DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1504-A421

METRO PTE LTD [Reg. No. 195700030E]

... Respondent

Decision Citation: [2016] SGPDPC 7

GROUNDS OF DECISION

20 April 2016

BACKGROUND

1. On 21 April 2015, the Complainant, [Redacted] (Replaced with Ms C), complained to the Personal Data Protection Commission (the "**Commission**") that she had been receiving calls from unknown numbers, and that when she conducted a search on Google, she discovered that her personal data and those of her family members were posted online on http://siph0n.net ("**Siph0n website**"). The Complainant had attributed the posting on the Siphon website to a data "leak" on the Respondent's part.

A. MATERIAL FACTS AND DOCUMENTS

2. On account of the complaint made, the Commission undertook an investigation, and sought the Respondent's response on the matter. The material facts of the case are as follows.

3. The Respondent had acknowledged that the personal data that was posted on the Siph0n website came from the database stored on its website, such data comprising personal data of individuals.[1]

4. The Respondent's corporate website was developed and supported by Grey Digital Southeast Asia (also known as Yolk Pte Ltd) ("**Grey Digital**"). The website was hosted by Limebox Hosting Solutions.

5. The Respondent's corporate website (http://www.metro.com.sg) was hacked into on 9 and 10 February 2014. Investigations were subsequently carried out by the Respondent's IT (information technology) support partners, namely Grey Digital and Vodien Internet Solutions Pte Ltd ("**Vodien**"), into the hacking incidents. However, the investigations were unable to determine the cause of the February 2014 hacking incidents or the person(s) that had carried out the hacking(s). The Respondent produced to the Commission a report from Grey Digital in respect of the two hacking incidents ("**Grey Digital's report**"). The Commission understands that the Respondent had taken steps to improve on its web security following the hacking incidents in February 2014.

6. In March 2015, it was discovered that the names, personal email addresses, NRIC numbers, personal mobile phone numbers, dates of birth and Facebook user IDs of the Respondent's customers were disclosed on the Siph0n website. This included the personal data of the Complainant and her family, which forms the subject of the complaint in this matter. The Respondent informed the Commission that the personal data that was posted on the Siph0n website was of 445 of its customers or users of the Respondent's website.

7. Following the March 2015 postings on the Siph0n website, the Respondent instructed Grey Digital to remove any user information from the server of the hacked corporate website.

8. The Respondent also engaged KPMG Singapore to carry out an assessment and audit of the security of its internal as well as external i.e. internet-facing systems. A copy of the report dated 19 May 2015 was produced to the Commission on 10 July 2015 ("**KPMG report**").

9. During its investigations, the Commission was informed by the Respondent that it had resolved several of the IT security issues raised in the KPMG report and that it had intended to address / taken steps to address the remaining issues and to further improve on its website and server security.

B. COMMISSION FINDINGS AND BASIS FOR DETERMINATION

Relevant issue in this case

10. Arising from the posting of personal data on the Siph0n website found in March 2015 and the IT security issues raised in the KPMG Report, the main issue in this case is whether the Respondent had in place reasonable security arrangements to protect the personal data in its possession or control, as required under Section 24 of the PDPA, when it came into effect on 2 July 2014.

11. Section 24 of the PDPA states that an organisation is obliged to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Section 24 of the PDPA came into effect on 2 July 2014.

Assessment of whether Respondent had complied with Section 24 of the PDPA

12. The Commission notes that the Respondent has attributed the postings that were discovered in March 2015 to the two hacking incidents in February 2014. The Respondent thus took the view that there was no further breach for the disclosures on the Siph0n website made in March 2015 following the two incidents. The Commission, however, notes that the Respondent was under an obligation to ensure that reasonable security arrangements were put in place to protect the personal data under Section 24 of the PDPA, when it came into force on 2 July 2014.

13. Despite the Respondent and/or Grey Digital apparently taking steps to improve the security of the Respondent's website and system following the two hacking incidents in February 2014, it was noted that the Respondent's system still contained numerous security issues and vulnerabilities when the security scan was conducted from March 2015 to May 2015. This is evidenced by the KPMG report dated 19 May 2015 that was produced to the Commission by the Respondent.

14. In the KPMG report, KPMG had found 30 issues with the system, comprising of 6 "Significant Issues", 11 "Reportable Issues" and 13 "Observations". Amongst the issues raised, Commission notes that there were 3 significant issues and 1 reportable issue with the external web application security, and 1 reportable issue in relation to the external network security.

15. In this regard, there was at least one signfiicant issue in the KPMG report which is indicative of a failure of reasonable security arrangements even as of 19 May 2015. This is the SQL injection vulnerability. The Commission understands that the SQL injection vulnerability would have been found in the programming code of the Respondent's external web applications, and may have been present in these web applications from the outset. In the Commission's view, this is a common and well-documented form of vulnerability that ought to have been reasonably anticipated, identified and rectified by the Respondent at an early stage.

16. The Commission also notes that even as of 19 May 2015, the Respondent's web servers were accessible to the internet; and hosted the Respondent's website, which is the interface from which the Respondent had collected and stored the personal data from its users or customers. Accordingly, any vulnerability in the web servers or the web applications would pose a real risk or threat to the security of the personal data that was collected and/or held by the organisation. It was therefore imperative that the Respondent take the necessary measures to ensure that the servers and web applications themselves would be secure and free from any known significant security risks or vulnerabilities. The fact that there were a number of issues with the security of the Respondent's IT system, particularly, the SQL injection vulnerability, indicated to the Commission that the web security was lacking. The Commission notes that the personal data from the previously affected database (ie the database which was hacked) was only transferred from the internet-facing webservers after the postings to the Siph0n website in March 2015.

17. Based on the above, the Commission finds that the Respondent had failed to make reasonable security arrangements to protect the personal data held in its web servers, and it is therefore in breach of Section 24 of the PDPA.

C. ACTIONS TAKEN BY THE COMMISSION

18. Given the Commission's findings that the Respondent is in breach of its obligations under Section 24 of the PDPA, the Commission is empowered under Section 29 of the PDPA to give the Respondent such directions as it

deems fit to ensure compliance with the PDPA. This may include directing the Respondent to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

19. In considering whether a direction should be made or given to the Respondent in this case, the Commission notes that:

    a. the Respondent had taken action to strengthen the security of its website, including engaging KPMG to undertake an internal IT security audit and assessment shortly after it had learnt of the posting of its customer's or user's personal data on the Siph0n website. However, the Respondent's actions (after the hacking incidents in February 2014) did not enable it to detect and address at least one significant security lapse until several months later (ie after May 2015).

    b. the data leak that gave rise to the complaint took place before July 2014, and there is no evidence that there has been a data breach to date, notwithstanding the Respondent's failure to make reasonable security arrangements.

20. In view of the factors noted above, the Commission has decided not to issue any direction to the Respondent to take remedial action or to pay a financial penalty. Instead, it has decided to issue a Warning against the Respondent for the breach of its obligations under Section 24 of the PDPA.

21. The Commission emphasises that it takes a very serious view of any instance of non-compliance with the PDPA, and it urges organisations to 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 organisation(s) accordingly.

YEONG ZEE KIN
COMMISSION MEMBER
PERSONAL DATA PROTECTION COMMISSION

---

[1] Personal data" under Section 2 of the PDPA means data, whether true or not, about an individual who can be identifed from that data; or from that data and other information to which the organisation has or is likely to have acess.