Ninja Logistics Pte Ltd

[2019] SGPDPC 39

Tan Kiat How, Commissioner — Case No DP-1804-B2020

Data Protection – Protection obligation – Unauthorised access to personal data – Insufficient security arrangements

14 October 2019

Introduction

1 Ninja Logistics Pte Ltd (the "**Organisation**") is a logistics company providing packaging, delivery and tracking services on behalf of retailers ("**Retailers**") to the Retailers' customers ("**Customers**"). This case concerns the disclosure of personal data via a delivery order tracking function on the Organisation's website (the "**Tracking Function Page**").

2 On 23 April 2018, the Personal Data Protection Commission (the "**Commission**") received a complaint that the Tracking Function Page could potentially be used to harvest personal data of the Customers. By changing a few digits of a Tracking ID, the complainant could access personal data of another Customer (the "**Incident**").

Facts of the Case

3 The Organisation first set up the Tracking Function Page in December 2014 to allow Customers to (i) enquire on the delivery status of their parcels; and (ii) confirm the identity of individuals who collect parcels on their behalf (where applicable). Generally, for a delivery, only a Retailer and the relevant Customers of the Retailer would be provided with a Tracking ID for parcels sent by the Retailer that were to be delivered by the Organisation to the Customer.

4 There were 2 types of Tracking IDs used by the Organisation, namely sequential and non-sequential Tracking IDs. According to the Organisation, the reason for having sequential numbers in some of the Tracking IDs was for recording and business analytics purposes. Since the launch of the Tracking Function Page, the Organisation was aware that Tracking IDs could potentially be manipulated by changing the last few digits of the Tracking ID. While Tracking IDs with non-sequential numbers may have a lower risk of manipulation, a random generation

of any 9 digits that happened to match a valid Tracking ID could still result in unauthorised access and disclosure of personal data.

5 For a period of approximately 3 months from launch of the Tracking Function Page, the Organisation unsuccessfully experimented with 2 methods as a second layer of authentication to the Tracking IDs. These methods involved using either the last 4 digits of a Customer's mobile number or the Customer's last name to verify the identity of the person using a Tracking ID. According to the Organisation, these methods were not workable due to difficulties such as the Retailers not having, or not wishing to disclose, the mobile number of their Customers or the Customers not being able to recall the name they had provided at the time of purchase. Hence, the Organisation ceased using a second layer of authentication in 2015.

6 At the material time, the Tracking IDs were thus the sole means of using the Tracking Function Page. Upon the entry of a valid Tracking ID, the following types of information (the "**Disclosed Data**") could be accessed from the Tracking Function Page, depending on the delivery status of the parcel in question (as indicated below):

(a) For parcels with a "Pending Pickup" status:

(i) only the Tracking ID;

(b) For parcels with a "On Vehicle for Delivery" status:

(i) the Tracking ID; and

(ii) the Customer's Address; and

(c) For parcels with a "Completed" status:

(i) the Tracking ID;

(ii) the Customer's address; and

(iii) the name and signature of the Customer or other individual who had collected the parcel on behalf of the Customer (this was upon clicking on "Retrieve Proof of Delivery" hyperlink).

7 Save for the one-time archival of 2.6 million Tracking IDs on 31 August 2016, the Organisation did not have any procedures to remove records of completed deliveries from the Tracking Function Page (i.e. those with the "Completed" status). The Organisation estimated that, at the time of the Incident, there were 1,262,861 unique individuals with valid Tracking IDs at the "Completed" status (the "**Affected Individuals**").

8 Upon being notified by the Commission of the Incident, the Organisation took the following remedial actions:

(a) Removed the Customer's address for the "Pending Pickup" and "On Vehicle for Delivery" delivery statuses;

(b) As of 23 August 2018, the Organisation implemented a system such that Tracking IDs would expire 14 days after the completion of the delivery[1];

(c) In August 2018, the Organisation engaged a Crest-certified security organisation for a one-year period to assist with establishing an overarching security framework with a data protection focus, which includes working out a data protection training program for the Organisation's employees who will all receive formal training on the Organisation's obligations with respect to the Personal Data Protection Act 2012 ("**PDPA**"); and

(d) Engaged a law firm to improve and document the Organisation's personal data protection policies.

Findings and Basis for Determination

9 As a preliminary point, the Disclosed Data for parcels with "Pending Pickup" and "On Vehicle for Delivery" delivery statuses did not include any data that could identify a Customer. However, the Disclosed Data for parcels with the "Completed" delivery status included the Customers' names, address and signature. Hence, such data constituted personal data where it related to an identified Customer. In particular, the Incident resulted in the exposure of the following personal data to unauthorised access (the "**Exposed Personal Data**"):

[1] The Organisation has since received feedback from some Retailers requesting to lengthen the validity period of the Tracking IDs, and is considering lengthening the validity period from 14 days to 45 days, but this has yet to be implemented.

(a) the names and signatures of Affected Individuals who had signed for parcels when collecting them; and

(b) potentially, the addresses of Affected Individuals who were Customers.

Whether the Organisation had contravened Section 24 of the PDPA

10 Section 24 of the PDPA 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 Commissioner found that the Organisation had failed to put in place reasonable security arrangements to protect the Exposed Personal Data for the following reasons:

(a) First, and as mentioned at [4], the Organisation was aware from the outset that Tracking IDs may be manipulated and had tried unsuccessfully to introduce a second layer of authentication. Notwithstanding its knowledge of the risk of unauthorised access and disclosure of the Exposed Personal Data through manipulation of the Tracking IDs, there was a glaring failure by the Organisation to operationalise an effective method of second layer authentication. Given the foreseeable risk of using Tracking IDs as the sole means of accessing and using the Tracking Function Page, it is inexcusable for the Organisation to neglect its obligations to implement a workable security arrangement to protect the Exposed Personal Data. This resulted in the Exposed Personal Data of a significantly large number of individuals being exposed to the risk of unauthorised access and disclosure for a period of close to 2 years; and

(b) Secondly, the Organisation did not have a procedure to remove the Exposed Personal Data from the Tracking Function Page after the completion of a delivery. The Organisation could have easily done so by setting a fixed period upon completion of a delivery after which the Tracking ID would no longer be valid (as they have done after being informed of the Incident). This would have significantly reduced the risk of unauthorised access and disclosure to the Exposed Personal Data.

11 Accordingly, the Commissioner found that the Organisation had contravened section 24 of the PDPA.

Representations by the Organisation

12 In the course of settling this decision, the Organisation made representations for the Commissioner to issue a warning in lieu of a financial penalty, or in the alternative, to reduce the quantum of financial penalty imposed for the reasons set out below.

13 First, on 31 August 2016, the Organisation archived a significant number (2.3 million) of Tracking IDs. As such, only Tracking IDs issued after 31 August 2016 were accessible at the date of the Incident (i.e. the Exposed Personal Data was subject to risk of unauthorised access and disclosure for less than 2 years)[2].

14 Secondly, keeping the Exposed Personal Data accessible from the Tracking Function Page was "*well-meaning and intended to be an additional feature of its platform to differentiate itself from its competitors*", and this allowed the Retailers and their Customers to access such information as and when required without having to contact the Organisation. Furthermore, some Retailers may not receive feedback from its customers promptly and would require the Tracking IDs to be accessible for a longer period in order to respond to feedback or conduct investigations.

15 Thirdly, the Organisation raised the following factors for the Commissioner's consideration:

(a) The names in the Exposed Personal Data may not be the full names of Affected Individuals and is "*considerably less sensitive and complete than other published cases*";

(b) There was only a single finding of breach of one obligation under the PDPA (i.e. Section 24); and

(c) There was no evidence to suggest any actual unauthorised access and/or exfiltration of data leading to loss or damage.

[2] Prior to the Organisation providing information in relation to the archiving of Tracking IDs on 31 August 2016, the Commissioner preliminarily found that the Exposed Personal Data was subjected to the risk of unauthorised access and disclosure for more than 2 years.

16 Finally, the Organisation also compared the present case with *Re K Box Entertainment Group Pte Ltd* [2016] SGPDPC 1 ("***K Box***") and *Re Horizon Fast Ferry Pte Ltd* [2019] SGPDPC 27 ("***Horizon Fast Ferry***"). The Organisation represented that the circumstances of these 2 cases were far more aggravated in comparison and the financial penalties imposed was $50,000 in *K Box* and $54,000 in *Horizon Fast Ferry*. The Organisation also represented that *Re Challenger Technologies Limited and others* [2016] SGPDPC 6 ("***Challenger***") is more similar to the present case, and a financial penalty was not imposed in *Challenger*.

17 Having carefully considered the representations, the Commissioner has decided to maintain the quantum of financial penalty set out at [20(a)] for the following reasons:

(a) While the Organisation did archive 2.6 million Tracking IDs on 31 August 2016, this was a one-off exercise. The Organisation did not have any procedures to remove records of completed deliveries from the Tracking Function Page (i.e. those with the "Completed" status). Notwithstanding the archival of the 2.6 million Tracking IDs, Exposed Personal Data of 1,262,861 unique individuals with Tracking IDs had been accumulated over a period of close to 2 years. This was not reasonable considering that the delivery information which Retailers and Customers may want to access would be for a limited post-delivery period (which was likely to be in the order of weeks rather than years);

(b) As for the factors in [15] raised by the Organisation, these had already been taken into consideration in the Commissioner's determination of the quantum of financial penalty; and

(c) With respect to the Organisation's representations comparing the present case to *K Box, Horizon Fast Ferry and Challenger*, the key distinguishing factor is the volume of personal data involved. The present case involves over 1 million Affected Individuals, which far exceeds the number of affected individuals in *K Box, Horizon Fast Ferry and Challenger*.[3] These cases therefore do not support the Organisation's representations for a warning to be issued in lieu of a financial penalty or a reduction in financial penalty.

[3] As compared to 1,262,861 unique individuals in this case, the number of affected individuals was found to be approximately 317,000 in *Re K Box Entertainment Group*, 295,151 in *Re Horizon Fast Ferry* and 165,306 in *Re Challenger Technologies Limited*

The Commissioner's Directions

18 In determining the directions to be imposed on the Organisation under section 29 of the PDPA, the Commissioner took into account the following aggravating factors:

(a) The Organisation was cognisant of the risks of unauthorised access and disclosure to the Exposed Personal Data through the Tracking Function Page but failed to resolve the issue for more than 2 years;

(b) The Exposed Personal Data of a significantly large number of individuals were exposed to the risk of unauthorised access and disclosure for close to 2 years; and

(c) The Organisation failed to remove Exposed Personal Data of a significantly large number of individuals from the Tracking Function Page when it was no longer necessary to keep them accessible online.

19 The Commissioner also took into account the following mitigating factors:

(a) the Organisation was cooperative in the investigations;

(b) the Organisation had, in effect, adopted an approach consistent with data protection by design by controlling the amount of information disclosed at different stages of the delivery process, thereby decreasing the risk of unauthorised access and disclosure; and

(c) there was no evidence of exfiltration of the Exposed Personal Data.

20 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to:

(a) Pay a financial penalty of $90,000 within 30 days from the date of the directions, 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 of such financial penalty until the financial penalty is paid in full; and

(b) Within 30 days from the date of this direction, implement a reasonable validity period for the Tracking IDs after completion of each delivery, which should be as reasonably short as possible while meeting business needs.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION