PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPCS 3

Case No. DP-2112-B9354

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

And

Fortytwo Pte. Ltd.

… *Organisation*

SUMMARY OF THE DECISION

Data Protection *– Protection obligation – Sensitivity of personal data - Unauthorised access to personal data – Unauthorised disclosure of personal data – Insufficient security arrangements - Failure to patch third-party software*

Data Protection *– Protection obligation - Incomplete, fictitious or pseudonymised data*

[2023 SGPDPCS 3]

SUMMARY OF THE DECISION

1. On 24 December 2021, Fortytwo Pte. Ltd. (the **"Organisation"**), an online furniture store, notified the Personal Data Protection Commission (the **"Commission"**) of malicious code injections on its website which led to the capturing of the email address and password of 6,241 individuals when they logged in to its website (the **"Incident"**). The name, credit card number, expiry date and CVV/CVN number of another 98 individuals' were also affected.

2. The Organisation requested for the matter to be handled under the Commission's expedited breach decision procedure. This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision; and admitted that it was in breach of section 24 of the Personal Data Protection Act (the "**PDPA**").

3. An issue that arose in this case is whether fictitious names or pseudonymous personal particulars form part of the personal data under the possession or control of the Organisation. The importance of this lies in how it may potentially reduce the size of the dataset that was at risk. In their addendum to the Written Statement, the Organisation stated that it does not verify the names provided by the users, and suggested that the impact of the Incident might be more limited as some of the users' names may be incomplete, fictitious or pseudonymous.

4. Section 2(1) of the PDPA defines "personal data" to be data, *whether true or not* (emphasis added), about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. The PDPA

caters for the situation where not every record of personal data that is under the possession or control of an Organisation is verified. It takes a practical approach, as the accuracy of personal data records will change with the passage of time (e.g. information becomes outdated) or individuals may intentionally provide inaccurate information (e.g. users hiding their age or using fictitious residential addresses to bypass restriction of services by age or geolocation). What matters is that the Organisation, having collected the information, takes steps to comply with their obligations under the PDPA, such as to protect them and to ensure that they are used in accordance with the purpose of their collection.

5. The situation is different when the organisation, as a data security or data management measure, applies pseudonymisation or anonymisation techniques on personal data that is in their possession or under their control. In such circumstances, if the risk of reidentification is adequately addressed and managed, the resulting dataset may be treated as anonymised. The key difference is the intention of the organisation and its ability to direct and control the data processing activities required to achieve the resultant anonymised dataset.[1]

6. In this case, the Organisation was collecting data from its customers. Their customer database contained names, email addresses and additional details such as their shipping address, billing address, and date of birth. It also contained credit card details of 98 customers. Even if some customers had provided incomplete, fictitious or pseudonymous personal particulars or payment details, the Organisation had collected personal data. For the purpose of this investigations, it matters not that some of these customers may have provided inaccurate information. The Organisation's obligations under the PDPA applies to the entire customer database.

[1] See Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*, at paras 3.5, 3.8 and 3.13.

7. The Organisation admitted that the Incident occurred because the threat actor had successfully exploited vulnerabilities present in the Magento open-source version 1.9.x.x which the Organisation had employed for its online store. These vulnerabilities were present because the Organisation failed to apply four Magento security patches released on 28 Nov 2017, 25 June 2019, 8 October 2019 and 28 April 2020 by Adobe.

8. Compounding the above, support for Magento version 1 had ended on 30 June 2020. The Organisation admitted that it should have upgraded to Magento open-source version 2.0 after Adobe ended the support for Magento 1 on 30 June 2020. The Organisation had planned to upgrade to Magento version 2 in early 2020, but its plans were disrupted by the COVID-19 pandemic. Having said that, Adobe had announced in November 2015 that it will end support for Magento 1.x in 36 months, i.e. by November 2018. In September 2018, Adobe then announced that it would extend the support to 30 June 2020. Given the ample notice given by Adobe to the Organisation of the need to upgrade the version of Magento Open Source which it was using in order to continue receiving support and security patches from Adobe, it is difficult to look past the Organisation's prolonged failure to do the needful and perform the necessary upgrades.

9. The Commission had consistently advised organisations on the importance of applying software patches. In our Guide to Data Protection Practices for ICT Systems, the Commission had highlighted that organisations should perform system patching promptly to fix security vulnerabilities. If software patches are not updated as recommended by the software provider, they may not contain the latest cybersecurity updates and may compromise the organisation's defence against cyber-attacks.

10. We note that the Organisation had considered and evaluated the four patches but decided to hold back on installing them. However, these four patches were released by Adobe to address several high severity risk issues and critical bugs, including the injection of malicious codes. The Organisation's failure to patch had increased the risks of a malicious code injection capable of capturing users' personal data.

11. In light of the above, the Organisation is found to have breached the Protection Obligation under section 24(a) of the PDPA.

12. The Commission notes that after the Incident, the Organisation took prompt remedial actions, including notifying affected individuals and various technical measures to improve its security. The Organisation is also taking steps to upgrade to Magento version 2.

13. In deciding the appropriate outcome in this case, the Commission considered the Organisation's cooperation throughout the investigation, the voluntary admission of breach of the Protection Obligation, and the prompt remedial actions taken.

14. Following the issuance of the Commission's preliminary decision, the Organisation represented that it was unfair to state that was a prolonged failure to perform the necessary upgrade. This is because there was a lead time of 6 months before the end of support when it made the decision to upgrade, before the COVID-19 pandemic disrupted its plans. The Organisation's representation is not accepted as, notwithstanding the disruptions caused by the pandemic, the Organisation had been given ample notice of the impending end of support but took no action to perform the necessary upgrade from November 2015 to early 2020.

15. Having considered the circumstances set out above, the factors listed at section 48J(6) of the PDPA and the representations made by the Organisation, the Deputy Commissioner for Personal Data Protection hereby finds the Organisation in breach and directs the Organisation to pay a financial penalty of S$8,000 within 30 days from the notice accompanying date of this decision, failing which interest at the rate specified in the Rules of Court in respect of judgement debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

16. The Organisation is also directed to:

a. Complete the upgrading of its website to a supported software version, including vulnerability assessment and penetration testing, within 6 months of the direction.

b. Inform the Commission with 14 days of the completion of the above.

The following is the provision of the Personal Data Protection Act 2012 cited in the above summary:

Protection of personal data

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.