PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPCS 7

Case No. DP-2304-C0935

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

And

Whiz Communications Pte. Ltd.

SUMMARY OF THE DECISION

Introduction

1 Whiz Communications Pte. Ltd. (the "**Organisation**") is a Singapore telecommunications service provider offering broadband internet access, local and long-distance digital IP telephony, prepaid and postpaid calling plans.

2 On 22 April 2023, the Personal Data Protection Commission (the "**Commission**") was alerted by the Singapore Police Force of a personal data breach incident involving the Organisation (the "**Incident**"), which the Organisation confirmed on 24 April 2023.

3 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 and to a breach of the Protection Obligation under Section 24 of the PDPA. Section 24 of the Personal Data Protection Act 2012 ("**PDPA**") requires an organisation to protect personal data in its possession or control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks (the "**Protection Obligation**").

Facts of the Incident

4 The Organisation's customer management system ("**CMS**") was designed and developed in 2016 by an external vendor. This external vendor did not process personal data on behalf of the Organisation and was not the Organisation's data intermediary. The Protection Obligation in respect of customer personal data processed by the CMS therefore fell solely on the Organisation.

5 The CMS from its initial design accepted any Python script requests that could be exploited for unauthorised exfiltration of customer personal data. This failure to block or manage scripts posed a data security risk and was a design flaw.

6 Post-Incident, the Organisation established through tracing web services and databased logs that Python scripts had indeed been used by the threat actor ("**TA**") to extract .jpg files from the CMS. 29,903 attempts from 8 overseas IP addresses were made over 5 days in March and April 2023, with 24,323 successful extractions of the personal data of 24,323 individuals.

7 The types of personal data exfiltrated were the front and back images of identification documents (i.e., NRIC, passport, student pass and dependent pass) and other supporting documents such as tenancy agreements and letters of approval for work permits issued by the Ministry of Manpower, Singapore.

8 Following the Incident, the Organisation took the following remedial actions:

(a) Rejected and denied all Python requests to the CMS;

(b) Restricted overseas IP addresses from connecting to the Organisation's network;

(c) Implemented two-factor authentication and enhanced the password complexity requirement for the CMS' admin users via web access; and

(d) Conducted a penetration test on the CMS.

Findings and Basis for Determination

9 As a Singapore telecommunications service provider, the Organisation had higher-level security needs. This extended to the Organisation's CMS that contained the personal data of individuals who subscribed to the telecommunications services provided by the Organisation.

10 First, the Organisation admitted it has breached the Protection Obligation under the PDPA as it failed to provide any security requirements to the CMS IT vendor, in particular, requirements that would have adequately addressed the data security risks posed by Python scripts.

11 The Organisation admitted that it failed to stipulate clear job specifications and security requirements to the IT vendor who developed the CMS. There was also no contractual obligation on the IT vendor to ensure that personal data would be protected. In SAP Asia Pte Ltd [2021] SGPDPC 6, the Commission had reiterated the need for organisations to provide clear job specifications and include data protection requirements when engaging IT vendors. Thereafter, organisations are also expected to ensure that the IT vendor has satisfied the job specifications and data protection requirements stipulated.

12 Secondly, the Organisation admitted that it was in breach of the Protection Obligation under the PDPA as it neither had a sufficiently complex password policy nor enforced one. In the Commission's Guide to Data Protection Practices for ICT Systems[1], the Commission recommended a minimum of 12 alphanumeric characters with a mix of uppercase, lowercase, numeric and special characters. We also recommended using phrases or paraphrase, combined with numbers and uppercase, lowercase and special characters, as these characteristics will make a password stronger and harder to decode.

13 Prior to the Incident, the Organisation's CMS admin user password complexity required only 9 alphanumeric characters with at least one uppercase, which clearly fell short of PDPC's recommended password complexity. We urge organisations to meet PDPC's recommended best practices relating to passwords, especially for privileged access accounts such as admin accounts.

[1] PDPC's Guide to Data Protection Practices for ICT Systems, page 15. Accessible at https://www.pdpc.gov.sg/help-and-resources/2021/08/data-protection-practices-for-ict-systems.

14 Third, the Organisation also admitted to a breach of the Protection Obligation of the PDPA as it failed to ensure reasonable access control to its CMS. Given the nature of personal data the Organisation was in possession and control of, the Organisation should have enhanced the access control to its CMS beyond the baseline of password protection. This could have taken the form of implementing multi-factor authentication for its CMS admin accounts, restricting access from overseas IP addresses to its CMS, and, last but not least, having an up-to-date web application firewall to defend against typical web application attacks.

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

The Deputy Commissioner's Decision

16 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 given the Organisation involved and the nature of the personal data affected in the Incident.

17 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.

18 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 to deter non-compliance with the PDPA.

19 Finally, I 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.

20 For the reasons above, I hereby require the Organisation to pay a financial penalty of $9,000 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.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION

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.

.