequency and sent to the customers and Organisation by the Hyperion System without any manual intervention from the Organisation (the “**Automated Payment Reminder System**”).

6. The Automated Payment Reminder System had been successfully implemented in other countries, and RCL Philippines put in place the following process to handle requests from Royal Caribbean Group entities related to the Hyperion System:

(a) RCL Philippines would receive a request from respective Royal Caribbean entity for a new process to be implemented in the Hyperion System;

(b) RCL Philippines would review the scope of the request and configure the Hyperion System;

(c) RCL Philippines would then run a test cycle and a test email would be generated to RCL Philippines to test for whether the content was in line with the request by the requesting Royal Caribbean entity;

(d) Thereafter, RCL Philippines would send a sample of the output email to the relevant Royal Caribbean entity to review; and

(e) The relevant Royal Caribbean entity would sign off on the implementation and RCL Philippines would then implement the new process to go live.

7. Investigations revealed that the Data Breach Incident occurred because RCL Philippines made an error in the coding of the email parameters in the Structured Query Language (“**SQL**”) script when configuring the Hyperion System as described in paragraph 6(b), leading to the Collated Payment Reminders being sent to the first customers in the mailing lists instead of the Organisation. Consequently, the personal data of the Singapore customers contained in the Collated Payment Reminders were disclosed to certain unrelated customers.

8. Both the Organisation and RCL Philippines were not aware of this error until they were informed of the Complaint to the Commission referenced in paragraph 1. As the Automated Payment Reminder System was new and unfamiliar to the Organisation at the material time, the Organisation and its employees were also not aware that it was supposed to be receiving the Collated Payment Reminders.

9. The Data Breach Incident happened after the Organisation provided lists of Singapore customers with outstanding payments due to RCL Philippines for processing with the Hyperion System. The Commission is of the view that the coding error that occurred during the configuration of the Hyperion System was wholly within RCL Philippines’ operations and that the Data Breach Incident did not arise from any business functions that the Organisation was conducting as a data intermediary on behalf of RCL.

10. In the above circumstances, the Deputy Commissioner for Personal Data Protection finds that the Organisation was not in breach of the Protection Obligation under section 24 of the PDPA.

11. We note that the Organisation had taken the following remedial actions:

(a) Conducted additional trainings for its employees to be mindful of the importance of data protection in its business processes;

(b) Reviewed its supervisory framework for new employees so that similar incidents would not happen again; and

(c) Reviewed its communication with RCL Philippines for implementation of any new processes.

## Sendtech Pte. Ltd.

## [2021] SGPDPCS 9

| **Case Number** | : | Case No. DP-2102-B7884 |
| --- | --- | --- |
| **Decision Date** | : | 22 July 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Sendtech Pte. Ltd. |

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

1. On 13 February 2021, Sendtech Pte. Ltd. (the “**Organisation**”) informed the Personal Data Protection Commission (the “**Commission**”) of a data breach incident. There was an unauthorized access to the Organisation’s Amazon Web Services (“**AWS**”) account via an access key (the “**Incident**”).

2. The Organisation became aware of the Incident on 10 February 2021 when its AWS account was shut down due to unusual account activity. The cause of Incident was a compromised AWS access key. This access key was created in 2015 when the Organisation was developing the backend of its server in its incipient stages. This AWS access key had not been rotated or changed since 2015. The Organisation suspected that the AWS could have been compromised through its former or current employees. First, all former developers had access to this key and some could still have the source code on their computers. Second, as most of the employees are working from home, it is possible that the AWS access key was compromised if the employees had accessed internet through a public WiFi connection.

3. With this compromised AWS access key, the attacker gained admin privileges, created another admin account and queried the buckets storing personal data. As a result, the personal data of 64,196 customers and 3,401 contractors and the contractors’ employees were accessed. There was no evidence of data exfiltration. For the customers, the personal data included the email address, contact number, home address and last four digits of the debit or credit card. For the contractors and their employees, the personal data included profile photo and copies of the NRIC or work permit (front and back).

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

a. Rotated all access keys;

b. Changed passwords for all servers;

c. Enhanced its audit trail on AWS buckets to log all read and write operation at the object level;

d. Checked and verified that its Github repositories was set to “Private”;

e. Engaged cybersecurity consultants to carry out assessment of its security setup and advise on improvements to the security measures; and

f. Developed new cybersecurity policies and processes which specifically include measures for credentials management.

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

6. The Organisation admitted it did not have specific AWS policies for the assignment of roles to rotate credentials. There was also a lack of detailed steps to manage credentials access of outgoing staff. Hence, the credentials were not rotated or changed whenever there are staff movement.

7. In the circumstances, the Organisation is found to have breached section 24 of the PDPA.

8. On 23 June 2021, the Organisation was notified of the Commission’s intention to impose a financial penalty of $10,000 based on the Commission’s consideration of the factors listed under section 48J(6) of the PDPA, and the circumstances of this case, in particular (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 Organisation was invited to make representations. Having considered the Organisation’s representations dated 25 June 2021 to reduce the financial penalty payable and to allow the Organisation to pay the financial penalty by way of an instalment plan the Deputy Commissioner hereby directs the Organisation to:

a. Pay a financial penalty of $9,000 in 12 instalments by the due dates as set out below, failing which the full outstanding amount shall become due and payable immediately and 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:

i. 1st instalment of $750 on 1 September 2021;

ii. 2nd instalment of $750 on 1 October 2021;

iii. 3rd instalment of $750 on 1 November 2021;

iv. 4th instalment of $750 on 1 December 2021;

v. 5th instalment of $750 on 1 January 2022;

vi. 6th instalment of $750 on 1 February 2022;

vii. 7th instalment of $750 on 1 March 2022;

viii. 8th instalment of $750 on 1 April 2022;

ix. 9th instalment of $750 on 1 May 2022;

x. 10th instalment of $750 on 1 June 2022;

xi. 11th instalment of $750 on 1 July 2022; and

xii. 12th instalment of $750 on 1 August 2022.

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

## ACL Construction (S) Pte Ltd

## [2022] SGPDPCS 2

| **Case Number** | : | DP-2107-B8598 |
| --- | --- | --- |
| **Decision Date** | : | 21 April 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | ACL Construction (S) Pte Ltd |

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

1. On 2 June 2021, the Personal Data Protection Commission (the **“Commission”**) was notified that data from ACL Construction (S) Pte Ltd (the **“Organisation”**), a company that provides pre-fabricated structures, structural steel products and construction services, was being offered for sale on the darkweb by one “Prometheus” (the **“Incident”**).

2. Investigations revealed that a few days ago, three ACL staff - a designer and two sales executives had experienced difficulties when they tried to log in to access their files. Thereafter, the ACL staff discovered that the files had been encrypted. The Organisation then sought external IT support.

3. The Organisation informed the Commission that the affected files contained the following data related to their projects:

(i) Quotation folder – quotations (to clients and from suppliers), delivery orders, invoices and other supporting documents;

(ii) Common folder – project document and photographs; and

(iii) Drawing folder – CAD drawings.

4. Our investigations revealed that the affected files contained the names of the Organisation’s customers, the relevant liaison person, their business contact number(s) and/or business email(s). As the names, business contact numbers and business emails were not provided by the individuals concerned for a personal purpose, they would constitute “business contact information” as defined under the Personal Data Protection Act (“**PDPA**”), and fall outside the scope of the Act by virtue of section 4(5) of the PDPA. Accordingly, while the Organisation may have suffered a data breach, no personal data was in fact affected.

5. This finding alone would have brought the matter to a close. However, in the course of our investigations, the Commission found out that the Organisation had failed to designate one or more individuals, commonly known as a Data Protection Officer (“DPO”), to be responsible for ensuring that the Organisation complies with the PDPA, as required under section 11(3) of the PDPA. The Organisation’s omission to have any data protection policies in place meant that it was also in breach of section 12(a) of the PDPA.

6. The Commission is cognizant that by virtue of the nature of the Organisation’s business, the Organisation primarily deals with business contact information from its corporate clients. Having said that, while no personal data may have been affected as a result of the Incident, the Organisation still has to comply with the accountability obligation, as set out in sections 11 and 12 of the PDPA so as to protect the personal data of its employees, and any other personal data it may incidentally process, come into control or possession of.

7. The Commission notes that after the Incident, the Organisation took prompt remedial actions and duly appointed a member of its staff to be responsible for ensuring that the Organisation complies with the PDPA.

8. Nonetheless, bearing in mind the Organisation’s low level of awareness of its obligations under the PDPA, 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 develop and implement policies and practices to comply with the provisions of the PDPA; and

b. Put in place a programme of compulsory training for employees of ACL on compliance with the PDPA when handling personal data.

## iClick Media Pte. Ltd.

## [2019] SGPDPCS 4

| **Case Number** | : | Case No. DP-1901-B3254 |
| --- | --- | --- |
| **Decision Date** | : | 04 October 2019 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | iClick Media Pte. Ltd. |

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

1. Following a complaint against EU Holidays Pte Ltd, (“**EU Holidays**”), the Personal Data Protection Commission conducted an investigation to determine whether EU Holidays had contravened the Personal Data Protection Act 2012 (the “**PDPA**”). In the course of investigations, it was found that EU Holiday’s IT vendor, iClick Media Pte Ltd (the “**Organisation**”), had not developed any internal policies and practices that are necessary for it to meet its obligations under the PDPA. In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 12 of the PDPA and decided to direct the Organisation to, within 60 days:

2. Put in place a data protection policy, including written internal policies, to comply with the provisions of the PDPA;

3. Develop a training programme for the Organisation’s employees in respect of their obligations under the PDPA when handling personal data and require all employees to attend such training; and

4. By no later than 7 days after the above actions have been carried out, the Organisation shall, in addition, submit to the Commission a written update.

## Saturday Club Pte Ltd

## [2019] SGPDPCS 6

| **Case Number** | : | Case No. DP-1906-B4109 |
| --- | --- | --- |
| **Decision Date** | : | 23 October 2019 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Saturday Club Pte Ltd |

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

1. Upon investigation into a suspected data breach, it was found that Saturday Club Pte Ltd (the “**Organisation**”) had not developed any internal policies and practices that are necessary for it to meet its obligations under the Personal Data Protection Act 2012 (“**PDPA**”). In the circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 12 of the PDPA and decided to issue the directions to the Organisation.

## Breach of the Do-Not-Call ("DNC") provisions by a financial advisor

## [2023] SGPDPCS 6

| **Case Number** | : | ENF-DNC-230119-0007 & Others |
| --- | --- | --- |
| **Decision Date** | : | 20 October 2023 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Lin DaoWen Kenny |

*Data Protection* – *Do Not Call Registry* – *Failure to check the Do Not Call Registry before sending specified messages*

*Data Protection* – *Do Not Call Registry* – *Dictionary attack* – *Sending applicable messages to telephone numbers generated by automated means*

1 The Do Not Call Registry (“**DNC Registry**”) is a national database kept and maintained by the Personal Data Protection Commission (the “**Commission**”) pursuant to section 39 of the Personal Data Protection Act 2012 (“**PDPA**”). Persons may register their Singapore telephone numbers with the DNC Registry so as to not receive unsolicited telemarketing calls and messages. The DNC Registry comprises of 3 separate registers (i) the No Text Message Register, (ii) the No Voice Call Register, and (iii) the No Fax Message Register.

2 From January 2023 to July 2023, the Commission received twelve (12) complaints arising from unsolicited telemarketing calls made by Lin DaoWen Kenny (the “**Individual**”) to telephone numbers registered on the No Voice Call Register of the DNC Registry (the “**Complaints**”).

3 The Commission commenced investigations to determine whether there had been any breaches of the “Do Not Call” provisions in Parts 9 and 9A of the PDPA (“**DNC Provisions**”). This case also illustrates how the employment of online tools to generate Singapore telephone numbers to market products or services may lead to a breach of section 48B(1) of the PDPA.

4 The Individual is a financial advisor. In order to generate leads, he used an Excel spreadsheet formula (“**randbetween**”) to generate a list of all numbers upon entering the extreme ends on a numerical spectrum. The Individual generated 1000 numbers (the “**Phone List**”) with the intention of finding Singapore telephone numbers to market his financial advisory services.

5 Of the 1,000 numbers generated on the Phone List, 384 corresponded to Singapore telephone numbers that were registered with the No Voice Call Register of the DNC Registry.

6 The Individual engaged a telemarketer to make marketing calls to the numbers on the Phone List to promote his financial advisory services. The Individual admitted that he failed to check if the telephone numbers were registered with the Do Not Call Registry before providing the Phone List to the telemarketer. Given the means by which the Individual generated the Singapore telephone numbers, the Individual was also unable to provide any evidence (written or otherwise) that he had obtained clear and unambiguous consent from the subscribers of the 384 DNC-registered numbers before making the marketing calls. In light of above, the Individuals has negligently contravened section 43(1) of the PDPA.

7 Further, by generating the 384 Singapore telephone numbers through the Excel spreadsheet formula mentioned above and engaging a telemarketer to make marketing calls to promote his financial advisory services, the Individual has also contravened section 48B(1) of the PDPA.

8 The Individual claimed to have inadvertently overlooked screening the numbers on the Phone List on this occasion. The Assistant Commissioner considered that the Individual had a previous compliance record of screening telephone numbers to ascertain if they were on the DNC Registry. Further, the Individual immediately ceased the telemarketing calls and promptly purchased more credits that can be used to screen if the telephone numbers were registered on the DNC Registry so as to ensure compliance with the DNC Provisions of the PDPA. Upon careful consideration of these facts, the Assistant Commissioner issued a warning to the Individual for contravening sections 43(1) and 48B(1) of the PDPA.

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

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

**Duty to check register**

**43.**—(1) Subject to section 48(2), a person must not send a specified message addressed to a Singapore telephone number unless the person has, at the time the person sends the specified message, valid confirmation that the Singapore telephone number is not listed in the relevant register.

**Prohibition on use of dictionary attacks and address-harvesting software**

**48B.**—(1) Subject to subsections (2) and (3), a person must not send, cause to be sent or authorise the sending of an applicable message.

(2) Subsection (1) does not apply to an employee (P) who sends, causes to be sent or authorises the sending of an applicable message in good faith —

(a) in the course of P’s employment; or

(b) in accordance with instructions given to P by or on behalf of P’s employer in the course of P’s employment.

(3) However, subsection (2) does not apply to a person (P) who, at the time the applicable message was sent, was an officer or a partner of the sender and it is proved that —

(a) P knew or ought reasonably to have known that the telephone number is an applicable telephone number; and

(b) the applicable message was sent with P’s consent or connivance, or the sending of the applicable message was attributable to any neglect on P’s part.

## SLP Scotia Pte. Ltd. and another

## [2022] SGPDPCS 10

| **Case Number** | : | DP-2007-B6585, DP-2007-B6591, DP-2007-B6594, DP-2007-B6598 |
| --- | --- | --- |
| **Decision Date** | : | 09 April 2022 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | SLP Scotia Pte. Ltd.; SLP International Property Consultants Pte. Ltd. |

*Data Protection* – *Consent obligation* – *No breach* – *Consent provided in collateral agreement*

1. Between 10 to 14 July 2020, the Personal Data Protection Commission (the “**Commission**”) received four complaints against SLP International Property Consultants Pte Ltd (“**SLPIPC**”) and its subsidiary SLP Scotia Pte Ltd (“**SLPS**”) (collectively, the “**Organisations**”). The complainants were property agents registered through SLPS (the “**Complainants**”).

2. As a merger was due to take place between the Organisations, on 7 July 2020, SLPIPC initiated the registration of salespersons in SLPS as salespersons in SLPIPC with the Council of Estate Agencies (“**CEA**”). CEA thereafter emailed the Complainants asking them to either initiate a salesperson application to join SLPIPC or disregard the email if they were not interested in registering with SLPIPC (the “**Incident**”).

3. The Complainants alleged that:

a. they had not consented to be contacted for such purposes; and

b. SLPS had improperly disclosed their personal data (including NRIC number, date of birth, and home address) to SLPIPC, and SLPIPC had in turn improperly disclosed the data to CEA.

4. CEA is the entity which administers the registration of salespersons (such as the Complainants) under the Estate Agents Act 2010 (“**EAA**”). Pursuant to section 29(1) of the EAA, a person may not act as a salesperson for any estate agent unless he or she is registered; the said register is maintained by the CEA pursuant to section 36 of the EAA. Further, under section 40(1) of the EAA, a salesperson may not be registered to act as a salesperson for more than one estate agent at any one time.

5. SLPIPC disclosed the personal data of the Complainants to CEA for the purposes of the change in registration from SLPS to SLPIPC. In doing so, SLPIPC was complying with its obligations under the EAA. The disclosure by SLPIPC to CEA was therefore not in breach of any of the provisions of the Personal Data Protection Act 2012 (“**PDPA**”), as under section 4(6) of the PDPA, obligations of a party under other written law take precedence over obligations under the PDPA.

6. The Commission’s investigation focused on whether the Organisations had breached the Consent Obligation under section 13 of the PDPA in relation to:

a. the disclosure of the Complainants’ personal data by SLPS to SLPIPC; and

b. the collection of the said data by SLPIPC from SLPS.

7. Investigations revealed that the Complainants had each, individually and separately, signed an agreement with SLPS (“**Associate’s** **Agreement**”) in which they had provided their consent for disclosure of their personal data in specific circumstances. Notably:

a. Clause 24 of the Associate’s Agreement provided that the Complainants consented to SLPS collecting, using and/or disclosing their personal data for one or more of the “Company Purposes”.

b. “Company Purposes” as defined in the Associate’s Agreement included disclosure of the Complainants’ personal data to SLPS’ related corporations, to facilitate and administer the real estate brokerage services to be provided by the Complainants under the Associate’s Agreement.

c. As SLPS was a subsidiary of SLPIPC, both Organisations were “related corporations” for the purposes of the Associate’s Agreement.

8. The disclosure and collection of the Complainants’ personal data had been carried out because of an upcoming merger between the Organisations, for business reasons. With the move towards merger at the material time, the Complainants had the option of providing their services under SLPIPC after the merger. This was found to fall under the ambit of “Company Purposes” pursuant to Clause 24 of the Associate’s Agreement, because the merger would have affected the Complainants’ ability to “facilitate and administer” their real estate brokerage services.

9. Consequently, the disclosure of the Complainants’ personal data by SLPS and the collection and disclosure of the same by SLPIPC as a related corporation was found to be consistent with the purposes for which the Complainants had provided consent in the Associate’s Agreement.

10. In light of the above, the Deputy Commissioner for Personal Data Protection finds that the Organisations did not breach the Consent Obligation under section 13 of the PDPA.

## Tripartite Alliance Limited

## [2021] SGPDPCS 3

| **Case Number** | : | Case No. DP-2003-B6000 |
| --- | --- | --- |
| **Decision Date** | : | 16 March 2021 |
| **Tribunal/Court** | : | Personal Data Protection Commission Decision Summary |
| **Coram** | : | — |
| **Counsel Name(s)** | : | — |
| **Parties** | : | Tripartite Alliance Limited |

1. On 3 March 2020, Tripartite Alliance Limited (the “**Organisation**”) notified the Personal Data Protection Commission (the “**Commission**”) that a server hosting its customer relationship management (“**CRM**”) system was infected with ransomware on or around 17 February 2020.

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 Data Protection Act (the “**PDPA**”).

**The Incident**

3. The Organisation is in the business of promoting fair and progressive employment practices, as well as providing mediation and advice in employment–related disputes.

4. The CRM system is a Software-as-a-Service (“**SaaS**”) solution provided by a software service provider engaged by the Organisation (the “**Vendor**”). The Organisation uses the CRM system to handle employment-related enquiries, feedback and complaints.

5. At the time of the incident, the CRM system contained approximately 12,000 individuals’ and 8,000 companies’ data (including information of the companies’ representatives). The types of data affected for each individual varied, but may include an individual’s name, identification number, contact number, email address, age, race, marital status, salary and compensation amount (if applicable).

6. On 17 February 2020, the CRM system was unavailable to users. The Vendor managed to restore the CRM system from a back-up copy within the next three hours.

7. Upon investigations, the Organisation determined that the CRM system suffered a ransomware attack. In particular, security logs obtained from the Vendor showed that hacking attempts were made on the database server between 7 and 14 February 2020.

8. The Organisation claimed that it had, since June 2019, expanded the scope of the IT services procured from the Vendor to include security monitoring services for the CRM system, such as the blocking of cyber-attacks based on alerts. However, there was inadequate process put in place to ensure that the Vendor proactively monitor the alerts and take actions to block malicious activities in a timely manner. Nevertheless, the Organisation accepts that it had the responsibility to ensure that the Vendor had the same understanding on its duty of care under the monitoring services contract and to oversee and supervise the work of the Vendor through clear instructions on regular reporting and updates by the Vendor.

9. Following the incident, the Organisation started close monitoring of the Vendor’s IT services support on a weekly basis to ensure timely update of patches and follow-ups on security alerts received. The Organisation also undertook an organisation-wide review to strengthen its management of all its third-party IT service providers, such as requesting these service providers to conduct cybersecurity audits, vulnerability assessment and penetration testing for the Organisation’s existing IT systems. The Organisation also informed the Commission that it will be migrating to a new CRM system and is currently working to terminate the existing CRM system.

10. The Organisation informed the Commission that the database in the CRM system was not protected by encryption at the time of the incident, which made the database vulnerable for exposure. However, there was no evidence that the hacker had exfiltrated the database.

**The Organisation’s Admission and the Commission’s Decision**

11. The Organisation admitted that it had breached the Protection Obligation under section 24 of the PDPA in failing to ensure that the Vendor had duly discharged its contractual data protection obligations. In particular, the Organisation admitted that it had not monitored the Vendor’s performance to ensure that the Vendor met the required information security standards.

12. As stated in previous decisions by the Commission[[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/107151.xml&queryStr=(personal%20data%20protection%20act)#fn1), organisations have to give proper instructions and exercise reasonable oversight over their vendors to ensure that their outsourced providers are indeed delivering the services contracted. Without reasonable oversight, the risk from any failure will fall on the organisation. In the circumstances, the Commissioner found that the Organisation was in breach of the Protection Obligation under section 24 of the PDPA.

13. As for the Vendor, it was a SaaS provider who provided the CRM system, including maintenance support, and security monitoring services. These services did not entail the processing of personal data. As such, the Vendor was not a “data intermediary” of the Organisation. Accordingly, the Vendor was not responsible for the protection of the individuals’ personal data under the PDPA in respect of the incident.

14. In determining the directions to be imposed on the Organisation for the breach, the Commissioner took into account the following factors:

**Aggravating**

(a) The high number of affected individuals, which is approximately 20,000;

(b) The nature of the affected data. In particular, the database contained details of employment-related complaints and disputes. Individuals would expect a high level of confidence when they convey such matters to the Organisation for handling;

**Mitigating**

(c) The Organisation’s upfront admission of breach of the Protection Obligation, and the prompt remedial actions to mitigate the effects and prevent recurrence of the incident; and

(d) There was no evidence of exfiltration of the database in the CRM system.

15. On account of the above, the Organisation is directed to pay a financial penalty of $29,000 within 30 days from the date of this direction. In view of the remedial action of the Organisation, the Commission will not be issuing any other directions.

[[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/107151.xml&queryStr=(personal%20data%20protection%20act)#fnref1) See for example, *Re Smiling Orchid (S) Pte Ltd and Ors* [2016] SGPDPC 19, *Re Royal Caribbean Cruises (Asia) Pte Ltd* [2020] SGPDPC 5*,* and *Re SCAL Academy Pte. Ltd.* [2020] SGPDPC 2.