Jade E-Services Singapore Pte. Ltd.

[2018] SGPDPC 21

Yeong Zee Kin, Deputy Commissioner — Case No DP-1801-B1632

Data Protection – Protection obligation

11 September 2018.

Background

1 The complaint concerns the failure to protect the personal data of individuals in the possession or under the control of Jade E-Services Singapore Pte. Ltd. (the "**Organisation**"). The Organisation is in the online clothing retail business and operates the e-commerce fashion retail website www.zalora.sg (the "**Website**") in Singapore.

2 The Complainant was a customer of the Organisation. She filed her complaint with the Personal Data Protection Commission (the "**Commission**") on 30 January 2018. The Complainant said she logged into her user account on the Website and was shown the account subpages of another customer. She could see the other customer's name, contact number, birth date, email address and residential address.

Material Facts and Finding

3 This case concerns section 24[1] of the Personal Data Protection Act 2012 (the "**PDPA**"). The issue was whether the Organisation had made reasonable security arrangements to protect the personal data of its customers that was in its possession or under its control. The Organisation was in possession and control of the personal data in the user account subpages of its customers. Customers, such as the Complainant, could access their user accounts on the Website.

4 As bot traffic took up much of the Website's bandwidth, the Organisation introduced a bot manager service on 30 January 2018. The bot manager would identify whether a request for subpages of the Website was made by a bot. It would then serve identified bots with cached subpages having the same URL as the actual subpages requested, therefore saving bandwidth. If there were no cached subpages with the same URL, the bot manager served the requested subpages. However, it would cache the subpages visited to be served to subsequent bot requests. The cache was refreshed every 24 hours.

5 The bot manager had a setting that would have prevented user account subpages containing personal data from being cached if it had been applied (the "**Setting**"). The Organisation, however, did not consider the possibility that the bot manager might misidentify an actual user as a bot. They believed that if users had logged in to the website with their username and passwords, the bot

[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.

manager would not consider them as a bot, and therefore not cache their account subpages. As such, the Organisation did not apply the Setting.

6 In the present complaint, the bot manager misidentified a user who logged in with his password as a bot. It cached her account subpages, which contained her personal data. They were then served to the Complainant, who was also misidentified as a bot. The Organisation should not have taken the risk of allowing web subpages with personal data to be cached for display. It should have applied the Setting from the start, when introducing the bot manager, to protect its customers' personal data. Following the incident, the Organisation had, on 1 February 2018, applied the Setting to disable the caching of subpages containing personal data.

Conclusion

7 I find on the facts above that the Organisation did not make reasonable security arrangements to protect the personal data of its customers. The Organisation is therefore in breach of section 24 of the PDPA. I took into account the number of affected individuals (estimated by the Organisation at 23), the type of personal data at risk of unauthorised access and the remedial action by the Organisation to prevent recurrence. 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
FOR PERSONAL DATA PROTECTION