PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 22

Case No DP-1708-B1027

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

And

Spize Concepts Pte Ltd

…Organisation

DECISION

Spize Concepts Pte Ltd

[2019] SGPDPC 22

Tan Kiat How, Commissioner – Case No DP-1708-B1027

4 July 2019

Background

1. This complaint concerns an incident involving the personal data of customers of Spize Concepts Pte Ltd ("**Spize**"). Spize operates a chain of food & beverage outlets in Singapore. Part of its offering involves allowing customers to place orders through its online portal, https://orders.spize.sg ("**Site**"). The orders placed online will then be delivered to the customer at the stipulated address.

Material facts

2. On 12 August 2017, the Personal Data Protection Commission ("**PDPC**") received a complaint from a member of the public regarding the Site. A link on the Site named "Call Center" ("**Link**") had allowed members of the public to view 3 tabs: "Customer Ordering", "Restaurants" and "Order Dashboard". Under the "Order Dashboard" tab, approximately 148 customers' personal data – specifically their names, contact numbers, email addresses and residential addresses ("**personal data sets**") – were disclosed ("**Incident**"). The Incident was caused by a user logging onto the Managing Director's administrator account to enable the Link to be publicly accessible on or around 9 February 2017. The Link was intended only for internal use and not accessible to the public.

3. Spize engaged Novadine, Inc. ("**Novadine**") to develop and host their Site and online ordering system in or around 2012. Personal data sets collected through the online ordering system were stored in databases within Novadine's servers. Upon receiving news of the Incident on 14 August 2017, Spize requested Novadine to rectify the weakness in the Site. Novadine subsequently disabled the Link. The Link has not been publicly accessible since 16 August 2017.

Findings and Basis for Determination

Issues for determination

4. The issues to be determined by the Commission are as follows:

a. Whether Spize had breached section 24 of the Personal Data Protection Act 2012 ("**PDPA**");

b. Whether Spize had breached section 11(3) of the PDPA by failing to designate an individual ("**DPO**") to be responsible for Spize's compliance with the PDPA, and section 12(a) of the PDPA by failing to develop and implement policies and practices necessary to meet its obligations under the PDPA;

c. Whether Novadine was a data intermediary of Spize;

d. Whether Spize had breached section 12(d)(i) of the PDPA by failing to be in a position to make information available on request about its policies and practices which addressed the processing of personal data by Novadine on behalf of Spize; and

e. Whether Spize had transferred personal data outside of Singapore in breach of section 26 of the PDPA.

Whether Spize had breached its obligation to protect personal data under section 24 of the PDPA

5. Section 24 of the PDPA provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or similar risks (the "**Protection Obligation**").

6. Spize had outsourced the hosting, support and maintenance of its online ordering system to Novadine. However, that did not detract from its obligation under section 24 of the PDPA. In *Re The Management Corporation Strata Title Plan No. 3696* [2017] SGPDPC 11, the PDPC had found that an organisation has the primary role and duty to protect personal data, even if the organisation had engaged another organisation (a data intermediary) to carry out the processing of personal data on its behalf.

7. Investigations revealed that Spize had failed to put in place or ensure the adoption of reasonable security arrangements to prevent data breaches such as the Incident from occurring.

8. First, Spize lacked knowledge of the Novadine system – in particular, knowledge that enabling the Link could disclose its customers' personal data to the public. Based on Spize's responses to the PDPC's queries during investigations, it was apparent that Spize and its Managing Director, whose account was used to enable the Link, did not know about the existence of the Link or the consequences of enabling it.

9. Second, Spize lacked knowledge of the security arrangements that were in place within the Novadine system to protect personal data under its control that was being processed on its behalf. Spize had to rely on the answers provided by Novadine in describing how the Site and online ordering system worked. It was also unable to describe its arrangements with Novadine to process, protect and manage the personal data.

10. Spize's lack of knowledge about how personal data was processed on its behalf by Novadine was caused and/or compounded by the lack of records in its possession. The staff previously responsible for documenting Spize's arrangement with Novadine had since left Spize. Spize also did not have any staff responsible to manage the relationship between Spize and Novadine.

11. The sum effect of the above is that Spize lacked knowledge of how the personal data that was being processed on its behalf by the Novadine system was protected.

12. Third, Spize's administrator accounts for the Novadine system, in particular the Managing Director's administrator account, lacked the necessary authentication and authorisation measures.

13. Spize mentioned that there was no password policy in place at the time of the Incident. Spize also acknowledged it did not set a mandatory password requirement when Novadine first created the accounts. The Managing Director's password was rudimentary and made up of 8 digits. According to the PDPC's Guide to Securing Personal Data in Electronic Medium (revised on 20 January 2017), there ought to be at least 1 alphabetical character and 1 numeric character for such passwords. Although the PDPC Guide serves only to provide guidance, it is an indicator of how far short the password complexity and security was in this case.

14. Spize also did not mandate that its Managing Director's administrator account password be changed regularly. Nor did Spize monitor and/or ensure there was proper access to the Managing Director's administrator account. Indeed, Spize acknowledged that the account password was shared among several people at the material time, but could not provide details on the identity of these people and their respective designations.

15. The need for proper password management policies and regular change of passwords was made clear in the earlier decision of *Re Orchard Turn Developments Pte. Ltd.* [2017] SGPDPC 12. In that case, the PDPC had highlighted that an organisation's password management policies and practices, which includes the regular change of passwords, formed an integral part of the security arrangements to protect personal data. Having failed to implement such proper password policies and practices, the PDPC had found the organisation in breach of section 24 of the PDPA.

16. Additionally, the improper handling and use of administrator accounts resulted in Spize not having control and to monitor which employees had access to the Managing Director's account. Consequently, when an unidentified party enabled the Link on 9 February 2017, Spize was unable to identify the employee responsible for doing so and discover the full facts surrounding the Incident.

17. In light of the foregoing, Spize was found to have failed to make reasonable security arrangements to protect its customers' personal data under its control or in its possession. Accordingly, the Commissioner is satisfied that Spize was in breach of section 24 of the PDPA.

Whether Spize had breached the Openness Obligation sections 11(3) and 12(a) of the PDPA

18. The PDPC's investigations revealed that Spize did not have any data protection policies, internal guidelines nor any accompanying terms and conditions in place at the material time. Spize also only appointed its Data Protection Officer on 21 August 2017, one week after the PDPC notified Spize of the weakness in its Site. In light of these shortcomings, the Commissioner is satisfied that Spize had breached its Openness Obligation under sections 11(3) and 12(a) of the PDPA.

Whether Novadine was a data intermediary of Spize and whether Spize breached section 12(d)(i) of the PDPA

19. An organisation has the same obligations as its data intermediary in respect of personal data processed on its behalf: see section 4(3) of the PDPA. In this regard, an organisation that engages a data intermediary to process personal data on its behalf would need to ensure that there are appropriate policies and practices in place (under section 12 of the PDPA) governing the data intermediary's processing of data. The question then is whether Novadine was a data intermediary of Spize and, if so, whether Spize has complied with section 12 of the PDPA in respect of personal data processed on its behalf.

20. Novadine has been in the business of providing software solutions for online food retail businesses since 2007. It is based in the USA and offers its enterprise-class Point-Of-Sale integrated online ordering software to multi-unit restaurant chains. When orders are placed on the Site, Novadine processes such orders and hosts them on its servers. Novadine is therefore the provider of software-as-a-service, instead of an off-the-shelf software vendor.

21. Spize had been using the ordering system provided by and run by Novadine since 2012 to process online orders from its Singapore customers. During this process, Novadine collected and processed the personal data of Spize's customers in Singapore. Novadine collected the customers' personal data through an

application designed, operated and maintained by Novadine through Spize's website. Spize's website and online ordering system were stored in Novadine's servers. Although Spize, when asked, could not produce any agreements or contracts with Novadine, on the totality of the documents produced by Spize, the Commissioner was satisfied that Novadine had processed personal data of Spize's customers.

