PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 37

Case No DP-1803-B1866

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

And

Zero1 Pte. Ltd.
XDEL Singapore Pte. Ltd.

… *Organisations*

DECISION

Zero1 Pte. Ltd.

XDEL Singapore Pte Ltd

[2019] SGPDPC 37

Tan Kiat How, Commissioner — Case No DP-1803-B1866

16 September 2019.

Background

1 Zero1 Pte. Ltd. ("**Zero1**") is a Mobile Virtual Network Operator founded in 2017. In order to deliver its SIM cards to its customers, Zero1 contracted XDEL Singapore Pte Ltd ("**XDEL**") for courier services. In the course of delivering the SIM cards, XDEL inadvertently disclosed the personal data of Zero1's customers. Central to this case is the question of whether XDEL and Zero1 (collectively referred to as the "**Organisations**") had made reasonable security arrangements to protect the personal data of Zero1's customers pursuant to their obligations under the Personal Data Protection Act 2012 ("**PDPA**").

Material Facts

2 In March 2018, XDEL was appointed by Zero1 to deliver SIM cards to the latter's subscribers. Zero1's subscribers would register for mobile services using Zero1's website. After their application had been processed, Zero1 would provide to XDEL the subscriber's information (including the subscriber's name, NRIC number, delivery address and contact number), the SIM card number and the subscriber's preferred time of delivery. In the event that the customer had authorised another person to receive the SIM card on his or her behalf (an

"**authorised recipient**"), the authorised recipient's information (name, NRIC number, contact number and delivery address) would additionally be provided to XDEL.

3 Each Zero1 subscriber was provided with a unique URL link which would allow them to access a customised delivery notification webpage through which they could monitor the status of their SIM card delivery (the "**notification webpage**"). It was through the notification webpages that the information of the subscribers and authorised recipients (the "**Personal Data**") were accessed.

4 The first batch of SIM card deliveries took place between 8 and 9 March 2018. 333 URLs linking to notification webpages containing the Personal Data of 292 individuals were sent out in support of this first batch of deliveries. Investigations revealed that there was unauthorised access ("Unauthorised Access") to 175 of the URLs which contained Personal Data. These URLs were accessed by 82 unique IP addresses over a span of about 34 hours, between 12 and 13 March 2018.

5 The Unauthorised Access was discovered after a post on an online forum thread warned other users not to reveal their Zero1 account numbers in public, indicating that it was possible to access another individual's delivery notification if one was able to determine another subscriber's membership number. The membership number of another subscriber was not difficult to determine as the membership numbers were generated in sequential order.

6 Further investigations uncovered the following causes leading to the unauthorised access of the Personal Data:

(a) Each notification webpage URL comprised of what XDEL called an "A code" and a "B code". A sample notification webpage URL took the following form: "https://www.xdel.com/ib/?A=00000000&B=4CC5". In this example, the A-code is 00000000 and the B-code is 4CC5.

(b) The A code is a Zero1 subscriber's membership number and also the consignment note value, which, as noted above, is a sequentially generated number.

(c) The B code is the last 4 characters of a calculated code, generated using a SHA1 hash on the consignment note number, with a secret salt. The B code served as a confirmation code. It was meant to secure the URLs against unauthorised access. The webpage was supposed to return the delivery status only when the correct B code of 4-character length was presented. The calculated B code of 4 characters meant that it was unlikely that an individual would be able to guess the correct code based on the A code, as there would have been 65,536 possible combinations.

(d) According to XDEL, the notification webpage system was developed in-house. In the course of investigations, XDEL admitted that its developer had failed to test for the scenario where a blank B code was presented.

(e) If B codes containing less than 4 characters were presented, the system would only check that the partial code presented matched the ending characters of the correct code. As such, if someone guessed the A code of a subscriber (which as mentioned above was easy enough to do given that the A code is a sequentially generated subscriber number) and left the B code blank, the system would identify this as a correct

code, and unauthorised access would be granted to the subscriber's personal data. By altering the A code values, this allowed individuals to see another person's delivery orders and their personal data.

Accordingly, the Unauthorised Access would likely have been prevented if the system was programmed to check the complete B Code instead of a partial code.

The Commissioner's Findings and Basis for Determination

The Relevant PDPA Provisions

7 In respect of this matter, the relevant provision is Section 24 of the PDPA. Section 24 requires an organisation to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").

Preliminary Issues

8 It is not disputed that the Personal Data is "personal data" as defined in section 2(1) of the PDPA. There is no question or dispute that the Organisations fall within PDPA's definition of an "organisation".

9 It is also not disputed that the Protection Obligation applies to both Zero1 and XDEL:

(a) The personal data of the Zero1 customers and the authorised recipients originated from Zero1 and was under Zero1's possession and/or control. For this reason, Zero1 had the obligation under section

24 of the PDPA to protect the personal data of its customers and that of the authorised recipients.

(b) XDEL was the data intermediary for Zero1. XDEL had entered into the "Service Agreement for the Provision of Domestic Courier Services" on 1 March 2018 (the "**service agreement**"). Pursuant to the agreement, XDEL was to provide for the storage of SIM cards, packing materials, and delivery service. Clause 11 of the Agreement stated that XDEL would "process the Personal Data" strictly for the purposes of providing the stated services to Zero1. This would necessarily encompass the processing of the personal data of Zero1's subscribers for the purposes of delivery. By virtue of section 4(2) of the PDPA, XDEL had the same obligation under section 24 of the PDPA to protect the personal data Zero1's subscribers and that of the authorised recipients.

10 The key issue is therefore whether the Organisations had protected the Personal Data in its possession and under its control by making reasonable security arrangements to prevent unauthorised access and similar risks.

Both Organisations failed to make reasonable security arrangements

11 After a review of all the evidence obtained by PDPC during its investigation and for the reasons set out below, the Commissioner is of the view that both Organisations had failed to make reasonable security arrangements to protect the personal data in its possession and control, and both have thereby breached the Protection Obligation under section 24 of the PDPA.

A. <u>Breach of the Protection Obligation by Zero1</u>

12 Zero1 was aware of the use of the notification webpage and had defined the type of information contained on the webpage. Presumably, Zero1 had assessed the necessity and risks of the personal data displayed on the notification webpage. Zero1 ought also to have satisfied itself that XDEL had put in place the reasonable security arrangements indicated in the service agreement, before allowing the webpage to be put into use. Zero1 failed to demonstrate it had done the above. It had relied entirely on the warranty with regard to data protection in the service agreement, as well as customer references provided by XDEL.

13 Reasonable security arrangements in this case would entail minimally making an effort to identify the possible risks and seeking assurance that the data intermediary had taken steps to protect against those risks. Unfortunately, Zero1 failed to do either. In fact, Zero1 were not even aware of the security arrangements undertaken by XDEL; neither did it make any effort to identify potential risks associated with the notification webpage. Zero1 has cited a lack of ability and expertise to audit XDEL's notification webpage source code as a reason for not doing so. This cannot be a valid defence as what is required is not technical oversight but an identification of foreseeable risks, and then requiring XDEL to take reasonable measures to address them. The extent of Zero1's due diligence in the circumstances did not require technical knowledge, but risk identification and assessment. For instance, Zero1 could have identified the risk as whether a stranger coming across the website would be able to makes changes to it and retrieve a subscriber's information; similarly, whether all information displayed on the notification page was necessary for the subscriber to monitor his SIM card delivery. Having articulated the risks, Zero1 ought to have worked with XDEL on assessing the likelihood of their occurrence, impact on subscribers should the risk occur and what steps XDEL could propose that would be reasonably effective in preventing the occurrence of the identified

risks and, should they nevertheless occur, minimise the impact of the risks. This process does not require technical expertise on the part of Zero1; and allows it to rely on XDEL to provide the technical expertise during the risk assessment and mitigation discussion.

14 It is therefore assessed that Zero1 did not meet the standard of having reasonable security arrangements in place.

B. Representations submitted by Zero1

15 Zero1 submitted its representations to the PDPC after a preliminary decision was issued:

(a) Zero1 had taken measures to identify and mitigate potential risks. As Zero1 did not have technical capabilities in coding, cyber security or data encryption, it relied on XDEL's declarations and assurances of its capabilities and track record. Zero1 also visited XDEL's operation centre to audit its processes and was satisfied that there were no foreseeable risk; and

(b) It is unreasonable to expect Zero1 to pinpoint the possible avenues by which personal data could be compromised. The Incident could not have been pre-empted by Zero1 without the relevant experience and technical knowledge.

16 Zero1 had previously highlighted that they lack technical expertise and this has already been dealt with at paragraph 13 above. It should be pointed out that while Zero1 may have audited the operation centre, this does not detract from the matters raised in paragraph 12 above.

17 In relation to the 2nd point raised in paragraph 15(b), what was required is for Zero1 to have engaged XDEL on the security arrangements that it had put in place to protect the personal data on the notification webpage, including generating URLs using the membership number and the B Code. This did not require technical expertise on the part of Zero1. It is in the failure to do so that the present breach is found.

18 In the circumstances, the Commissioner maintained his finding that Zero1 is in breach of section 24 of the PDPA.

C. Breach of the Protection Obligation by XDEL

19 XDEL created the notification webpage system knowing that it would be used to contain the personal data of Zero1 subscribers and their designated authorised recipients.

20 XDEL ought to have taken reasonable security arrangements to protect the personal data from unauthorised access. The reasonable arrangements in this case include adequate testing to verify that the measures were correctly implemented. In this regard, XDEL had implemented the B code to prevent unauthorised access of the notification webpage. The B code would have prevented unauthorised access had it worked as intended.

21 However, while XDEL tested the notification webpages to make sure they could not be accessed by an incorrect B code, they failed to test for scenarios where the B code was absent or when an incomplete B code was used. Since the B code was, by design, a 4-character field, it would seem obvious that the module should have been designed to cater for the situation where the B code did not meet this condition and thereafter to test for this scenario. Given that the B code was crucial to the verification of the user and granting the user

access to the user's personal data, tests should have been conducted to ascertain the behaviour of the webpage in the absence of the B code. Their failure to do such tests rendered their efforts to reasonably secure the Personal Data hosted on the notification webpage insufficient.

22 Accordingly, it is assessed that XDEL, like Zero1, did not meet the standard of having reasonable security arrangements in place. XDEL's failure to meet this standard is more serious than that of Zero1, given that XDEL was the party that was responsible for the webpage notification system that failed.

D. Representations by XDEL

23 XDEL submitted representations to the PDPC on the quantum of the financial penalty only. It asked for a reduction of the financial penalty quantum as it had recently incurred expenses to relocate to new premises. As this is not a mitigating factor or relevant in determining the financial penalty quantum, the Commissioner has decided to maintain the initial financial penalty quantum. Given its current cash flow considerations, the Commissioner has varied his directions to XDEL, as set out below, to allow XDEL to pay the financial penalty in instalments.

The Commissioner's Directions

24 Having found the Organisations to be in breach of section 24 of the PDPA, the Commissioner is empowered under Section 29 of the PDPA to give the Organisations such directions as he deems fit to ensure compliance with the PDPA.

25 In determining the appropriate directions to be imposed on each of the Organisations, the Commissioner has taken into account the following aggravating factors:

(a) The Personal Data disclosed, which included the personal addresses of the subscribers and authorised recipients, as well as their NRIC numbers, was sensitive in nature.

(b) Approximately 292 individuals were affected by the unauthorised access.

26 The following mitigating factors have also been taken into account:

(a) Zero1 voluntarily notified the PDPC that the Personal Data of the subscribers and authorised individuals had been breached.

(b) XDEL acted swiftly to rectify the notification webpage system. By 13 March 2018, they had managed to modify the code checking function on the webpage to check for the length of the confirmation code, thereby correcting the technical vulnerability. XDEL also added an "alert trigger" that would notify its IT department if an IP address entered 3 or more consecutive wrong codes, as an additional control to prevent any further unauthorised access.

27 Having considered all the relevant factors of the case, including the relative responsibilities and culpabilities of both organisations, the Commissioner hereby makes the following directions:

(a) Zero1 is to pay a financial penalty of $4,000.00 within 30 days from the date of the Commissioner's direction, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall

accrue and be payable on the outstanding amount until the financial penalty is paid in full; and

(b) XDEL is to pay a financial penalty of $7,000.00 in 3 instalments as set out below, failing which, the full outstanding amount shall become due and payable immediately and interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full:

(i) 1st instalment of $2,500 within 30 days from the date of the Commissioner's direction;

(ii) 2nd instalment of $2,500 within 60 days from the date of the Commissioner's direction; and

(iii) 3rd instalment of $2,000 within 90 days from the date of the Commissioner's direction,

28 Given the remediation efforts undertaken by the Organisations, no further directions relating to the breach itself are issued.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION