DECISION OF THE
PERSONAL DATA PROTECTION COMMISSION

Case Number: DP- 1603-A652

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

And

(1) Singapore Telecommunications Limited (UEN No. 199201624D)

(2) Tech Mahindra (Singapore) Pte Ltd (UEN No. 200203658M)

... Organisations

Decision Citation: [2017] SGPDPC 4

GROUNDS OF DECISION

06 April 2017

1. This is a case where an error made by the 2nd Organisation in updating a database resulted in the personal particulars of a single customer ("**Affected Customer**") replacing personal particulars in the profiles of numerous users of Singapore Telecommunications Limited ("**Singtel**"). Consequently, the Affected Customer's personal particulars could be viewed by the other Singtel customers on the MySingtel mobile application ("**MySingtel Application**") and the MyBill (mybill.singtel.com) and MyAccount (myaccount.singtel.com) portals on Singtel's website.

2. The main issue in the investigation was whether the Organisations breached their Protection Obligation under Section 24 of the Personal Data Protection Act 2012 ("**PDPA**"). The following sets out the Commission's findings on the matter.

A. MATERIAL FACTS

3. Singtel is a telecommunications company that had, as part of its services, a single sign on service for its customers, allowing them to use the same access credentials to access his or her different Singtel accounts and bills across

Singtel's applications and portals. This service is known as ONEPASS. Singtel had engaged Tech Mahindra, an Information Technology ("**IT**") vendor, to provide application development, maintenance and support services for ONEPASS ("**ADMS Services**"). This includes updating customer profiles in the ONEPASS database.

4. The genesis of this matter can be traced to when Singtel and Tech Mahindra had sought to rectify an issue with the Affected Customer's ONEPASS account. On 26 February 2016, the Affected Customer had informed Singtel about the login difficulties with his ONEPASS account. Following this, Singtel escalated the Affected Customer's issue to Tech Mahindra. Tech Mahindra subsequently determined that an update was needed to the Affected Customer's profile on the ONEPASS database, and executed a database script to update the profile.

5. On 29 February 2016, Singtel received several reports from ONEPASS users. These affected different systems in different ways. Some customers reported that their MySingtel Application profile had been modified to reflect the Affected Customer's account number, billing address and services. A number of Singtel customers also reported that the NRIC field in their ONEPASS profiles on the MyBill and MyAccount portals had been modified to reflect the Affected Customer's NRIC number. Apart from these, all other personal details of the user, such as the user's name and address, remained unaffected.

6. A total of 2.78 million ONEPASS users' accounts were affected, out of which 2,518 users had viewed the Affected Customer's NRIC number through the MySingtel Application before Singtel disabled access to the MySingtel Application.

7. Shortly after receiving reports of the incident, Singtel shut down the MySingtel Application and disabled access to the ONEPASS profile webpages on the MyBill and MyAccount portals. Singtel also notified the Affected Customer of the incident.

8. Singtel's investigations disclosed that the incident was caused by a coding issue in the database script that was executed by Tech Mahindra. The Tech Mahindra employee who prepared the database script had omitted a "where" clause in the script, which was required to limit the application of the changes to the Affected Customer's profile. This was in breach of standard operating procedures that were in place at that time.

B. COMMISSION FINDINGS AND BASIS FOR DETERMINATION

Issues for determination

9. The issues to be determined by the Commission are as follows:

   (a) whether Tech Mahindra was acting as a data intermediary for Singtel in relation to the ONEPASS users' personal data; and

   (b) whether each of the Organisations complied with its obligation under Section 24 of the PDPA in respect of the Data Breach Incident.

Issue (a): Whether Tech Mahindra was acting as a data intermediary for Singtel in relation to the ONEPASS users' personal data?

10. Tech Mahindra was engaged by Singtel to provide ADMS Services, which covered a range of support activities such as troubleshooting, incident management, and application maintenance services, including ONEPASS and single sign on services. Crucially, Tech Mahindra was also granted access to Singtel's database to maintain customer profiles on the ONEPASS database. The maintenance of customer profiles amounts to "processing" personal data on behalf of Singtel. Accordingly, it was acting as a data intermediary (as defined in Section 2(1) of the PDPA) of Singtel.

11. A data intermediary has a duty to comply with the Protection Obligation under Section 4(2) of the PDPA. At the same time, the organisation has the same obligation in respect of personal data processed by a data intermediary on its behalf and for its purposes as if the personal data were processed by the organisation itself under Section 4(3) of the PDPA.

12. In accordance with Sections 4(2) and (3) of the PDPA, both Singtel and Tech Mahindra have concurrent obligations to make reasonable security arrangements to protect the personal data of Singtel customers that are in their possession and/or under their control.

Issue (b): Whether each of the Organisations complied with its obligation under Section 24 of the PDPA in respect of the Data Breach Incident?

Singtel

13. In this case, the Commission finds Singtel to have complied with its obligation under Section 24 of the PDPA to put in place reasonable security arrangements to protect personal data.

14. First, Singtel had put in place a contract requiring Tech Mahindra to comply with the PDPA, adhere to all of Singtel's access and security policies, processes and directions, and to ensure that its employees are trained to comply with all data protection laws and security measures before it is given control and access to the personal data in Singtel's systems. Having a contract that sets down the obligations and responsibilities of a data intermediary to protect personal data is a prudent first-step for organisations to take. One of the key benefits of having such a contract is that it would make clear the parties' respective roles, obligations and responsibilities to protect the personal data.

15. Second, Singtel had also followed through with operational procedures and checks to ensure that Tech Mahindra carried out its functions to protect personal data. Singtel and Tech Mahindra had a standard operating procedure ("**SOP**") governing the management of the ONEPASS database. If a database script change was required, the employee making the change was required to run the database script in the development environment before running the database script in the actual production environment. In this way, any errors or issues arising from the database script are contained in the test-bedding environment without impacting on or affecting the live system. This enables an organisation to detect and rectify any issues or errors in the script before the actual implementation.

16. Singtel had also given Tech Mahindra specific instructions for the updating of the Affected Customer's profile on the ONEPASS database. In an email on 2 April 2015, Singtel made specific reference to the "where" clause in the database script and gave specific instructions that the "where" clause of each database update script had to be a primary key, i.e. it could not be left blank. The function of the "where" clause is to introduce a restrictive parameter on the operation of the programmatic instructions to specific records, columns or tables in the database. In this case, by specifying the Affected Customer's record in the "where" clause, the database script would have selected only his record for the operation.

17. Third, Singtel conducted annual on-site security reviews of Tech Mahindra's off-site premises as part of its governance process and required Tech Mahindra to confirm its compliance with various security protocols. Singtel also conducted penetration tests on the MySingtel Application, the MyAccount and MyBill portals as well as the ONEPASS system and fixed the vulnerabilities, which were unrelated to the data breach incident, found during the penetration tests.

18. In light of the above, the Commission finds that Singtel made reasonable security arrangements in compliance with the Protection Obligation under Section 24 of the PDPA.

Tech Mahindra

19. The Commission, however, finds Tech Mahindra to be in breach of its obligation, as a data intermediary, under Section 24 of the PDPA.

20. The Commission finds that even though there were in place internal SOPs and policies regarding the modification or processing of personal data in the ONEPASS database by Tech Mahindra, it failed to comply with them during the actual handling and management of the personal data.

21. First, notwithstanding Singtel's email instructions to include the "where" clause in the database script, Tech Mahindra failed to comply with the instructions, and left it out from the database script.

22. Second, Tech Mahindra did not comply with Singtel's SOP highlighted at paragraph 15 above. Tech Mahindra did not check that the database script was functioning properly in a test-bedding environment before execution in the production environment. Consequently, the personal data of 2.78 million ONEPASS users' personal data was modified and replaced by personal data from the Affected Customer when Tech Mahindra executed the database script containing the erroneous code.

23. Third, although Tech Mahindra implemented internal security arrangements, it did not adhere to its own SOPs. Tech Mahindra had a practice (which was not documented) for the database update script to be reviewed by a more senior member of the support team before execution. Additionally, employees were also expected to verify that an update was correct after the execution of the database update script. However, in this case, both these layers of checks were omitted.

24. In the Commission's assessment, given the above failures and missteps, Tech Mahindra failed to make reasonable security arrangements to protect the personal data of Singtel customers that it processed on behalf of Singtel. Accordingly, Tech Mahindra is in breach of Section 24 of the PDPA.

C. THE COMMISSION'S DIRECTIONS

25. In exercise of the power conferred upon the Commission pursuant to Section 29 of the PDPA, the Commission directs that Tech Mahindra pay a financial penalty of S$10,000 within thirty days from the date of the Commission's direction.

26. In assessing the breach and remedial directions to be imposed, the Commission considered various factors relating to the case, including the mitigating and aggravating factors set out below:

(a) the personal data disclosed in the data breach incident, particularly the Affected Customer's NRIC number, is of a sensitive nature;

(b) not only was the Affected Customer's NRIC number disclosed without authorisation, there was also an unauthorised modification of the personal data of 2.78 million ONEPASS users;

(c) the data breach incident could have been avoided if Tech Mahindra had followed Singtel and Tech Mahindra's SOPs;

(d) of the 2.78 million ONEPASS users whose accounts had been modified, only 2,518 users had viewed the Affected Customer's NRIC number;

(e) Tech Mahindra and Singtel had jointly notified the Commission of the data breach incident, and was cooperative in the course of the investigation; and

(f) Singtel and Tech Mahindra took prompt remedial and preventative actions.

27. The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA. Organisations should take the necessary action to ensure that they comply with their obligations under the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisations accordingly.

YEONG ZEE KIN
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION COMMISSION