PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPCS 13

Case No. DP-2108-B8798

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

And

Budgetcars Pte. Ltd.

SUMMARY OF THE DECISION

1. On 25 August 2021, the Personal Data Protection Commission (the "**Commission**") received a complaint that the delivery tracking function (the "**Tracking Function Page**") on the website of Budgetcars Pte Ltd (the "**Organisation**") could be used to gain access to the personal data belonging to another individual. By changing a few digits of a Tracking ID, the complainant could access the personal data of another individual (the "**Incident**").

2. The Organisation is a logistics company delivering parcels to customers ("Customers") on behalf of retailers ("Retailers").

3. The personal data of 44,357 individuals had been at risk of unauthorised access. The datasets comprised name, address, contact number and photographs of their signatures.

4. The Tracking Function Page was set up in December 2020 to allow Retailers and Customers to (i) keep track of the delivery status of their parcels; and (ii) confirm the identity of individuals to collect parcels on their behalf (where applicable). The Tracking IDs were generated by Retailers and comprised either sequential or non-sequential numbers. Although generated by Retailers, the Organisation adopted the Tracking IDs for use on its own Tracking Function Page that allowed their customers to track their deliveries, which would disclose personal data listed above. The Protection Obligation therefore required the Organisation to ensure that there were reasonable access controls in its use of the Tracking IDs for giving access to an individual's personal data.

5. The risk of unauthorised access to personal data from altering numerical references, both sequential and non-sequential, have featured in the published decisions of the Commission in *Re Fu Kwee Kitchen Catering Services* [2016] SGPDPC 14, and more recently, in *Re Ninja Logistics Pte. Ltd.* [2019] SGPDPC 39. Insecure direct object reference has long been a well-known security risk to personal data. The Organisation failed to have reasonable access control to the affected individuals' personal data when it simply adopted Tracking IDs generated by the Retailers without factoring in this risk.

6. The Organisation also admitted that it did not have in place a process to protect personal data through proper safeguards by archiving personal data relating to a completed delivery order after a reasonable period of time has lapsed. To reduce the risk of access to personal data through frontend applications, they should be removed and archived within a reasonable time. The Organisation's failure to do

so resulted in more personal data at risk in the Incident than should have been the case.

7. In the circumstances, the Organisation is found to be in breach of section 24 of the PDPA.

8. Upon being notified by the Commission of the Incident, the Organisation took the following remedial measures after the Incident:
   a. Removed all personal data from the Tracking Function Page;
   b. Engaged its IT solutions provider to re-examine management of the Tracking Function Page;
   c. Post-delivery expiry of Tracking ID after 14 days; and
   d. Implemented checks to prevent sequential Tracking IDs from being uploaded onto the Tracking Function Page.

9. The Commission accepted the Organisation's request for this matter to be handled under the Commission's expedited breach decision procedure. This meant that the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. The Organisation also admitted that it was in breach of section 24 of the Personal Data Protection Act (the "**PDPA**").

10. In *Re Ninja Logistics Pte. Ltd.* cited above, the organisation had been aware of the risk from manipulation of Tracking IDs. However, a counter-measure which the organisation initially introduced was abandoned due to operational issues and was not replaced. This resulted in a significantly larger dataset (>1.2 million) that was exposed to the risk of unauthorised access over a period of close to 2 years. In

comparison, the number of affected individuals in the present case was lower as the Organisation was only handling deliveries for a few Retailers at the time of the Incident.

11. Having considered the circumstances set out above and the factors listed in section 48J(6) of the PDPA, including (i) the Organisation's upfront voluntary admission of liability; and (ii) the prompt remedial action undertaken by the Organisation, the Commission considered that it would be appropriate not to require the payment of a financial penalty but to direct the Organisation to do the following:
    a. To put in place the appropriate contractual provisions to set out the obligations and responsibilities of both the data controller and data intermediary to protect the Organisation's personal data, and the parties' respective roles in protecting the personal data;
    b. To engage qualified security service provider to conduct a thorough security audit of its technical and administrative arrangements for the security and maintenance of its website that contains personal data in the Organisation's possession or control;
    c. Provide the full security audit report to the Commission, no later than 60 days from the date of the issue of this direction;
    d. Rectify any security gaps identified in the security audit report, review and update its personal data protection policies as applicable within 60 days from the date the security audit report is provided; and
    e. Inform the Commission within 1 week of completion of rectification and implementation in response to the security audit report.

The following is the provision of the Personal Data Protection Act 2012 cited in the above summary:

Protection of personal data

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –
(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and
(b) the loss of any storage medium or device on which personal data is stored.