PERSONAL DATA PROTECTION COMMISSION

[2025] SGPDPCS 2

Case No. DP-2406-C2585

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

And

Ezynetic Pte. Ltd.

DECISION

Data Protection *– Protection obligation – Disclosure of personal data – Lack of access controls – Failure to conduct reasonable periodic security review*

SUMMARY OF THE DECISION

1 Ezynetic Pte. Ltd. (the "**Organisation**") is a Singapore-incorporated Software-as-a-Service ("**SaaS**") provider that provides information technology solutions and services to licensed moneylenders in Singapore.

2 On 26 June 2024, the Personal Data Protection Commission (the "**Commission**") was informed about a data breach incident involving the Organisation's servers being infected by ransomware on or about 24 June 2024. Consequently, 190,589 individuals' personal data was exfiltrated and posted for sale on the dark web (the "**Incident**").

3 The Organisation requested, and the Commission agreed, for the investigation to proceed under the Expedited Decision Procedure ("**EDP**"). This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. It also admitted to a breach of the Protection Obligation under Section 24 of the Personal Data Protection Act 2012 ("**PDPA**").

Facts of the Case

4 The Organisation operates an information technology system which was linked to the Moneylenders Credit Bureau ("**MLCB**") platform operated by Credit Bureau (Singapore) Pte Ltd[1] via Application Protocol Interfaces ("**APIs**") (the "**moneylending system**").

[1] Credit Bureau (Singapore) Pte Ltd is the designated credit bureau by Ministry of Law Singapore to operate the MLCB platform.

5 The Organisation's clients would input personal data of their prospective loan applicants and borrowers into the moneylending system which would allow them to verify the applicants' and borrowers' loan eligibility, generate the MLCB credit reports, track the loans, instalments, collections, payments and generation of profit and loss reports.

6 On 24 June 2024, the Organisation discovered that it could not access the moneylending system, and the relevant databases had been deleted by a threat actor who managed to gain access to its database server.

7 Investigations found that the threat actor had exploited a vulnerable web service application to gain access and control of its system administrator ("**SA**") account[2] to access the moneylending system. After gaining access to the moneylending system, the threat actor exfiltrated the personal data of the affected individuals.

8 The personal data exfiltrated included a combination of the name, address, email address, telephone number, NRIC number, date of birth and the financial information available in the MLCB Credit Reports of 190,589 individuals.

9 The MLCB platform was not compromised as the Incident only involved unauthorised access into the Organisation's internal systems by the threat actor.

10 Investigations revealed the following lapses by the Organisation that had contributed to the Incident:

[2] The SA account login, short for *system administrator,* is one of the riskiest server-level principals in SQL Server. It's automatically added as a member of the sysadmin fixed server role and, as such, has all permissions on that instance and can perform any activity.

a. The Organisation failed to disable or adequately secure the SA account which is a well-known SQL server account, and is often targeted by malicious users. The access controls mechanism implemented for the SA account was inadequate. The password, at the time of the Incident, which was p@ssword1 or Password@1, was susceptible to brute force attacks; and

b. The Organisation did not perform any periodic vulnerability assessment or penetration testing of its infrastructure.

Remedial Action

11 Following the Incident, the Organisation promptly took the following remedial actions:

a. Rebuilt its entire network and migrated to a cloud environment for its servers;

b. Enhanced security measures were implemented for the new network after consultations with the Cybersecurity Agency of Singapore ("**CSA**") and the Ministry of Law Singapore; and

c. Notified all affected clients on 1 July 2024.

Findings and Basis for Determination

Whether the Organisation had contravened the Protection Obligation

12 Under section 24(a) of the PDPA, organisations must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks.

13 Taking into account the Organisation's admission, and for the reasons set out below, the Deputy Commissioner determines that the Organisation failed to implement reasonable security arrangements to protect the personal data in its possession and/or control, thus acting in breach of section 24 of the PDPA:

a. Failure to have reasonable access control. The volume and types of personal data in the possession and under the control of the Organisation required it to have adopted enhanced access controls. Given that the SA account granted privileged access to the Organisation's moneylending system, adequate authorisation and authentication processes were required. This includes the implementation and enforcement of a strong password policy that includes a minimum level of password complexity, and a fixed period of password validity or regular change of passwords, the weak password used for the moneylending system during the Incident was an inadequate security arrangement to safeguard the personal data contained in the moneylending system.

b. Failure to conduct reasonable periodic security review. At the time of the incident, no network vulnerability assessments or penetration testing had been conducted. As stated in page 5 of the Commission's Checklists to

Guard Against Common Types of Data Breaches (the "**Checklists**")[3], organisations should, as a basic practice, periodically conduct web application vulnerability scanning and assessments post deployment. The Organisation's failure to conduct reasonable periodic security review amounted to a breach of section 24 of the PDPA.

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

The Deputy Commissioner's Preliminary Decision

Financial Penalty

15 In determining whether to impose a financial penalty on the Organisation under Section 48J of the PDPA, the Commission considered that a financial penalty was appropriate given the role of the Organisation as a SaaS provider that processes personal data entrusted to it by its client. As a SaaS provider, the Commission the Organisation should possess the necessary technical expertise to implement reasonable cybersecurity measures to address the evolving threats.

16 In deciding the appropriate financial penalty amount, the Commission first considered the impact of the personal data breach on the individuals affected and the nature of Organisation's non-compliance with the PDPA. In addition, in order to ensure that the financial penalty imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with the PDPA, the Commission also considered the Organisation's annual turnover.

[3] https://www.pdpc.gov.sg/help-and-resources/2021/08/data-protection-practices-for-ict-systems

17 The Commission also considered the following factors:

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

b. The Organisation voluntarily admitted to breach of the Protection Obligation under the EDP; and

c. This is the Organisation's first instance of non-compliance with the PDPA.

18 Based on the foregoing, the Deputy Commissioner made a preliminary decision to impose a financial penalty of $17,500 on the Organisation for its breach of the Protection Obligation.

19 In addition, to ensure the Organisation's compliance with the Protection Obligation, the Deputy Commissioner also directed the Organisation, under section 48I of the PDPA, to obtain CSA's Cyber Trustmark Certification for its new IT network and report to the Commission on its completion.

Representations Made by the Organisation

20 The Organisation was notified of the preliminary decision by way of the Commission's letter dated 2 December 2024 and was invited to make representations. On 3 December 2024, the Organisation made the following representations to the Commission seeking a waiver or reduction in the financial penalty:

a. The Organisation had expended significant financial commitment to investigate, mitigate the effects of the breach and fortifying its systems against future cybersecurity threats;

b. It had suffered significant operational disruptions and continued financial losses as a result of the Incident; and

c. It had maintained full transparency and cooperation with all regulatory bodies throughout the investigation.

21 After careful consideration, the Organisation's representations were not accepted for the reasons outlined below:

a. The fact that the Organisation has expended significant financial commitment to implement remedial measures post-data breach does not warrant a further reduction, as it is a necessary part of its obligation to implement reasonable security arrangements under the Protection Obligation.

b. The operational disruptions and financial losses suffered by the Organisation were part of the vicissitudes of dealing with the aftermath of a serious data breach incident and its previous non-compliance with the Protection Obligation. Whilst the Organisation did provide some invoices showing that it had incurred expenses to implement remedial measures, these did not show that the Organisation is in such a dire financial situation that the imposition of a financial penalty of $17,500 would adversely impact its ability to continue its business; and

c. The Commission had already taken into account of the cooperativeness of the Organisation, in arriving at the preliminary decision.

The Deputy Commissioner's Decision

22 Having considered all the relevant circumstances of this case, the Deputy Commissioner hereby requires the Organisation to pay a financial penalty of $17,500 within 30 days from the date of the relevant notice accompanying this decision, failing which interest at the rate specified in the Rules of Courts in respect of judgement debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

23 For completeness, the Organisation is also directed to:

a. Obtain CSA's Cyber Trustmark Certification for its new IT network within 9 months from the date of this Decision; and

b. To report to the Commission within 14 days upon completion of the above action outlined above.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION

The following section(s) of the Personal Data Protection Act 2012 had been cited in the above Summary of The Decision:

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.