PERSONAL DATA PROTECTION COMMISSION

[2018] SGPDPC [12]

Case No DP-1711-B1312

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

And

Watami Food Service Singapore Pte Ltd

… *Organisation*

DECISION

Watami Food Service Singapore Pte Ltd

[2018] SGPDPC [12]

Mr. Yeong Zee Kin, Deputy Commissioner — Case No DP-1711-B1312

14 May 2018

1. Watami Food Service Singapore Pte Ltd (the "**Organisation**") is in the restaurant business. On 10 November 2017, information was received the Organisation's internal Staff Code Name List (the "**List**") was accessible via its website. The List contained personal data of 405 employees of the Organisation, namely their full names and staff codes.

2. The List was to facilitate the entry of new employee staff codes into the Organisation's point-of-sale system. This information is not current as it was dated between 2009 and 2013. The List was meant for internal use within the Organisation.

3. The Organisation did not know when or why the List was uploaded into the Organisation's website server. As there was no restriction on access, the List was indexed by search engines and made publicly searchable online. The URL containing the List was subsequently removed by Fairwin International Limited ("**Fairwin**"), a vendor the Organisation engaged to maintain its website.

4. The Organisation was in possession and/or control of the personal data in the List. Section 24[1] of the Personal Data Protection Act ("**PDPA**") required the Organisation to protect the personal data in the List. This included protection against risk of unauthorised access.

5. I rely on the common law concept of *res ipsa loquitur* in this case as the Organisation is unable to explain how the List which it maintained for internal use was uploaded onto its

[1] Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

website. The Organisation also did not exercise reasonable control of the information on its website, since it was not aware that the List has been accessible on its website and searchable via online search engines.

6. Neither did it adopt reasonable steps to monitor against information leak on its website. The period that the List was thus exposed could possibly have commenced from 2013, but could also have been a shorter period. The Organisation's poor oversight and control did not enable it to establish the period of exposure. As a result, the personal data of its staff remained on its website undetected until being contacted by the PDPC. Exercising better oversight of its website content could have led to an earlier discovery and removal of the URL giving access to the List.

7. In the course of investigations, it was further discovered that the Organisation failed to train its staff to protect the personal data in its possession or control. The Organisation's privacy policy included proper personal information management. However, its staff were not trained in protecting personal data other than occasional reminders, for example to use alphanumeric passwords. No formal instructions were given to staff on the Organisation's data protection policies or other forms of data protection training.

8. Accordingly, I find that the Organisation did not put in place reasonable security arrangements to protect personal data in its possession or control against risk of unauthorised access. The Organisation is therefore in breach of section 24 of the PDPA.

9. In assessing the breach and determining the directions to be imposed on the Organisation, I took into account the following:

    a. The Organisation's prompt instruction to Fairwin to delete the URL on its website;

    b. The Organisation's cooperation in the investigation; and

    c. Its remedial measures, where the Organisation restricted access to the website server to only one person, also reminded all staff that all documents containing sensitive personal data should be password-protected and not be uploaded online.

10. In view of the factors noted above, I have decided to issue a warning to the Organisation for the breach of its obligation under section 24 of the PDPA as neither further directions nor a financial penalty is warranted in this case.

YEONG ZEE KIN
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION COMMISSION