PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 13

Case No. DP-1904-B3731

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

And

Singapore Telecommunications Limited

… *Organisation*

DECISION

Singapore Telecommunications Limited

[2020] SGPDPC 13

Yeong Zee Kin, Deputy Commissioner — Case No. DP-1904-B3731

5 August 2020

Introduction

1 On 28 March 2019, Singapore Telecommunications Limited (the "**Organisation**") was notified by a customer of an issue with its MySingtel mobile application (the "**Mobile App**") – customers were able to view on the Mobile App their previously assigned service numbers[1] (the "**Recycled Numbers**") and the related usage information of other customers who were the current users of the Recycled Numbers (the "**Incident**"). The Organisation notified the Personal Data Protection Commission (the "**Commission**") of the Incident on 17 April 2019.

Facts of the Case

2 The Organisation is a multinational telecommunications conglomerate headquartered in Singapore. Through the Mobile App, the Organisation's customers can conveniently manage the Organisation's services including (but

[1] The service numbers comprised mobile phone numbers, user IDs for the Organisation's broadband internet services and service numbers for the Organisation's TV services.

not limited to) the payment of their bills, keeping track of their local mobile data usage, talk time and SMS, subscribing to a roaming plan to suit their travel needs etc. Communications between the Mobile App and the Organisation's servers are conducted via an Application Programming Interface ("**API**"). This would include the retrieval of active service numbers associated with a user of the Mobile App.

3 The Organisation engaged a software services provider who was in charge of developing and introducing code changes for the purpose of code updates to the API (the "**Vendor**"). As part of a scheduled code update on the day of the Incident, the Vendor made changes to the API code. In addition, the Vendor also conducted code optimisation by running a tool called SonarQube, which identifies and recommends inefficient code for removal. On this particular occasion, SonarQube recommended the removal of the code which governed the condition that decoupled Recycled Numbers from their previous users (the "**Condition**"). The Vendor followed SonarQube's recommendation and removed the Condition.

4 Before the code changes were deployed to production, the Vendor raised a Technical Change Request form ("**TCR**") to notify the Organisation of the changes made. However, the Vendor omitted to report the removal of the Condition in the TCR submitted to the Organisation.

5 Prior to accepting the code changes to the API for deployment, the Organisation conducted business user acceptance testing for business needs and regression testing for existing functionality. Given that this was a scheduled code update, these tests were limited in scope to the changes reported in the TCR. As the removal of the Condition was not reported in the TCR, the Organisation was unaware of this change, and did not conduct testing on the

impact to the operation of the Mobile App due to removal of the Condition. Following the pre-launch testing, the code changes were approved by the Organisation for deployment.

6 The removal of the Condition led to the API retrieving both active and Recycled Numbers associated with a user of the Mobile App, resulting in the Incident. According to the Organisation, 384 of its customers were affected by the Incident (the "**Affected Individuals**"). The following types of personal data of the Affected Individuals' that was at risk of unauthorised access through the Mobile App included (collectively, the "**Personal Data Sets**"):

(a) Recycled Numbers[2];

(b) Installation addresses of those Affected Individuals who subscribed to the Organisation's broadband and TV services;

(c) Usage details including mobile phone talk time, number of text messages sent and amount of mobile data used;

(d) Value-added services subscribed to;

(e) Price plans of the various services subscribed to; and

(f) Billing cycles for the Recycled Numbers.

[2] There was a total of 404 unique Recycled Numbers belonging to the Affected Individuals.

7 Upon being notified of the Incident, the Organisation promptly carried out the following actions to mitigate the effects of the Incident:

(a) Blocked access to the Mobile App a few hours after being notified of the Incident;

(b) Implemented a fix for the Mobile App the day after the Incident, and restored access to the Mobile App; and

(c) Reversed five erroneous transactions relating to roaming and callerID that were processed during the Incident.

8 In addition, to prevent a recurrence of the Incident or similar risks:

(a) The Organisation will be implementing additional regression test scenarios which will cover testing of Recycled Numbers;

(b) The Organisation has also implemented the following enhancements on the Mobile App:

(i) To prevent any historical services from being retrieved and displayed on the Mobile App, only active services will be displayed moving forward; and

(ii) Enhanced the Mobile App to ensure that only information retrieved for the customer's identifiers in the authenticated session is displayed on the Mobile App.

Findings and Basis for Determination

9 As a preliminary point, the Organisation owned the Mobile App and was in possession and control of the Personal Data Sets. The Vendor's role, in the context of the Incident, was to develop and introduce code changes to the API

for the purposes of the code update. The Vendor did not process the Personal Data Sets on behalf of the organisation and was accordingly not a data intermediary. In the circumstances, the responsibility to protect the Personal Data Sets fell squarely on the Organisation.

10 Section 24 of the Personal Data Protection Act 2012 (the "**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**").

11 As highlighted in previous decisions[3], an organisation is not required to provide an absolute guarantee for the protection of personal data in its possession. What is expected of the organisation is to make such security arrangements as a reasonable person would consider appropriate, given the nature of the personal data involved and the particular circumstances of the Organisation. The Protection Obligation is not automatically breached upon the occurrence of a data leak, and this case is an example of an application of this principle.

12 The Commission's investigations revealed that the security arrangements put in place by the Organisation to protect the Personal Data Sets was reasonable in the circumstances for the reasons explained below.

---

[3]*Re Tiger Airways Singapore Pte Ltd* [2017] SGPDPC 6 and *Re BHG (Singapore) Pte Ltd* [2017] SGPDPC 16.

(a) First, the Organisation emphasized to the Vendor the need for personal data protection of the Organisation's customers by making it part of the contractual terms in the Statement of Works[4]. Specifically, the Statement of Works contained data protection clauses requiring the Vendor to establish security processes and actively enforce policies addressing personal data protection, follow industry standard measures to protect the Organisation's customers' personal data, and exercise the same degree of care to guard against unauthorised disclosure. In addition, the Organisation verified the data protection arrangements put in place by the Vendor to protect its customers' data[5]. This included conducting audits on the Vendor to ensure the adequacy and effectiveness of IT controls and processes implemented by the Vendor, and to ensure that the Vendor's staff conformed to the said IT controls and processes. Further, in order to increase its vendors' knowledge and awareness of the PDPA's requirements, the Organisation also conducted mandatory annual briefings for its vendors on the PDPA, the Organisation's cybersecurity policy for third party vendors as well as information security. These annual briefings were attended by the Vendor's employees.

---

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

[5] *cf. Re SCAL Academy Pte Ltd* [2020] SGPDPC 2 at [8]: Organisation instructed its vendor to prevent documents from being "leaked" online, but did not check with its vendor what security arrangements were put in place to ensure this.

(b) Second, the Organisation ensured that the pre-launch tests for code changes were reasonably scoped to pick up and rectify errors and/or flaws prior to deployment.

(i) The Organisation had conducted business user acceptance testing based on the change requests set out by the Vendor in the TCR. As mentioned at [5], there was no testing conducted on the impact to the operation of the Mobile App due to removal of the Condition – the Organisation was not aware of the removal of the Condition because it had not been reported in the TCR. Given that there was no reason for the Organisation to suspect any additional code changes in a scheduled routine code update, it was reasonable for the Organisation to perform testing only on those changes set out in the TCR[6].

(ii) As part of its quality assurance measures, the Organisation conducted various testing of critical business functions of the Mobile App, including user acceptance testing and regression testing. The results from the tests were reviewed by directors in the Organisation's business and IT departments before the code changes were approved for deployment to the Mobile App.

---

[6]*cf:* The Commission's previous decisions where organisations were found in breach of Section 24 of the PDPA for not conducting sufficiently scoped pre-launch tests before introducing new changes to its systems that processed personal data. See for example: *Re Flight Raja Travels Singapore Pte Ltd* [2018] SGPDPC 18 (organisation introduced a new mobile application) and *Re Singapore Telecommunications Limited* [2019] SGPDPC 49 (organisation migrated its database of customer accounts to a new billing system).

13 In conclusion, nothing in the Commission's investigations pointed to the cause of the Incident being due to a systemic problem in the Organisation's measures to protect the Personal Data Sets. Instead, this appeared to be a one-off incident that was difficult to foresee in the circumstances. Having carefully considered all the relevant circumstances and for the reasons set out above, I find that the Organisation had not contravened its obligations under section 24 of the PDPA.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION