COMMISSIONER FOR PERSONAL DATA PROTECTION

[2019] SGPDPC 27

Case No DP-1710-B1202

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

And

Horizon Fast Ferry Pte. Ltd.
(UEN No. 201221074R)

… *Organisation*

DECISION

Horizon Fast Ferry Pte. Ltd.

[2019] SGPDPC 27

Tan Kiat How, Commissioner — Case No DP-1710-B1202

25 July 2019

1 On 9 October 2017, the Complainant informed the Personal Data Protection Commission (the "**Commission**") that by entering her passport number in the booking form on the Organisation's website, her name, gender, nationality, date of birth and passport expiry date were automatically populated in the corresponding fields on the form on the Booking Site without any requirement for further authentication (the "**Incident**").

Material Facts

2 The Organisation is a Singapore-based ferry operator with ferry services running between Singapore and Batam.

3 As part of its service offerings, the Organisation operates a website that allows passengers to purchase ferry tickets directly from the Organisation online ("**Booking Site**"). At the material time, passengers who wanted to purchase ferry tickets through the Booking Site were required to provide the following personal data (the **"Personal Data Set**") as set out in the form on the Booking Site ("**Booking Form**"):

(a) the passenger's full name;

(b) gender;

(c) nationality;

(d) date of birth;

(e) passport number; and

(f) passport expiry date.

4 The same Personal Data Set was collected from passengers and entered into the Organisation's Counter Check-In System ("**CCIS**") when they checked in at the check-in counter. The CCIS is an internal system used by the Organisation's counter staff to manage the passenger check-in process and is only accessible by authorised counter staff.

5 As a matter of practice, all Personal Data Sets collected from the Booking Site and the CCIS were stored and retained on the Organisation's internal database (the "**Database**") even after the last travelling date of the passenger's itinerary to facilitate and speed up subsequent check-ins for passengers who have previously travelled with the Organisation ("**Returning Passengers**").[1]

6 In this regard, one of the features of the CCIS was the auto-retrieval of the personal data of Returning Passengers. By entering a Returning Passenger's passport number, the CCIS would automatically retrieve the Personal Data Set associated with a Returning Passenger's passport number from the Database and populate the remaining fields in the Booking Form. Counter staff would no longer need to manually enter the Returning Passenger's personal data. The personal data retrieved from the Database was only meant to be accessible by authorised counter staff on the CCIS.

Booking Site revamp

7 In or around May 2017, the Organisation engaged an independent contractor (the "**Contractor**") on an informal basis to revamp the Booking Site, specifically to improve the user interface and user experience, such as when purchasing ferry tickets online. The parties did not enter into any written contract for the revamping of the Booking Site and all instructions and requirements for the revamp of the Booking Site were conveyed either verbally or through WhatsApp text messages. The Organisation did not inform or instruct the Contractor of its data protection obligations in relation to the personal data in the Database.

8 Unbeknownst to the Organisation and contrary to its intention, the Contractor replicated the auto-retrieval and auto-population feature (which was only meant to be used in the internal CCIS) in the Booking Site as part of the website revamp. Consequently, whenever a user entered a passport number which matched a Returning Passenger's passport number in the

[1] The Organisation also represented that the Personal Data Sets were retained on the Database for audit and accounting and internal reporting purposes.

Database, the system would automatically retrieve and populate the remaining fields in the Booking Form with the Personal Data Set associated with the Returning Passenger's passport number. As the Organisation failed to conduct proper user acceptance tests before launching the revamped Booking Site, the Organisation was not aware of this function until it was notified of the Incident.

9 At the time of the investigation, there were a total of 444,000 Personal Data Sets stored in the Database.[2] However, the Organisation represented that out of the 444,000 Personal Data Sets, there were only a total of 295,151 unique passengers whose Personal Data Sets were stored in the Database as a number of passengers had made bookings under different passport numbers (valid and expired).[3]

10 The Organisation took the following remedial actions shortly after it was notified of the Incident:

(a) the Organisation commenced investigations and removed the auto-retrieval and auto-population feature from the Booking Site a little more than a week after the Organisation was first notified of the Incident;

(b) the Organisation conducted checks to ensure that the auto-retrieval and auto-population feature was disabled from the Booking Site; and

(c) the Organisation implemented administrative measures to protect the personal data in their possession, such as ensuring that documents containing booking data and passenger manifests were properly shredded at the end of the day, that monthly reports with passenger data were kept in a locked room and sent for mass disposal at the end of the financial year and the Organisation appointed a data protection officer to be responsible for ensuring the Organisation's compliance with the PDPA.

Findings and Basis for Determination

11 The two main issues for determination are:

[2] Approximately three months after the date of the Complaint, on 12 December 2017.
[3] Other than the Personal Data Sets, some users also supplied their mobile phone numbers. There were 5,218 unique mobile numbers collected and stored in the Database as at 12 December 2017.

(a) whether the Organisation complied with its obligations under sections 11(3) and 12(a) of the PDPA; and

(b) whether the Organisation breached section 24 of the PDPA.

12 The Personal Data Sets stored in the Database are "personal data" as defined in section 2(1) of the PDPA. In particular, given that the unauthorised disclosure of the Personal Data Set as a whole could have led to an increased risk of such personal data being used for illegal activities such as identity theft or fraud, they are personal data of a more sensitive nature.[4]

Whether the Organisation complied with its obligations under sections 11(3) and 12(a) of the PDPA

13 Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be responsible for ensuring compliance with the PDPA. In a similar vein, section 12(a) of the PDPA requires an organisation to develop and implement policies and practices that are necessary to meet its obligations under the PDPA (collectively, the "**Openness Obligation**").

14 As mentioned above, all passengers who purchased ferry tickets from the Organisation were required to provide the personal data in the Personal Data Set to the Organisation either at the time of booking through the Booking Site or at the Organisation's check-in counter.

15 However, even though the Organisation routinely collected and processed large volumes of personal data in the course of its business, the Organisation demonstrated a blatant disregard for its data protection obligations.

16 By its own admission, at the time of the Incident, the Organisation did not designate any individual to be responsible for ensuring that the Organisation complies with the PDPA, i.e. a data protection officer ("**DPO**"). The Organisation's current DPO was only appointed after 6 November 2017, when the Organisation was first informed of the Incident.

17 Similarly, the Organisation's privacy policy was only implemented and uploaded on its Booking Site after it was informed of the Incident. While the Organisation represented that it

[4] See *Re: Singapore Management University Alumni Association* [2018] SGPDPC 6 at [20]

had an internal guideline titled "Workplace policies: confidentiality" in place at the time of the Incident, apart from a reference to its commitment to "*[e]stablish data protection practices (e.g. secure locks, data encryption, frequent backups, access authorization)*", the internal guidelines do not set out any actual practices or processes to protect the personal data in the Organisation's possession.

18 The development and implementation of data protection policies is a fundamental and crucial starting point for organisations to comply with their obligations under the PDPA. This was highlighted in *Re M Star Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 (at [25]) ("***M Star Movers***"):

> At the very basic level, an appropriate data protection policy should be drafted to ensure that it gives a clear understanding within the organisation of its obligations under the PDPA and sets general standards on the handling of personal data which staff are expected to adhere to. To meet these aims, the framers, in developing such policies, have to address their minds to the types of data the organisation handles which may constitute personal data; the manner in, and the purposes for, which it collects, uses and discloses personal data; the parties to, and the circumstances in, which it discloses personal data; and the data protection standards the organisation needs to adopt to meet its obligations under the PDPA.
>
> An overarching data protection policy will ensure a consistent minimum data protection standard across an organisation's business practices, procedures and activities (e.g. communications through social media).

19 Likewise, the DPO plays a vital role in building a robust data protection framework to ensure the organisation's compliance with its obligations under the PDPA regardless of the size of the organisation.[5]

20 As highlighted in *M Stars Movers* (at [34]), the responsibilities of a DPO include, but are not limited to:

> (a) ensuring compliance with the PDPA when developing and implementing policies and processes for handling personal data, including processes and formal procedures to handle queries and/or complaints from the public;
>
> (b) fostering a data protection culture and accountability among employees and communicating personal data protection policies to stakeholders;

[5] *M Stars Movers* at [37].

(c) handling and managing personal data protection related queries and complaints from the public, including making information about the organisation's data protection policies and practices available on request to the public;

(d) alerting management to any risks that might arise with regard to personal data; and

(e) liaising with the Commissioner on data protection matters, if necessary.

21 In the circumstances, it is clear that the Organisation failed to meet its obligations under sections 11(3) and 12(a) of the PDPA. Had the Organisation met its Openness Obligation under the PDPA, the Organisation would have had a clearer understanding of its data protection obligations under the PDPA and appropriate measures may have been put in place earlier which could have prevented the Incident from occurring.

Whether the Organisation breached the Protection Obligation under the PDPA

22 As a preliminary point, although the Contractor appears to have been responsible for carrying out the Booking Site revamp, seeing as the parties did not enter into any written agreement and there was no evidence to suggest that the Contractor stored, held or managed the personal data in the Database on behalf of the Organisation, the Contractor is not a data intermediary of the Organisation. The Organisation is solely responsible for complying with all the data protection obligations under the PDPA, including the obligation to make reasonable security arrangements to protect the personal data in its possession or under its control under section 24 of the PDPA.

23 At the time of the Incident, the Database was shared by the Booking Site and the CCIS. However, the Organisation conceded that it omitted to inform the Contractor of its data protection obligations and did not instruct the Contractor to put in place proper safeguards to protect the personal data in the Organisation's possession or control.

24 In this regard, one of the key considerations for organisations as highlighted in the Guide on Building Websites for SMEs (at [4.2.1]) is the importance of emphasising the need for personal data protection to their IT vendors:

> Organisations should emphasise the need for personal data protection to their IT vendors, by making it part of their contractual terms. The contract should also state clearly the responsibilities of the IT vendor with respect to the PDPA. When

discussing the scope of outsourced work, organisations should consider whether the IT vendor's scope of work will include any of the following:

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

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

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

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

25 Even more concerning was the fact that the Organisation did not put in place reasonable arrangements to discover risks to its personal data when changes were made to the Booking Site that was linked to the Database which held the personal data of close to 300,000 individuals. The Organisation did not conduct any proper user acceptance testing prior to the launch of the revamped Booking Site. The only test that the Organisation carried out was to key in a simulated passport number to test the new user interface. However, as the simulated passport number did not match any record in the Database, the Organisation failed to detect the auto-retrieval and population feature in the revamped Booking Site.

26 Websites connected to the Internet are subject to a multitude of cyber threats that may compromise the website and expose any personal data it collects. Organisations should therefore ensure that the protection of the personal data and the security of the website is a key design consideration at each stage of the website's life cycle – be it during the requirements gathering, design and development stage or when conducting user acceptance testing or deployment and operations and support.[6]

27 As a result of the Organisation's failure to conduct proper user acceptance tests, the gap in the revamped Booking Site which allowed for the unauthorised access to personal data stored

[6] See PDPC's Guide on Building Websites for SMEs at [3.2] to [3.3].

in the Database went undetected. This was not rectified for approximately one month, thereby causing the personal data of close to 300,000 of the Organisation's passengers to be exposed to the risks of unauthorised disclosure.

28 As a matter of good practice, organisations should consider whether there is a need to conduct a data protection impact assessment whenever a new system or process is being introduced, developed or implemented that involves the handling of personal data or an existing system or process is being reviewed or substantially redesigned.[7]

29 In this regard, the Guide to Data Protection Impact Assessments (published on 1 November 2017) (at [1.2]) states that:

> A [Data Protection Impact Assessment] involves identifying, assessing and addressing personal data protection risks based on the organisation's functions, needs and processes. In doing so, an organisation would be better positioned to assess if their handling of personal data complies with the PDPA or data protection best practices, and implement appropriate technical or organisational measures to safeguard against data protection risks to individuals.

30 In adopting this view, the Commissioner agrees with the observations in the Joint Guidance Note issued by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia on the proper use of risk assessment tools for all new projects involving personal information:[8]

> Privacy risks evolve over time. Conducting risk assessments, at least on an annual basis, is an important part of any privacy management program to ensure that organizations are in compliance with applicable legislation.
>
> We have seen instances of organizations offering new services that collect, use or disclose personal information that have not been thoroughly vetted from a privacy perspective. Proper use of risk assessment tools can help prevent problems. Fixing a privacy problem after the fact can be costly so careful consideration of the purposes for a particular initiative, product or service, and an assessment that minimizes any privacy impacts beforehand is vital.

---

[7] See PDPC's Guide to Data Protection Impact Assessments.

[8] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia, Getting Accountability Right with a Privacy Management Program <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/>

> As a result, such assessments should be required throughout the organization for all new projects involving personal information and on any new collection, use or disclosure of personal information. Organizations should develop a process for identifying and mitigating privacy and security risks, including the use of privacy impact assessments and security threat risk assessments.
>
> [Emphasis added.]

31 In view of the above and the Organisation's failure to put in place adequate security arrangements to protect the personal data in the Database, the Commissioner finds that the Organisation was in breach of the Protection Obligation under section 24 of the PDPA.

32 Finally, although the Organisation did not intend to offer the auto-retrieval and auto-population function in its Booking Site, organisations that do offer such functions should take note of the following comments made by the UK Information Commissioner's Office ("**ICO**") in the Personal Information Online Code of Practice on the use of auto-completion facilities for forms and passwords:

> If your site offers auto-completion facilities for forms and passwords, it is good practice to notify users if this could leave them vulnerable, for example if their mobile device or laptop is stolen. However, ultimately users have a role to play in protecting themselves online, for example by adjusting the auto-complete settings on their browser or on a website they visit. Autocompletion can present a particular risk where an individual's payment card details have been retained for 'auto-fill' purposes. This may mean not offering auto-completion in certain contexts – e.g. on password fields for authorising payments.
>
> [Emphasis added.]]

Directions

33 Having found that the Organisation is in breach of sections 11(3), 12(a) and 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1 million.

34 In deciding whether to direct an organisation to pay a financial penalty, one of the Commissioner's key objectives is to promote compliance with the PDPA. As such, while the Commissioner will seek to ensure that the financial penalty imposed is reasonable and

proportionate on the facts, the financial penalty should also be sufficiently meaningful to act both as a sanction and as a deterrent to prevent similar contraventions of the PDPA.

35 In this regard, as highlighted in the Advisory Guidelines on Enforcement of the Data Protection Provisions (at [24.1]) the Commissioner will take into account factors such as the seriousness and impact of the organisation's breach and will consider if the organisation had acted deliberately, wilfully or if the organisation had known or ought to have known of the risk of a serious contravention and failed to take reasonable steps to prevent it.

36 In adopting this view, the Commissioner agrees with the ICO's Guidance About the Issue of Monetary Penalties Prepared and Issued Under section 55C(1) of the Data Protection Act 1998 ("**ICO Guidance on Monetary Penalties**") (at [34] to [37]):

> **The Commissioner's aim in imposing a monetary penalty**
>
> The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA or with PECR.
>
> The penalty must be sufficiently meaningful to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening person and by others.
>
> This applies both in relation to the specific type of contravention and other contraventions more generally. Here, the Commissioner will have regard to the general approach set out in paragraphs 42 to 46 below.
>
> The Commissioner will seek to ensure that the imposition of a monetary penalty is appropriate and the amount of that penalty is reasonable and proportionate, given the particular facts of the case and the underlying objective in imposing the penalty.

37 With the foregoing principles in mind, the Commissioner took into account the following aggravating and mitigating factors in assessing the breach and determining the directions to be imposed:

Aggravating factors

(a) the Organisation routinely collects and processes the personal data of a large number of individuals in the course of its business but did not have adequate data protection policies or practices in place;

(b) the Personal Data Sets in collected and stored in the Database, such as the individual's nationality, passport number and passport expiry date, are of a sensitive nature particularly when disclosed as a whole. In this regard, attention is drawn to the decision in *Re: Singapore Management University Alumni Association* [2018] SGPDPC 6 ("***SMU AA***") at [20] where it was stated that *"the use of an NRIC Number generation tool would make it relatively easy for a motivated hacker to systematically query the webpage and, if successful, he would have been able to definitively link the NRIC Number to the full name, address and other personal data of the member, potentially resulting in significant harm to the individual, such as through identity theft or an unauthorised person impersonating the affected member";*

(c) the Organisation demonstrated a blatant lack of regard for its data protection obligations prior to the Incident. Despite the fact that the PDPA came into full force on 2 July 2014 and advisory guidelines and/or guides which are relevant to the contravention were available, the Organisation only appointed a DPO more than three years after the PDPA came into full force and appears to have ignored or not given these guidelines and/or guides the appropriate weight;

(d) as a result of the Organisation's lack of regard for its data protection obligations, the personal data of at least 295,151 of the Organisation's passengers were exposed to the risks of unauthorised disclosure;

Mitigating factors

(e) the Organisation had cooperated fully in the investigation and was forthcoming and transparent in admitting its mistakes in contributing to the unauthorised disclosure;

(f) remedial actions were taken and the Organisation took increased efforts to heighten employees' awareness of the Organisation's data protection obligations under the PDPA;

(g) there was no evidence to suggest any actual unauthorised access and/or exfiltration of data leading to loss or damage; and

(h) there was limited disclosure to possibly one individual who would have had to enter a Returning Passenger's passport number that matched the passport number in the Database.

38 The Organisation submitted representations, after being informed of the proposed decision in this case, requesting a warning in lieu of a financial penalty or otherwise to reduce the quantum of the financial penalty imposed. In support of this, the Organisation made the following representations:

(a) The Organisation asserted that the revamped Booking Site was only operational in or around October 2017, and the auto-retrieval and auto-population feature was only accessible to users (other than the authorised counter staff) from October 2017 to 14 November 2017. Thus, the Personal Data Sets were only at risk of unauthorised disclosure for this period of time;

(b) The Organisation did not deliberately nor wilfully breach the PDPA and upon notification of the Incident, the Organisation took remedial actions [9] and was cooperative during the investigations, and

(c) The risk of unauthorised disclosure is low as an individual would need to possess the exact passport number to trigger the auto-complete feature which would disclose the corresponding Personal Data Set.

39 With respect to the issue raised in paragraph 38(a), the Commissioner accepted the clarifications as to the period of time for which the Personal Data Sets were at risk of unauthorised disclosure, and the quantum of the financial penalty has been adjusted accordingly.

40 With regards to paragraph 38(b), the remedial actions taken by the Organisation and the fact that the Organisation was cooperative during the investigations, have already been taken into account as mitigating factors at paragraphs 37(e) and 37(f) above in determining the appropriate quantum of the financial penalty. Also, the deliberateness or wilfulness of the Organisation in breaching the PDPA is not a relevant consideration in this case where it was

[9] Including those set out in paragraph 10.

found that the Organisation failed to put in place the necessary security arrangements to protect the Personal Data Set.

41 With regards to paragraph 38(c) above, these are matters that had already been taken into consideration in assessing the financial penalty and as set out at paragraphs 37(g) and 37(h) above .

42 Having considered all the relevant factors of this case, the Commissioner hereby direct the Organisation to pay a financial penalty of S$54,000 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 be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION