PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPCS 4

Case No. DP-2210-C0345

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

And

Autobahn Rent A Car Pte. Ltd.

SUMMARY OF THE DECISION

1 On 21 October 2022, Autobahn Rent A Car Pte. Ltd. (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a personal data breach (the "**Incident**").

2 The Organisation operates a car-sharing service, Shariot, in Singapore. On 24 September 2022, the Organisation received customer feedback that a photograph on its mobile application had been replaced with a pornographic photograph. The Organisation discovered that the pornographic photograph had been uploaded through an unrevoked administrator account belonging to an ex-employee, who had

left the Organisation in May 2022. The ex-employee received an email from an unknown sender on 10 September 2022 stating that his personal laptop had been hacked and demanding Bitcoins as ransom payment. The threat actor was able to log into the Shariot's mobile application administrator portal through the administrator account belonging to the ex-employee, and used the export CSV function to download a copy of the Shariot's users personal data.

3 Subsequently, on 21 October 2022, a cybersecurity solutions provider alerted the Organisation of a cybercrime forum post offering the sale of a Shariot database containing personal data. The Commission commenced investigations to determine whether the Incident disclosed any breaches of the Personal Data Protection Act 2012 ("**PDPA"**) by the Organisation.

4 The Organisation requested, and the Commission agreed, for this matter to proceed under the Expedited Decision Breach Procedure. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision. It admitted to a breach of the Protection Obligation under Section 24 of the PDPA.

5 The Organisation's internal investigations discovered that compromise of the dormant administrator account credentials enabled the unauthorised access to Shariot backend admin web portal, leading to the exfiltration of 53,000 personal data sets of Shariot users. The personal data that were affected in the Incident included names,

email addresses, mobile phone numbers, NRIC numbers and general location data (e.g. Bishan, Toa Payoh or Orchard).

6 Following the Incident, the Organisation took the following remedial action:

(a) Immediately conducted an internal audit of its administrator accounts to ensure that any employee access that was not required was revoked;

(b) Enhanced its software code and admin panel user interface to mask displayed or exported NRIC numbers to show only the last 4 characters; and

(c) Conducted cyber hygiene and awareness training for all staff handling personal data.

7 The Organisation admitted that it had failed to ensure it had reasonable security arrangements in place to prevent the unauthorized access or disclosure of the personal data in its possession or control, as it failed to implement and ensure reasonable access control to its backend admin web portal. First, the Organisation failed to revoke the login credentials of an administrator account belonging to an ex-employee once the employment relationship came to an end in May 2022. As a result, the ex-employee's administrator login credentials remained active, which – when compromised – enabled the malicious actor access into its network.

8 Second, the Organisation also admitted that the Incident would not have happened if it had implemented multi-factor authentication ("**MFA**") as an additional

access control for its administrator accounts that had access to its sizeable user database. In *Re Lovebonito [2022] SGPDPC 3*, the Commission had highlighted the need for organisations to strengthen access control, through the use of a one-time password ("OTP") or 2FA/MFA, to such accounts. Indeed, regardless of whether an account is an administrative account, once an account is granted access rights to a database containing sensitive personal data records or a significant volume of personal data that would adversely impact the affected individuals in the event of a personal data breach, we would encourage organisations to consider implementing enhanced access controls to the account such as through the use of a OTP or 2FA/MFA to better safeguard the personal data.

9 For the above reasons, the Organisation was determined to have breached the Protection Obligation.

The Deputy Commissioner's Decision

10 In determining whether the Organisation should be required to pay a financial penalty under Section 48J of the PDPA or if directions would suffice, I considered that a financial penalty was appropriate as the personal data breach was not insignificant. In deciding the appropriate financial penalty amount, I first considered all the relevant factors listed at Section 48J(6) of the PDPA, in particular, the impact of the personal data breach on the individuals affected and the nature of Organisation's non-compliance with the PDPA. In this regard, while the NRIC numbers and general

location data was affected, this is less serious than if the NRIC images and specific GPS location had been disclosed.

11 In deciding what would be the appropriate financial penalty amount, I also considered the organisation's turnover to arrive at a figure that would, in my mind, be a proportionate and effective amount, to ensure compliance and deter non-compliance with the PDPA. On the facts of this particular case, the organisation's turnover has been taken into consideration to arrive at a proportionate and effective financial penalty. I also considered the following mitigating factors, which led to a further reduction in the financial penalty:

(a) The Organisation was cooperative during the course of our investigations;

(b) The Organisation voluntarily admitted to breach of the Protection Obligation under the Commission's Expedited Decision Procedure; and

(c) The Organisation took prompt remedial actions following discovery of the Incident.

12 For the reasons above, I hereby require the Organisation to pay a financial penalty of $3,000 within 30 days of the date of the relevant notices accompanying this decision, 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.

13 In addition to the financial penalty imposed, the Organisation is also directed to do the following:

(a) Implement processes for systems and applications revocation within a reasonable window of cessation of need for access by an employee;

(b) Strengthen access controls measures to administrator accounts with access to databases holding personal data;

(c) Conduct reasonable security review of technical and administrative arrangements for the protection of personal data in possession or under control of the Organisation within 60 days of the date of this Direction;

(d) Rectify any security gaps identified in the security review directed above; and

(e) Inform the Commission within 1 week of the completion on the steps directed above.

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

Protection of personal data

24. An organisation must 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 or disposal or similar risks and;
(b) the loss of any storage medium or device on which personal data is stored.