PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPC 1

Case No. DP-2002-B5827

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

And

PINC Interactive Pte. Ltd.

… *Organisation*

DECISION

PINC Interactive Pte. Ltd.

[2022] SGPDPC 1

Lew Chuen Hong, Commissioner — Case No. DP-2002-B5827

4 February 2022

Introduction

1 On 2 February 2020, the Personal Data Protection Commission ("**the Commission**") received feedback about a Twitter post dated 31 January 2020 which revealed that the personal data of users of www.pincstyle.com had been exposed. The tweet included a snapshot of the data ("**the Incident**"). The Commission commenced investigations into the Incident thereafter.

Facts of the Case

2 The website www.pincstyle.com was created and managed by PINC Interactive Pte. Ltd. ("**the Organisation**") at the material time. Investigations revealed that sometime in October 2019, a database comprising 252,813 records was accessed and exfiltrated from the Organisation's staging servers (the "**Staging Database**"). The Staging Database is a synthetic database containing personal data of 3,916 actual users, while the remaining 248,897 records were fake or "dummy" data modelled after the real data. The synthetic database was used to facilitate development and testing on the staging servers. The personal data from the 3,916 actual users that were exposed in the Incident included the name, username, email address, contact number (for some users) and a password hash. For completeness, the 3,916 user records in the Staging Database is equivalent to 1.6% of the Organisation's total database of 252,813 user records.

3 Investigations revealed two likely causes of the Incident. First, the developers, who are the Organisation's employees, had retained a copy of the Staging Database on their own personal devices, and the database was exfiltrated when the developers' computers were compromised. The Organisation stated that while they had instructed the developers to use strong passwords, the developers were left to manage the security settings on their own computers, and only had antivirus software installed.

4 Second, unauthorised access may have occurred from May 2019 to October 2019 when the Organisation did not require authentication for the Application Programming Interface ("**API**") under testing ("**Staging API**"), which pointed to the Staging Database containing the personal data of real users, despite the Staging Database being accessible over the Internet. The Organisation only implemented access key authentication from October 2019 onwards.

Remedial actions

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

a. Updated the API with new authentication keys;

b. Limited the access of authentication keys to only the senior developers;

c. A password reset was initiated for affected users via email; and

d. Developers were instructed to delete their local copy of the Staging Database and scan their own computers for malware.

Findings and Basis for Determination

Whether the Organisation contravened the Protection Obligation

6 Section 24 of the Personal Data Protection Act 2012 ("**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 "**Protection Obligation**"). For the reasons set out below, the Organisation failed to implement reasonable security arrangements to protect the personal data in the Staging Database.

7 Firstly, the Organisation had failed to accord adequate protection to the personal data by allowing their employees, i.e. the developers, to store local copies of the Staging Database in their own personal devices, without implementing any additional security requirements. Allowing their employees to store the Staging Database in their own personal devices constituted a breach of the Protection Obligation, given that the Staging Database did not merely contain purely synthetic data, but also the personal data of real users.

8 Secondly, the Organisation was also in breach of the Protection Obligation as it merely instructed its employees not to use weak passwords on their personal devices, and left it to each individual employee to decide if and what level of security measures ought to be implemented on their own personal devices to protect the personal data. Indeed, even though the developers had purportedly installed antivirus software on their own personal devices, the Organisation was unable to provide the product name, version, or the frequency of the antivirus updates that the developers supposedly implemented on their end when questioned.

9 In *Learnaholic Pte. Ltd.*[1], the Organisation was found in breach of section 24 of the PDPA as the personal data affected had been sent to and stored in the work email account belonging to the Organisation's representative in an *unencrypted* form. After completing the task at hand, the representative failed to delete the email containing the personal data that he received. Instead, the representative kept the email containing the personal data, in case he needed it in future. As a result, the hacker had free rein to the personal data affected once he obtained access to the email

[1] [2019] SGPDPC 31.

account. In a similar vein, the Organisation here has failed to adopt adequate security measures when it simply allowed its employees to retain a copy of the Staging Database on their own personal devices, without putting any thought to the security measures that ought to be implemented to protect the personal data.

10 Finally, while we appreciate that the Organisation wanted the Staging API to mirror the production environment, it was not a reasonable "protection" measure to commingle synthetic data with the personal data belonging to real users, without processing the personal data of the real users before doing so, as this meant that the Staging Database contained the data of real users. Having decided to use personal data belonging to real users in the Staging Database, the Organisation has breached the Protection Obligation by failing to require authentication before the Staging API could be accessed. If the Organisation's intention was not to require authentication for the Staging API, the Organisation should have chosen to use only synthetic data in the Staging Database. In *How to Guard Against Common Types of Data Breaches* (the "**Handbook**"),[2] the Commission identified the five most common gaps in ICT system management and processes, and observed at page 11 of the Handbook that:

> "Out of convenience, many organisations use production data for system testing in their test environments. But as test environments tend to be much less secured, there is a high risk of data breach in a test environment."

11 In the Handbook, the Commission explained that synthetic data can be generated either from scratch using commercial tools or by anonymising production data, and recommended that organisations can create synthetic data (i.e. fake personal data or data anonymised from real data) for **development and testing purposes in non-production environments** instead of using real data.

[2] https://www.pdpc.gov.sg/news-and-events/announcements/2021/05/handbook-on-how-to-guard-againstcommon-types-of-data-breaches-now-available

12 In this case, the Organisation could have chosen to use 100% synthetic data or anonymise the personal data before using them if it did not wish to require authentication for the Staging API. In light of the above, we are also of the view that the Organisation breached the Protection Obligation by using personal data belonging to real users in the Staging Database, but failing to require authentication before the Staging API could be accessed.

Whether the Organisation contravened the Accountability Obligation

13 Section 12(a) of the PDPA requires an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA (the "**Accountability Obligation**").

14 The Organisation admitted that they did not have any data protection policies or practices in place for their "non-technical" employees, who have access to "public user data". In its reply, the Organisation drew a distinction between its "technical" and "non-technical staff", and stated that for the "technical" staff, the data protection policies in place extended to the Organisation's team lead providing a briefing to the "technical" staff of the system, rules for branch creation and the code standard during onboarding. The information provided by the Organisation to its "technical" staff, during their onboarding, serves merely to facilitate the performance of these employees' core duties, and cannot be equated with or amount to data protection policies or practices.

15 Indeed, the Organisation's reply reflects a lack of understanding of what data protection policies and processes seek to achieve and implement. We have previously stressed the critical role that data protection policies and practices play in increasing awareness and ensuring accountability of an organisation's obligations under the PDPA in *Re Aviva Ltd*[3]. We also explained in *Re Singapore Cricket Association*[4] that data protection policies and practices ensure that employees will be able to better

[3] [2018] PDP Digest 245 at [32].
[4] [2019] PDP Digest 270 at [19].

protect personal data when they are first able to recognise a matter as one involving data protection.

16 Given the Organisation's reply, it follows that the Organisation did not in fact have any data protection policies or processes in place to guide their employees on how to comply with the PDPA in carrying out their work functions. The Organisation has therefore breached the Accountability Obligation.

The Commissioner's Directions

17 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and if so, the amount of such financial penalty, the factors listed at section 48(6) of the PDPA were taken into account, as well as the following aggravating and mitigating factors:

Aggravating Factors

(a) The Organisation allowed its employees to keep local copies of the Staging Database on their personal devices, without considering and undertaking any security measures needed to protect the personal data of real users;

Mitigating Factors

(b) The Organisation was cooperative in the course of investigations and had provided prompt responses to PDPC's requests for information; and

(c) The Organisation was implemented remedial actions to address the Incident.

18 In the course of settling this decision, the Organisation made representations on the amount of financial penalty that the Commissioner intended to impose.

The Organisation raised the following factors for the Commissioner's consideration:

(a) The Organisation had engaged an external consultancy firm to ensure that its obligations under the PDPA are upheld to the highest standards with periodic audits, training and risk assessments; and

(b) The Organisation was incorporated in 2018 and is still a relatively young company. Since its inception, it had been suffering significant losses in its operation.

19 Having considered the Organisation's representations, as well as all the relevant factors of this case, the Commissioner hereby decided to impose a reduced financial penalty of $12,500 on the Organisation. The quantum of financial penalty has been calibrated and reduced after due consideration of the Organisation's financial circumstances, bearing in mind that any financial penalty imposed should not be crushing or cause undue hardship on organisations.

20 Taking into account all the relevant facts and circumstances, the Commissioner hereby:

(a) Requires the Organisation to pay a financial penalty of $12,500 within 30 days from the date of the relevant notice accompanying this decision, failing which interest at the rate specified in the Rules of 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;

(b) Directs the Organisation to:

(i) Develop and implement internal data protection policies and practices to comply with the PDPA within 60 days of the relevant direction accompanying this decision;

(ii) Ensure that no local copies of the database are stored on the personal computers of any employees (including both developers and senior developers) within 60 days of the relevant direction accompanying this decision; and

(iii) To notify the Commission within 1 week of the completion of this direction.

21 Although the Commissioner has imposed a lower financial penalty on the Organisation in this case, the financial penalty was arrived at after considering the dismal state of the Organisation's finances, and should be confined to the specific facts of this case.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION