This decision is subject to final editorial corrections approved by the tribunal and/or redaction pursuant to the publisher's duty in compliance with the law, for publication in LawNet.

Avant Logistic Service Pte. Ltd.

[2019] SGPDPC 28

Yeong Zee Kin, Deputy Commissioner — Case No DP-1802-B1709

Data protection – Protection obligation – Unauthorised disclosure of personal data – Insufficient security arrangements

30 July 2019.

Background

1 On 25 November 2017, a customer of Ezbuy Holdings Ltd. ("**Ezbuy**") made a complaint to the Personal Data Protection Commission (the "**Commission**") alleging that her personal data had been disclosed to another customer of Ezbuy without her consent by an employee of Avant Logistic Service Pte. Ltd. (the "**Organisation**"). The facts of this case are as follows.

2 Ezbuy provides an online e-commerce platform that allows its customers to shop for items from various online retailers and platforms around the world. It engaged the Organisation to provide delivery services in Singapore. The Organisation is an affiliate of Ezbuy and its delivery personnel are required to adhere to Ezbuy's Privacy Policy and the terms and conditions in Ezbuy's

Employee Handbook and Ezbuy's Delivery and Collection Standard Operation Procedure ("**SOP**").

3 When a customer ordered an item through Ezbuy's platform, they would be offered two modes of delivery, (i) delivery to a designated collection point (referred to by Ezbuy as "self-collection"), or (ii) delivery to the customer's address. If the customer opted for self-collection, the customer would proceed to the designated collection point at a specified time. The delivery personnel there would verify their identity using their Ezbuy user ID or their mobile number registered with Ezbuy and then hand over the package with their item.

4 On 9 November 2017, the complainant scheduled to self-collect a package that she ordered from Ezbuy at a collection point in Bishan at around 6.30 p.m. One of the Organisation's employees (referred to in this Decision as "**OA**"), was assigned to distribute packages there that evening. When the complainant met OA at the collection point, he gave the complainant two packages (the "**Packages**") after verifying her identity. The complainant noticed that the Packages were not hers because they bore the user ID and mobile number of another person (referred to in this Decision as "**CA**"). According to the complainant, she informed OA of this but was told to take the Packages as they were tagged to her mobile number in the Ezbuy system. The complainant also alleged that OA asked her to inform Ezbuy's customer service that the

wrong packages had been sent to her. The complainant then left the collection point with the Packages.

5 CA arrived to collect the Packages shortly after the complainant left. OA informed her that someone else had already collected the Packages and told her that he would try to locate them and arrange for their subsequent delivery. At this time, OA did not realise that it was the complainant who had collected the Packages.

6 Later that night, OA sent CA screenshots of two delivery lists containing Ezbuy user IDs and mobile telephone numbers of some Ezbuy customers (the "**Disclosed Data**"). The first list that was sent contained the Ezbuy user IDs and mobile telephone numbers of eight Ezbuy customers who had been scheduled to collect their packages at Bukit Panjang. (This was apparently sent by mistake.) The second list contained the user IDs of four Ezbuy customers, including that of the complainant, who had been scheduled to collect their packages at Bishan. The telephone numbers in the second list were redacted by OA. However, OA also sent the complainant's mobile telephone number to CA. OA explained to CA that he suspected that the complainant had collected the Packages because his records showed that the complainant had not collected her own packages.

7 CA eventually managed to find the complainant's Facebook and Instagram pages using the complainant's Ezbuy user ID as the complainant had used the same name (which was not her real name) for her Facebook, Instagram and Ezbuy user IDs. CA then sent a series of messages to the complainant via Facebook Messenger in order to recover the Packages. The complainant subsequently returned the Packages to Ezbuy.

Remedial actions by Ezbuy and the Organisation

8 After being informed of the incident by the Commission, Ezbuy and the Organisation jointly undertook the following measures to prevent the unauthorised disclosure of customers' personal data in the future:

(a) All delivery personnel are required to request for <u>both</u> a customer's user ID and mobile telephone number for verification during the self-collection process;

(b) Ezbuy's Delivery and Collection SOP was updated to comply with the provisions of the PDPA and to highlight the importance of the PDPA. In particular, a clause was added by Ezbuy stating that no customer information can be disclosed to any party under all circumstances, and that any unauthorised disclosure will lead to disciplinary action as listed in Ezbuy's Employee Handbook;

(c) A briefing was conducted to all delivery personnel to reinforce the instruction and policy that no customer's personal data should be provided to any third party under all circumstances, and this briefing is repeated to all delivery personnel every morning; and

(d) Ezbuy revised its Employee Handbook to include detailed enforcement and disciplinary actions to be taken for breach of confidentiality and employee misconduct, including any leak or sale of customer data.

Findings and Basis for Determination

Was the Disclosed Data personal data?

9 As a preliminary issue, I find that most of the Disclosed Data was personal data within the meaning of the PDPA. The term "personal data" is defined in section 2(1) of the PDPA as follows:

> "personal data" means data, whether true or not, about an individual who can be identified –
>
> (a) from that data ["**Direct Identification**"]; or
>
> (b) from that data and other information to which the organisation has or is likely to have access ["**Indirect Identification**"]."

10 The mobile telephone numbers disclosed by OA constitute personal data since they enable Direct Identification of the respective individuals. As explained in the Commission's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* [at 5.9 to 5.10], an individual's personal mobile telephone number is a 'unique identifier' and capable, on its own, of identifying the individual.

11 On the other hand, since Ezbuy user IDs do not enable Direct Identification, whether they qualify as "personal data" depends on whether they enable Indirect Identification. In this case, CA was able to find the complainant's Facebook and Instagram pages and identify her using the complainant's Ezbuy user ID. The complainant's Ezbuy user ID therefore constitutes personal data under the PDPA, even though the user ID did not contain complainant's real name, as it enabled Indirect Identification of the complainant.

12 Although organisations cannot be expected to know in advance if the user IDs of their customers enable Indirect Identification, they should not assume that user IDs *per se* do not constitute personal data as such an assumption may not, in fact, be true (as seen from this case). Organisations should therefore exercise prudence in handling user IDs. As there is no evidence that the other Ezbuy user IDs in the Disclosed Data allowed for Indirect

Identification, I grant the Organisation the benefit of the doubt and accept that they do not constitute personal data. Nevertheless, it remains that the personal data of nine individuals (corresponding to the nine mobile telephone numbers disclosed) was disclosed without their consent or the authorisation of the Organisation.

Whether the Organisation had made reasonable security arrangements

13 Section 24 of the PDPA requires organisations to protection personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised use, disclosure and similar risks. Although the Organisation's delivery personnel were required to comply with Ezbuy's Privacy Policy and Employee Handbook, this was, at the time of the incident, inadequate as they did not inform employees of exactly what they were required to do in order to protect customers' personal data:

(a) Ezbuy's Privacy Policy only stated its commitment to ensuring security of customer information and that "suitable physical, electronic and managerial procedures" had been put in place to safeguard customer information; and

(b) Ezbuy's Employee Handbook only included a provision highlighting that customer information (among others) was confidential.

14 At the time of the incident, the Organisation had not made any effort to impress upon its delivery personnel the need to protect personal data in their possession. The Organisation did not have measures in place, such as policies or standard operating procedures, to prohibit the unauthorised use or disclosure of personal data by its delivery personnel. The Organisation also had not provided any instruction or training to its delivery personnel on the proper handling of personal data and on compliance with the PDPA.

15 In the course of the Commission's investigation, the Organisation sought to rely on a clause in OA's employment contract which prohibited him from disclosing confidential information, including customer information, without the Organisation's prior consent (the "**Confidentiality Clause**"). While such clauses are relevant to an organisation's security arrangements to protect personal data, they are insufficient on their own because they typically do not elaborate on what constitutes personal data, nor how employees should handle and protect it. Organisations are expected to provide their staff with *specific, practical instruction* on how to handle personal data and comply with the PDPA (*Re Hazel Florist & Gifts Pte Ltd* [2017] SGPDPC 9 at [18]). This is particularly important for the Organisation's delivery personnel who frequently handle personal data and are on the frontline of the Organisation's customer-facing operations where the potential for improper use and disclosure of personal data cannot be ignored.

16 In the circumstances, I find that the Organisation had not made reasonable security arrangements to protect the personal data comprised in the Disclosed Data. The Organisation is accordingly in breach of section 24 of the PDPA.

17 One additional point I wish to address is that when OA was asked about the incident, he claimed that he had given the complainant the Packages as the complainant had provided him with CA's Ezbuy user ID and mobile telephone number for verification. As there is no evidence that the complainant and CA were known to each other, I do not find OA's recollection of the events to be credible or acceptable. In any case, this does not detract from the above conclusion that the Organisation had failed to make reasonable security arrangements as required under section 24 of the PDPA.

Outcome

18 Taking the totality of the circumstances into account, I have decided not to impose a financial penalty in this case. In particular, I note that:

(a) The breach was a one-off incident, with few affected individuals and relatively little personal data disclosed (comprising the nine mobile telephone numbers and user IDs);

(b) The Organisation took prompt remedial actions to prevent a recurrence of such an incident; and

(c) The Organisation was cooperative during investigations.

19 Instead, I have decided to issue the following directions to the Organisation to ensure its compliance with the PDPA:

(a) To put in place the appropriate written policies and process safeguards which are necessary for it to protect personal data in its possession or under its control within 30 days from date of this direction;

(b) To arrange for personal data protection training for its staff within 60 days from date of this direction; and

(c) To inform the Commission in writing of the completion of each of the above within 1 week of completion.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION