Civil Service Club

[2020] SGPDPC 15

Tan Kiat How, Commissioner — Case No. DP-1907-B4180

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

1 April 2020

Introduction

1 On 2 July 2019, the Personal Data Protection Commission (the "**Commission**") received a complaint from a member (the "**Complainant**") of the Civil Service Club (the "**Organisation**"). According to the Complainant, when he accessed his virtual membership card (the "**Virtual Card**") through the Organisation's membership web portal on the same day – "https://gateway.csc.sg" (the "**Membership Portal**"), he discovered that he was able to access a web directory – "https://gateway.csc.sg/webclub/facilities/tmp" (the "**Directory**"). The Directory contained profile photographs of other members (and their respective NRIC/FIN numbers which were used as file names for their profile photographs), including the Complainant's (the "**Incident**").

Facts of the Case

2 The Organisation is a social club for all Public Service officers in Singapore, and also welcomes staff of Social Service Organisations and the general public to join as associate members. Membership benefits include booking of sports facilities, functions rooms and chalets, as well as members' rates for club events and recreational activities.

3 In October 2009, the Organisation engaged the services of an IT vendor (the "**Vendor**") to develop its Club Management System ("**CMS**"). The Vendor's scope of work was set out in a contract entered into between the parties in November 2009 (the "**Contract**"). The Organisation launched the CMS, including the Membership Portal, in stages. On 1 March 2019, the Organisation launched the Virtual Card on the Membership Portal, and members' NRIC/FIN numbers were used as file names for members' profile photographs.

4 The Organisation has 2 separate servers hosted in its premises – the "enterprise" server (the "**Enterprise Server**") and the "gateway" server (the "**Gateway Server**"). The Organisation stored its business and personal data on the Enterprise Server. The Gateway Server was specifically deployed to isolate the rest of the Organisation's network (which may contain personal data or business data) from the public.

5 When a member accessed his/her Virtual Card, the software on the Membership Portal retrieved a copy of the member's profile photograph from the Enterprise Server and stored it temporarily in the Directory. The Directory resided in the Gateway Server. The files in the Directory (including members' profile photographs) were designed such that they could not be accessed by the public. If the member logged out from the Membership Portal, his/her profile photograph would be deleted from the Directory at that point in time. However, if the member closed the web browser directly without logging out of the Membership Portal, his/her profile photograph in the Directory would only be deleted during the monthly "housekeeping" process. Other than members' profile photographs stored temporarily in the Directory (and their respective NRIC/FIN numbers which were used as file names for their profile photographs), the Gateway Server did not contain any other personal data.

6 Prior to the Incident, there was an issue arising from members submitting their profile photographs in different file formats and sizes for the Virtual Card. The Vendor planned to monitor the situation for three months until 9 July 2019 and troubleshoot the issue during this period.

7 At first, the Vendor attempted to perform troubleshooting in a test environment using dummy photographs. However, the test environment could not replicate the issue with the Virtual Cards. In order to observe members'

behaviour patterns when they accessed their Virtual Cards and to collect statistics on photograph file sizes and time of creation, the Vendor enabled public access to the Directory on 3 occasions so that it could perform troubleshooting remotely. The Vendor also postponed the monthly "housekeeping" process for the Directory by pushing it back from June 2019 to July 2019.

8 The Vendor only required a few minutes of remote access to perform remote troubleshooting, and had, as part of its testing procedures, a requirement that engineers restore all changes made during testing. On the first 2 occasions, public access to the Directory was disabled within 15 minutes. However, on 24 June 2019 (i.e. the 3rd occasion of remote troubleshooting), the Vendor's engineer omitted to disable public access to the Directory but erroneously reported that he had done so. As a result, approximately 1,770 members' profile photographs (and their respective NRIC/FIN numbers which were used as file names for their profile photographs) (the "**Members Data**") could be accessed by anyone who obtained the URL to the Directory, including the Complainant on the date of the Incident.

9 Upon being notified of the Incident, the following remedial actions were taken:

(a) The Organisation and the Vendor took immediate action to disable access to the Directory;

(b) The Vendor enhanced the "housekeeping" processes for the Directory such that the members' profile photographs are deleted immediately after displaying them on the respective members' Virtual Cards (i.e. there are no files containing members' profile photographs stored in the Directory at any time); and

(c) The Organisation discontinued the use of NRIC/FIN numbers as membership numbers, and the members' profile photographs are no longer named using NRIC/FIN numbers.

The Commissioner's Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the PDPA

10 As a preliminary point, the Organisation owned the Enterprise Server and Gateway Server, and was in possession and control of the Members Data at all material times. While the Organisation had engaged the Vendor to develop the CMS, which included the Membership Portal, the scope of the Vendor's work did not involve processing of any personal data on behalf of the Organisation. The Vendor was therefore not a data intermediary, and the responsibility to protect the Members Data fell squarely on the Organisation.

11 Section 24 of the Personal Data Protection Act 2012 ("**PDPA**") provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or similar risks (the "**Protection Obligation**"). The Organisation failed to put in place reasonable security arrangements to protect the Members Data for the reasons explained below.

12 As mentioned at [3], the Organisation started engaging the Vendor's services in October 2009. The Contract between the parties was entered into before the PDPA came into full force on 2 July 2014 (the "**Appointed Day**"). Before the Appointed Day, the Data Protection Provisions of the PDPA (i.e. Parts III to VI of the PDPA) were not in force, and the Organisation was not subject to these provisions in relation to personal data in its possession or control. However, after the Appointed Day, it became incumbent on the Organisation to take proactive steps to comply with the Data Protection Provisions of the PDPA in respect of the existing personal data held in its possession or control, as well as any new personal data that may come into its possession or control. It was not enough for the Organisation to leave matters

status quo, if this would not enable it to meet the requirements and standards of the Protection Obligation.[1]

13 In the present case, the Commission's investigations revealed that after the Appointed Day, the Organisation's engagement of the Vendor's services included work in relation to the developing and troubleshooting of the Virtual Cards on the Membership Portal. According to the Organisation, it was not aware that (i) Members Data had been stored temporarily in the Directory; and (ii) the Vendor's troubleshooting involved enabling public access to the Directory. Notwithstanding this, given that the Organisation's engagement of the Vendor's services included work in relation to the Virtual Cards that contained Members Data, the Vendor (although not engaged to process the Members Data) may nevertheless handle the Members Data incidentally or make software system design decisions that affect the security of the Members Data in the course of providing its services.

14 In the circumstances, and in order for the Organisation to comply with the Protection Obligation, the Organisation should have ensured that it provided sufficient clarity and specifications on requirements to the Vendor (when developing and troubleshooting the CMS, Membership Portal and Virtual

[1] See *Re Social Metric Pte Ltd* [2017] SGPDPC 17 at [10] – [11].

Cards) to protect the Members Data. There are various ways that the Organisation could have done so:

(a) The Contract was entered into by the parties before the Appointed Day and did not contain any provisions on the protection of personal data.[2] In view of the scope of services provided by the Vendor after the Appointed Day as set out at [13], the Organisation could have reviewed the Contract to include clauses setting out requirements for the Vendor to protect the Members Data. As highlighted in the Commission's *Guide on Building Websites for SMEs* (revised 10 July 2018) at [4.2.1], organisations should emphasize the need for personal data protection to their IT vendors by making it part of their contractual terms. In this regard, the Organisation could have adapted relevant clauses from the Commission's *Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data* (published 20 July 2016) to suit the Organisation's particular circumstances and needs.

(b) Further and/or in the alternative, the Organisation could have reviewed and revised the requirements specifications and software

[2] The Contract contained only a confidentiality clause requiring each party to protect information identified by the other party as confidential.

systems design documentation to include (i) requirements relating to how personal data (including the Members Data) should be handled as part of the design and layout the CMS and the Membership Portal;[3] and (ii) technical and other measures that protect the personal data (including the Members Data).

15 From the Appointed Day, the Organisation's failure to take any reasonable steps to ensure sufficient obligations are imposed on the Vendor (when developing and troubleshooting the CMS, Membership Portal and Virtual Cards) to protect the Members Data was a breach of its obligations under section 24 of the PDPA. A period of about five years had elapsed since 2 July 2014 to 2 July 2019. The Organisation, as owner of the CMS, should have included it as part of its personal data asset inventory and ensured that its data protection policies covered personal data held in the CMS. Had this been done, the Organisation would have identified these gaps in the business requirements for the CMS, which would have set it down the path to rectifying these gaps through one or both of the options discussed in the preceding paragraph. The Organisation, as owner of the CMS, is responsible for identifying the omission and articulating its business requirements relating to the protection of personal data stored in the CMS. This would have led to action by the Vendor in

[3] See Commission's *Guide on Building Websites for SMEs* (revised 10 July 2018) at [4.2.1].

recommending technical fixes to enhance the CMS. It is the failure to identify the omission and articulate business requirements, and for a not-trivial period of five years, that is the gravamen of the Organisation's breach of the PDPA.

The Commissioner's Directions

16 In determining the directions, if any, to be imposed on the Organisation under Section 29 of the PDPA, the Commissioner took into account the following mitigating factors:

(a) The Organisation cooperated with investigations;

(b) There was limited risk to the Members Data arising from the Incident because (i) there was only one complaint received; and (ii) even if the Incident had not occurred, the Directory's exposure to public access would have been discovered and rectified by 9 July 2019 because the Organisation and Vendor had planned to carry out a security audit on that date; and

(c) The Organisation took prompt remedial action to rectify the Incident.

17 Having considered all the relevant factors of this case, the Commissioner directs the Organisation to pay a financial penalty of S$20,000 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 it is paid in full. The Commissioner has not set out any further directions given the remediation measures already put in place.