22. Based on the above, the Commissioner is satisfied of the following. First, Novadine had processed personal data of Spize's customers in line with the arrangement stated above. Novadine was therefore Spize's data intermediary at the time of the Incident. Section 4(2) of the PDPA imposes on organisations that engage data intermediaries to do so "pursuant to a contract which is evidenced or made in writing". Spize was unable to provide documentary record to show that it had in place a contract with Novadine. The PDPC had made various requests for production of such documentation, but Spize was unable to produce information on its contract and/or arrangement with Novadine.

23. Second, Spize ought to have ensured that the policies and practices developed under section 12(a) of the PDPA addressed Novadine's processing of personal data on its behalf. Given that Novadine was Spize's data intermediary, Spize should also have had policies in place that addressed how Novadine processed personal data on Spize's behalf. As discussed in the preceding paragraph, one specific category of policies and practices is contractual documentation relating to the scope of the data intermediary relationship. Another is the category of policies and practices relating to the transfer of its clients' personal data outside Singapore that will be discussed in the next section.

24. Third, it follows that Spize was also in breach of its obligation under section 12(d)(i) of the PDPA to make information available on request about the policies and practices it had implemented, which addressed how Novadine was to process

personal data on its behalf. Accordingly, Spize was in breach of section 12(d)(i) of the PDPA.

Whether Spize had transferred personal data outside Singapore in breach of section 26 of the PDPA

25. Spize knew that Novadine was a software-as-a-service provider that was based in the United States of America. It does not have any operations or other presence in Singapore. In choosing to use a data intermediary that is based outside Singapore, Spize had to ensure that Novadine was bound by legally enforceable obligations to protect personal data that it received to a standard comparable to that under the PDPA: Reg 9(1)(b) of the Personal Data Protection Regulations 2014 (PDPR). Pertinent to this case, Spize could have done so either by assessing that Novadine was subject to domestic laws in the US that provided comparative protection: Reg 10(1)(a) of the PDPR; or through a contract: Reg 10(1)(b) read with 10(2) of the PDPR. Alternatively, if Spize determined that the transfer came within one of the deeming provisions under Reg 9(3) of the PDPR, then the assessment of comparable protection under US law or imposition of comparable protection through contract will not be necessary. The most pertinent exception in this case is Reg 9(3)(b) of the PDPR, as the personal data of Spize customers were transferred to Novadine for the processing of their online food orders. As such, it could possibly be a transfer that is "necessary for the performance of a contract between the individual and the transferring organisation": Reg 9(3)(b) of the PDPR.

26. In the ordinary case, organisations are expected to make an assessment of the risks of trans border transfer of personal data in their possession or under their control and come to a conclusion as to how identified risks (if any) can be addressed. In this case, it is arguable whether the use of a US-based provider for online ordering system was a question of necessity or a question of commercial choice. This makes a difference whether Spize can benefit from the deeming provision in Reg 9(3)(b) of the PDPR, or whether it ought to have complied with

Reg 10 of the PDPR to ensure comparable protection by contract or through an assessment of US law.

27. The Organisation's omission to consider its obligations under section 26 of the PDPA when transferring personal data outside Singapore constitutes a breach of the transfer limitation obligation under section 26. Assessments that US law provided comparative protection or that the transfer came within one of the deeming provisions under Reg 9(3) of the PDPR, eg contractual necessity under Reg 9(3)(b), should ordinarily be documented as part of the policies and practices that Spize ought to have developed and maintained. Alternatively, if transfer was on the basis of contract, clauses sufficient to meet the requirements of Reg 10(1)(b) read with 10(2) of the PDPR should have been embodied in the contract between Spize and Novadine. The lack of policies and practices (including the lack of contractual documentations) evidencing the scope of Spize's engagement of Novadine is already the basis of a finding of breach of section 12(d)(i) of the PDPA.

Directions

28. The Commissioner is empowered under section 29 of the PDPA to give the Organisations such directions as it deems fit to ensure the Organisations' compliance with the PDPA.

29. Having carefully considered all the relevant factors noted above, pursuant to section 29(2) of the PDPA, and the investigation and assessment of this matter having been completed, the Commissioner is satisfied that:

a. Spize did not make reasonable security arrangements and is in breach of section 24 of the PDPA;

b. Spize breached its Openness Obligation under sections 11(3) and 12(a) of the PDPA;

c. Spize breached its obligation under section 12(d)(i) of the PDPA to make information available on request about the policies and practices it had implemented that would address how Novadine would process personal data on its behalf; and

d. Spize breached its obligation under section 26 of the PDPA.

30. Having carefully considered all the relevant factors of this case, the Commissioner hereby directs that Spize pays a financial penalty of S$20,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

31. In assessing the breach as determining the directions to be imposed on Spize in this case, the Commissioner took into account the fact that the Incident involved actual disclosure of customers' personal data through the Link via Spize's website.

32. That said, the Commissioner also took into account the following mitigating factors.

33. First, the Commissioner accepted Spize's representations that following the Incident, the organisation had taken steps to:

a. Implement a customised data protection framework;

b. With help from external consultants, draft the necessary processes and policies and conduct data protection training for its employees;

c. Engage a new IT vendor to change the Site (to be hosted locally) and online ordering system; and

d. Put in place proper access controls within the system.

34. The Commissioner is satisfied that the above actions taken are reasonable and address the breaches that occurred in the present instance. They should also prevent recurrences of the Incident.

35. Second, Spize took prompt action to inform Novadine to remove the Link from the public domain.

36. Finally, Spize was largely cooperative during the investigations, notwithstanding its inability to explain the technical cause of the breach.

37. Spize, after receiving the preliminary Decision, made the following representations in support of its request for a reduction in the quantum of the financial penalty imposed:

a. Spize reiterated the steps it had taken to comply with the PDPA after the Incident, namely,
   i. planning for an annual review of its data protection policy;
   ii. planning for re-training its current employees on the PDPA, in particular its IT team;
   iii. planning to send its employees for talks and seminars on PDPA updates;
   iv. initiating access-code restrictions as well as setting up separate accounts for employees; and
   v. terminating its engagement with Novadine and setting up a new website hosted by a company in Singapore;

b. The incident was unintentional and was a result of human error; and

c. The financial penalty is "a hefty price to pay" given a separate incident that Spize suffered last November (which was not related to personal data protection).

38. The Commissioner declines Spize's request for a reduction in the quantum of the financial penalty for the following reasons:

a. The Commissioner had already taken into account the steps taken by Spize in reaching his decision on the quantum of the financial penalty (see paragraph 33 above);

b. The unintentional nature of the data breach is not relevant as a mitigating factor given that the investigations revealed that the breaches related to a failure to put in place the necessary processes and practices and did not relate to the specific action by the employee; and

c. An organisation which has difficulty in paying a financial penalty imposed may request that the financial penalty be paid in instalments. The fact that Spize suffered a separate incident is, however, not a relevant consideration in determining the quantum of the financial penalty imposed, although its impact on Spize's cashflow may be a relevant factor to consider in a request for instalment payment of the financial penalty.

39. Further, the Commissioner hereby directs Spize to carry out the following within 60 days:

a. Put in place a data protection policy and internal guidelines to comply with the provisions of the PDPA and, in particular, to prevent future recurrences of the breaches that had occurred in this case;

b. Train all employees of Spize handling personal data on the obligations under the PDPA and the organisation's data protection policies after direction (a) has been completed;

c. Put in place proper access controls for the management of administrators' accounts within its food order delivery and catering services website and online ordering system; and

d. Put in place measures to ensure that it is able to make information available about its policies and practices (including information set out in contracts/agreements entered into with its data intermediaries that contractually require the relevant data intermediary to implement specific reasonable arrangements) necessary to meet its obligations under the PDPA.

40. The Commissioner also directs that Spize informs the PDPC of the completion of each of the above within 1 week of implementation.

41. The Commissioner urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. Appropriate enforcement action against non-compliant organisations will be taken.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION