The Travel Corporation (2011) Pte. Ltd.

[2019] SGPDPC 42

Tan Kiat How, Commissioner — Case No. DP-1810-B2821

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

Data Protection – Openness obligation – Failure to designate one or more persons to be responsible for ensuring that the organisation complies with the PDPA

19 November 2019

Introduction and Material Facts

1 The Travel Corporation (2011) Pte. Ltd. (the "**Organisation**") offers travel packages both directly to Singapore customers and via third party travel agencies. On 1 October 2018, the Organisation notified the Personal Data Protection Commission (the "**Commission**") regarding the loss of a portable hard disk (the "**Hard Disk**") which contained unencrypted files with the personal data of the Organisation's customers, employees and suppliers (the "**Incident**"). The facts and circumstances of the Incident are as follows.

2 On 25 July 2018, a new employee of the Organisation left the office with her laptop and the Hard Disk; and misplaced both these devices on her way home. She initially only informed the Organisation about the loss of the laptop and a police report was made on 31 July 2018. The misplaced laptop did not contain any personal data. She eventually informed the

Organisation about the loss of the Hard Disk on 21 September 2018 and the Organisation made another police report that day.

3 The table below summarises the number of affected individuals and their corresponding types of personal data contained in the Hard Disk:

S/N.	Category	Types of Personal Data in the Hard Disk	Number of Individuals Affected
1.	Customers	Name, Email Address, Phone Number, Date of Birth and Postal Address	5,437
2.		Same as item 1 plus Passport Number	21
3.		Same as item 1 plus NRIC Number	242
4.	Prospective Customers	Same as item 1	11,000
5.	Employees	Name, Office Email Address and Office Phone Number	30
6.	Suppliers	Names, Company Address, Email Address, Mobile Number, Office Number	1,900
		Total number of individuals	**18,630**

4 It also emerged in the course of the Commission's investigations that the Organisation had not appointed any data protection officer ("**DPO**") prior to the data breach incident on 25 July 2018.

Remedial actions by the Organisation

5 The Organisation subsequently took the following remedial measures:

(a) The Organisation ceased the use of portable storage devices and implemented the use of cloud-based storage for personal data in its possession; and

(b) The Organisation appointed a DPO on 22 October 2018.

Findings and Basis for Determination

Whether the Organisation had breached its obligation to protect personal data under section 24 of the PDPA

6 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by making reasonable security arrangements. A review of the evidence disclosed that business contact information of the Organisation's own employees and its suppliers comprised about 10% of the total number of affected individuals. Pursuant to 4(5) of the PDPA, section 24 of the PDPA did not apply to such personal data. However, the personal data of the Organisation's customers and prospective customers (the "**Customers' Personal Data**") have to be protected under the PDPA.

7 The Organisation failed to protect its Customers' Personal Data as it failed to implement appropriate internal policies governing the use of portable storage devices containing personal data. While the Organisation has a Portable Computer and Storage Devices Policy that stipulated that '*portable computing and storage devices used for business purposes must have designated custodians*', the Organisation did not have any operational frameworks or procedures in place that effectively implements this policy in its individual business units. The

Organisation only relied on verbal instructions to instruct its employees not to bring any portable storage devices out from the office premises. Further, the Organisation did not implement any password protection policies or data encryption policies for its portable storage devices, including the Hard Disk, although it had clear guidelines in its Acceptable User Policy and Information Sensitivity Policy to do so.

8 In the circumstances, the Commissioner found that the Organisation had not made reasonable security arrangements to protect its Customers Personal Data. The Organisation is accordingly in breach of section 24 of the PDPA.

Whether the Organisation was in breach of section 11(3) of the PDPA

9 Section 11(3) of the PDPA requires organisations to designate one or more individuals (typically referred to as a DPO) to be responsible for ensuring that they comply with the PDPA. Appointing a DPO is important in ensuring the proper implementation of an organisation's data protections policies and practices, as well as compliance with the PDPA: see *e.g. Re M Stars Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 at [31] to [37].

10 As the Organisation failed to appoint a DPO prior to the data breach incident, the Commissioner found the Organisation in breach of section 11(3) of the PDPA.

The Commissioner's Directions

11 In view of the above findings, the Commissioner directs the Organisation to pay a financial penalty of $12,000 within 30 days from the date of this direction, failing which,

interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

12 In coming to this finding, the following mitigating factors were taken into account:

(a) the Organisation notified the Commission of the Incident and fully co-operated with the Commission's investigations;

(b) the Organisation promptly implemented remedial measures, as set out at paragraph 5, to address the breach;

(c) the Organisation is actively addressing system security related recommendations provided by an external auditor; and

(d) the Commission had not received any complaints as a result of the Incident.

13 In view of the remedial measures taken by the Organisation, the Commissioner decided not to impose any other directions.

The Organisation's Representations

14 After the preliminary decision was issued to the Organisation, it made representations for a warning be issued instead of an imposition of a financial penalty. The Organisation did not dispute the finding that it had breached section 24 of the PDPA.

15 In support of its request for a warning instead of the imposition of a financial penalty, the Organisation represented that it had taken the following rectification and remediation measures:

(a) conducting a PDPA impact and gap analysis;

(b) developing and enhancing internal PDPA policies and procedures;

(c) improving current back-up systems and disaster recovery plans across the business promptly following the Incident;

(d) notifying the affected individuals as soon as possible after the Incident;

(e) filing a police report in case of potential misuse, ransom and/or other criminal activity;

(f) arranging for PDPA training for employees;

(g) publishing a privacy notice / statement on its website; and

(h) demonstrating proper coordination and practices in place; and

(i) appointing a DPO.

16 The majority of the matters raised in mitigation are essentially remediation measures following from the gap analysis that the Organisation had performed. Due consideration had already been given to the prompt action that the Organisation took when the quantum of financial penalty was initially determined. None of the measures warrants an adjustment to the

quantum of the financial penalty. Hence, the Organisation did not provide sufficient justification for the financial penalty to be replaced with a warning.

17 In its representations, the Organisation had provided an explanation for its failure to appoint a DPO. It had sent 2 employees to attend a data protection certification course. The Organisation explained that it did not appoint a DPO at the material time as its employees who attended the Certified Information Privacy Manager ("**CIPM**") course had failed to pass the CIPM exams despite multiple attempts and the Organisation was under the impression that they could not be appointed as DPOs without passing the relevant exams.

18 This misapprehension conflates the obligation to appoint a DPO and what is a reasonable way to go about it. The obligation for organisations to designate a DPO to ensure compliance with the PDPA under section 11(3) of the PDPA is a mandatory requirement under law. In the ideal case, the person appointed would be qualified to perform the role and undertake the responsibilities of a DPO at the time of appointment. The PDPA does not specify what these qualifications are. Furthermore, the pool of qualified DPOs, while growing, is small. There will be many instances where organisations will not be able to identify a member of staff or management who is already qualified. It is, therefore, perfectly acceptable to appoint a DPO and then send her for the necessary courses. In these situations, the Organisation should monitor

the DPO’s progress to ensure that there is no tardiness in completing the courses and achieving the requisite qualification.
