PERSONAL DATA PROTECTION COMMISSION

[2018] SGPDPC 20

Case No DP-1805-B2096

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

And

Dimsum Property Pte. Ltd.

… Organisation

DECISION

Dimsum Property Pte. Ltd.

[2018] SGPDPC 20

Yeong Zee Kin, Deputy Commissioner — Case No DP-1805-B2096

21 August 2018

Background

1 The complaint concerns the failure to protect the personal data of individuals in the possession or under the control of Dimsum Property Pte. Ltd. (the "**Organisation**"). The Organisation operated a website www.snappyhouse.com.sg (the "**Website**"), providing a platform for homeowners to sell and rent out property directly to others.

2 The Complainant was a member of the public who had visited the Website. On 9 May 2018, the Complainant filed a complaint with the Personal Data Protection Commission (the "**Commission**") that images of identification documents were made publicly accessible on the Website through 2 Web directories (or folders):

a. www.snappyhouse.com.sg\templates\bootstrap2-responsive\assets\images\avatar (the "**Avatar Directory**"); and

b. www.snappyhouse.com.sg\templates\bootstrap2-responsive\assets\images\indentity (the "**Identity Directory**").

Material Facts

3 The Avatar Directory contained images uploaded by registered users on the Website as their profile avatars. These images included photographs of individuals, and one even included a photograph of a user's passport. The Organisation intimated that image of the passport may have been intentionally or erroneously uploaded by the user.

4 The Identity Directory contained images of identification documents uploaded by 30 registered users for verification purposes. The Organisation had been collecting and storing these documents in the folder since November 2015, until the Website was taken down on 24 May 2018.

5 In total, the personal data of 31 individuals were accessible to the public. The passport image in the Avatar Directory and the 30 identification documents in the Identity Directory disclosed personal data such as individuals' name, photograph, address, passport number, NRIC number, thumbprint, date of birth, place of birth, gender, nationality, and date of issue/expiry of passport.

6 The Organisation had engaged the services of an overseas vendor (the "**Vendor**") to design and develop the Website. The completed Website was delivered in November 2015. No personal data had been transferred to the Vendor for the development of the Website.

7 The Organisation subsequently hired its own in-house developers in November 2015. The in-house developers took over the development and administration of the Website in January 2016. However, there was no further update or development of the Website since July 2016, and users continued to register on the Website and use the Website's functions until March 2018. The

Website was taken down by the Organisation on 24 May 2018 and is no longer accessible. The Organisation was unclear if the Identity Directory had been publicly accessible at the time when the Website was delivered by the Vendor, or had been made publicly accessible by its own in-house developers.

8 The Organisation was in possession and control of the personal data that appeared on the Website. Section 24[1] of the Personal Data Protection Act 2012 ("**PDPA**") therefore required the Organisation to make reasonable security arrangements to protect the personal data, which included protecting against the risk of unauthorised access. Moreover, the protection obligation did not extend to the Vendor as the Vendor did not process any personal data on behalf of the Organisation and was not a data intermediary. The Organisation therefore retained full responsibility for the IT security of its website, and the personal data contained within.

Findings and Basis for Determination

9 The issue was whether the Organisation had made reasonable security arrangements to protect the personal data of its customers that was in its possession and control. The Organisation admitted that it was unaware of the need to protect the personal data that it stored in the web directories. This, in turn, resulted in the Organisation's failure to implement reasonable security arrangements to protect the personal data it had collected and kept in the 2 web directories. The Organisation should have protected the personal data by

[1] Section 24 of the PDPA requires organisations to protect personal data in their possession or under their control. They are required to make reasonable security arrangements against unauthorised access, collection, modification and other risks listed in section 24.

implementing access controls to limit web access to the 2 web directories to authorised users.

Conclusion

10 In light of the above, 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. In assessing the appropriate enforcement action in this case, I took into account the following:

a. The Organisation's prompt actions to remove the personal data from public access;

b. The number of individuals affected;

c. The impact of the breach; and

d. The Organisation had ceased operations of the Website.

11 Having considered these factors, I have decided to issue a warning to the Organisation for the breach of its obligation under section 24 of the PDPA without any directions or financial penalty.

YEONG ZEE KIN
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION