PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPCS1

Case No. DP-2202-B9480

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

And

Kingsforce Management Services Pte Ltd

SUMMARY OF THE DECISION

1. On 31 January 2022, the Personal Data Protection Commission (the **"Commission"**) was notified by Kingsforce Management Services Pte Ltd (the **"Organisation"**) of the sale on RaidForums, on or about 27 December 2021, of data from its jobseeker database (the "**Incident**").

2. The affected database held approximately 54,900 jobseeker datasets, comprising name, address, email address, telephone number, date of birth, job qualifications, last and expected salary, highest qualification and other data related to job searches.

3. External cyber security investigators identified outdated website coding technology, with critical vulnerabilities, as the cause of the Incident.

4. The Commission accepted the Organisation's request for handling under the Commission's expedited breach decision procedure. The Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision, and to breach of section 24 of the Personal Data Protection Act ("the **PDPA**").

5. The Organisation admitted work had not been completed on the website at launch owing to contractual disputes with the developer. The Organisation subsequently engaged IT maintenance vendors in an effort to ensure the security of the website. However, maintenance had been ad-hoc and limited to troubleshooting functionality issues from bugs, glitches and/or when a page failed to load.

6. In breach of the Protection Obligation, the Organisation failed to provide sufficient clarity and specifications to its vendors on how to protect its database and personal data. In *Re Civil Service Club*, the Commission had pointed out that organisations that engage IT vendors can provide clarity and emphasize the need for personal data protection to their IT vendors by a) making it part of their contractual terms, and b) reviewing the requirements specifications to ensure that personal data protection is reflected in the design of the end-product.[1] Further, post-execution of the contract, an organization is also expected to exercise reasonable oversight over its vendor during the course of the engagement to ensure that the vendor is protecting the personal data by adhering to the stipulated requirements.[2]

[1] Re *Civil Service Club* [2020] SGPDPC 15.
[2] *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317 at [16] and [17].

7. Another breach of the Protection Obligation by the Organisation was failure to conduct reasonable periodic security reviews, including vulnerability scans, since the launch of its website. The requirement for and scope of reasonable periodic security reviews had long been established in the published decisions of the Commission.[3] The PDPC's Guide to Data Protection Practices for ICT Systems also emphasized the need to periodically conduct web application vulnerability scanning and assessments, post deployment, as a basic practice to ensure compliance with the Protection Obligation under the PDPA.[4]

8. The Organisation is therefore found to have breached the Protection Obligation under section 24(a) of the PDPA.

9. In deciding the enforcement action in this case, the Commission considered the Organisation's efforts towards website security, cooperation throughout the investigation, voluntary admission of breach of the Protection Obligation and the prompt remediation taken. The last included immediate suspension of its website, and the engagement of a new developer to develop a new and enhance web application. The Commission also notes that the affected personal data was no longer or accessible following the shutdown of RaidForums. In the circumstances, the Commission directs the Organisation to do the following:

    a. To submit to the Commission, within twenty-one (**21**) days from the date of issue of this Direction, a plan to ensure regular patching, updates and upgrades

[3] See, *eg*, *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317; *Re Bud Cosmetics Pte Ltd* [2019] PDP Digest 351; and *Re Watami Food Service Singapore Pte Ltd* [2019] PDP Digest 221.
[4] Pages 21 and 22 of the Guide to Data Protection Practices for ICT Systems.

for all software and firmware supporting its website(s) and applications through which personal data in its possession may be accessed.

b. To state whether it intends to implement the plan by engagement of qualified external services or by relying on its own resources, and if by engagement of qualified external services, to state in detail the job specifications for software and firmware patching, updates, and upgrades to be stipulated to the vendor.

c. To outline each implementation step with deadlines to ensure that the entire implementation is completed within sixty (**60**) days from the date of issue of this Direction.

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 is possession or under its control by making reasonable security arrangements to prevent-

(a) unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks; and
(b) the loss of any storage medium or device on which personal data is stored.