Editorial note: An application for reconsideration was filed against the decision in *Re Chizzle Pte Ltd* [2019] SGPDPC 44. Upon review and careful consideration of the application, the Commissioner has decided to affirm the finding of breach of section 24 of the PDPA as set out in the decision and the direction. The Reconsideration Decision can be found at *Re Chizzle Pte Ltd* [2020] SGPDPCR 1.

Chizzle Pte. Ltd.

[2019] SGPDPC 44

Tan Kiat How, Commissioner — Case No. DP-1807-B2495

Data protection – Protection obligation – Disclosure of personal data – Insufficient security arrangements

26 November 2019

Introduction

1 Chizzle Pte. Ltd. (the "**Organisation**") provides a mobile application (the "**Mobile App**") designed to connect learners and teachers in Singapore, Australia and India. On 31 July 2018, the Organisation notified the Personal Data Protection Commission (the "**Commission**") of a cyberattack (the "**Incident**") which had compromised the personal data of about 2,213 users of the Mobile App, including some users in Singapore (the "**Affected Individuals**").

Material Facts

2 On 30 July 2018, the Organisation noticed that the Mobile App had stopped responding. It was found that an unauthorised party had deleted its database containing the personal data of the Affected Individuals (the "**Chizzle Database**") and left a ransom demand in text. The personal data in question included the names, dates of birth, genders, email addresses and some mobile numbers and residential addresses of the Affected Individuals (the "**Compromised Personal Data**"). Before this, on 9 July 2018, the Organisation had changed the Chizzle Database from Amazon's Relational Database Service to the MySQL relational database.

3 Since 2016, the Organisation had a "L.A.M.P." stack (i.e. Linux operating system, Apache HTTP server, MySQL server and PHP) (collectively with the Mobile App, the "**System**") as part of its IT infrastructure. "phpMyAdmin", a MySQL database administration tool, was installed with the L.AM.P stack. The tool was configured to allow remote access to it from the Internet. The Organisation believed that the unauthorised party gained entry into the Chizzle Database through the phpMyAdmin tool by a brute force attack. However, it did not have the logs to prove that a brute force attack had taken place. Regardless, the unauthorised party gained entry to the Chizzle Database through the phpMyAdmin tool. This gave the unauthorised party full control, including reading, writing and deleting data.

Remedial actions by the Organisation

4 Following the Incident, the Organisation has taken measures to prevent unauthorised access to the Chizzle Database in the future, including the following:

(a) IP address access via phpMyAdmin (i.e. use of IP address to find and reach the Chizzle Database) was turned off and the phpMyAdmin tool was uninstalled;

(b) The IP address of the Organisation's servers, including the Chizzle Database server, were changed; and

(c) The Mobile App and Chizzle Database were moved to new hardware in case any residual malware or Trojans remained in the old hardware.

Findings and Basis for Determination

*Whether the Organisation had breached its obligation to protect personal data under section 24 of the Personal Data Protection Act 2012 ("**PDPA**")*

5 Section 24 of the PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

6 The Organisation had failed to conduct any security review of its System although past decisions by the Commission had made clear the need for such reviews (see e.g. *WTS Automotive Services Pte Ltd.* [2018] SGPDPC 26, *Bud Cosmetics* [2019] SGPDPC 1 and *Watami Food Service Singapore Pte Ltd* [2018] SGPDPC 12).

7 The Organisation claimed that it was not even aware that the phpMyAdmin tool was part of its System. It also claimed it had no need of the tool. A reasonable security review

would have included a review of all web-connected features of the System. Through such a review, the Organisation would have found the phpMyAdmin tool and could have decided whether to remove or keep it. If the Organisation had decided to retain the tool, the review would have given opportunity for the Organisation to review its security against web-based threats.

8 However, as found above, the Organisation failed to conduct a security review. It therefore missed the opportunity to determine its need for the phpMyAdmin tool and to address the security requirements of the tool, if retained. A security review would have been the arrangement through which the Organisation could reasonably have prevented the unauthorised entry into the Chizzle Database through the tool.

9 On the facts above, the Commissioner found that the Organisation had not made reasonable security arrangements to protect the Compromised Personal Data and was accordingly in breach of section 24 of the PDPA.

The Organisation's Representations

10 After the preliminary decision was issued, the Organisation submitted representations requesting for a reduction to the quantum of financial penalty. In support of its assertion that the proposed penalty was "more than likely to push [it] to a brink of closing the business", the Organisation submitted copies of its financial statements and bank account statements. The Organisation did not disagree with, or make any representations relating to, the Commissioner's findings that it had breached section 24 of the PDPA.

11 In general, financial penalties imposed under the PDPA reflect the seriousness of the breach and do not take into account the financial position of the organisation in question. However, a financial penalty is not meant to impose a crushing burden on the organisation and cause undue hardship: *Re Sharon Assya Qadriyah Tang* [2018] SGPDPC 1 at [34]. In the present case, the financial standing that was gleaned from the submitted financial statements and bank account statements was dire. In order to avoid imposing a crushing burden on the Organisation, the Commissioner has decided to reduce the financial penalty. For this reason, the financial penalty imposed in this case should not be taken as establishing a precedent for future cases.

12 In order to ensure that the Mobile App is robust and secure, the Organisation should adopt a data protection by design approach. While the optimal approach is to do so from the commencement of every developmental project, it is nevertheless still possible to do so during the maintenance phase, whenever there are enhancements: Data Protection by Design Guide, at p 35. The Organisation is directed to review its developmental processes in order to adopt a data protection by design approach for future enhancements to the Mobile App. Making changes to its practices will help the Organisation scale its Mobile App for future growth, and will pay longer term dividends than a hefty financial penalty.

The Commissioner's Directions

13 In view of the above findings, the Commissioner decided to direct the Organisation to pay a financial penalty of $8,000 within 30 days from the date of this direction, 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.

14 In addition, the Commissioner decided to issue the following directions to the Organisation to ensure its compliance with the PDPA:

(a) Engage duly qualified personnel to conduct a security audit of its mobile application and accompanying IT system;

(b) Furnish a schedule stating the scope of risks to be assessed and the time within which a full report of the audit can be provided to the Commission within 30 days of this direction;

(c) Rectify security gaps identified in the security audit;

(d) Develop an IT security policy to guide its employees on the security of personal data on its mobile applications and accompanying IT systems within 60 days from the date of completion of the above-mentioned security audit;

(e) Within 120 days of this decision, review and revise its developmental processes in order to adopt a data protection by design approach for future enhancements to its mobile application; and

(f) Inform the Commission in writing of the completion of each of the above directions within 1 week of completion.