Re Chizzle Pte Ltd

[2020] SGPDPCR 1

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

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

14 February 2020

Background and Application for Reconsideration

1 In *Re Chizzle Pte Ltd* [2019] SGPDPC 44 (the "**Decision**"), Chizzle Pte Ltd (the "**Organisation**") was found to be in breach of section 24 of the Personal Data Protection Act 2012 (the "**PDPA**"). The grounds of decision and the full facts of the case are set out in the Decision. Briefly, an unauthorised party had gained access to the Organisation's servers, deleted a database (referred to as the "**Chizzle Database**" in the Decision) which contained certain personal data (referred to as the "**Compromised Personal Data**" in the Decision) and left a ransom demand in text (the "**Incident**"). The Organisation was found to have failed to make reasonable security arrangements to protect personal data in its possession and/or control and directed to pay a financial penalty of $8,000 and undertake various measures to ensure its compliance with the PDPA. The Organisation has now submitted an application for the reconsideration of the

Decision (the "**Application**") that in substance appears to be a request for all the directions imposed to be lifted or, in the alternative, a reduction in the quantum of the financial penalty imposed.

The Organisation's Submissions

2 The Organisation raised two sets of arguments in the Application. The first related to its assertion that it was not in breach of PDPA while the second sought a reduction in the quantum of the financial penalty imposed.

(a) Whether the Organisation was in breach of the PDPA

3 In support of its assertion that it was not in breach of the PDPA, the Organisation contends that it had taken appropriate steps which were standard practice in the industry to protect the Compromised Personal Data and there were no procedural or process errors, system issues, personnel oversight, callousness or mistake that resulted in the unauthorised access to the Chizzle Database and deletion of the said personal data.

4 In this regard, the Organisation raised the following points:

(a) The IT infrastructure of the Organisation is hosted on one of the best in class service providers i.e. Amazon Web Services;

(b) The Organisation was a victim of a deliberate security breach on its system as is evident by the ransom note left by the hacker;

(c) The IP address of the servers on which the database and the phpMyAdmin tool resided were not published;

(d) The password of the database (which is the password that needs to be used to log on to the phpMyAdmin tool) was changed frequently and also was a complex password; and

(e) The Cloudflare tool was implemented as a firewall and prevention of DDOS attacks.

5 However, the matters set out at [4] above do not demonstrate that the Organisation has fulfilled its obligations under section 24 of the PDPA based on the facts of this case. In particular:

(a) The Incident was not a result of a deliberate security breach on the hosting service for the Organisation's System (as defined in the Decision) or a result of any security vulnerabilities at the infrastructure or hosting layer. Instead, the unauthorised access to the Organisation's System was through the phpMyAdmin tool which was under the Organisation's direct control (i.e. not within hosting service provider's control). The fact that the IT System was hosted on Amazon Web Services does not address any security risks that originate within the Organisation's System. Any security measures implemented by the

hosting service provider would not have been able to address the vulnerabilities in the Organisation's System and would not have prevented the occurrence of the Incident;

(b) The Organisation is not absolved from its failure to protect personal data merely because the security of its system was deliberately breached by an external malicious actor. Section 24 of the PDPA requires the Organisation to implement security arrangements to protect personal data from unauthorised access, disclosure and deletion, amongst others, including where the access, disclosure or deletion is caused by a deliberate security breach;

(c) While the IP address of the relevant servers were not published publicly, hackers may not require knowledge of the IP address to gain access into systems. As an example, hacking tools can detect the presence of specific applications, such as the phpMyAdmin tool, using the hostname and the tool's default URL name

(d) While the password of the database Chi!zzle@2018 may have met recommended complexity rules in form[1], it was in fact a weak

[1]See PDPC's Guide to Securing Personal Data in Electronic Medium which states that one of the good practices recommended for passwords used for authentication is to have a length of at least 8 characters, 1 alphabetical character and 1 numeric character.

(*cont'd on next page*)

password that was guessable and vulnerable to brute force attacks. In this regard, various articles/guides[2] have stated that the use of an organisation's name as a component of the password is not recommended because it is not difficult to guess and cracked by hackers. The digits "2018" as a component of the password was also guessable, for example, through brute force or dictionary attacks. As such, the password used by the Organisation failed to prevent unauthorised copying and deletion of the Chizzle Database; and

(e) The usage of Cloudflare would not have prevented the Incident as there was no DOS/DDOS attack involved.

6 Furthermore, the Organisation's Application did not address the grounds of the Decision on which the finding that the Organisation had breached section 24 was based, which is that the Organisation had failed to conduct any security review of its System. In this regard, the Decision states:

> 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

[2]For example, please see https://support.microsoft.com/en-us/help/4026406/microsoft-account-how-to-create-a-strong-password and https://community.sophos.com/kb/en-us/127952.

> 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.

7 While the Organisation has in its Application asserted that its IT vendor undertook a security review and testing at regular intervals, such a security review was only conducted for the purposes of testing the security of the Organisation's mobile application (which is installed on mobile devices) and not the Organisation's System (which is hosted on the cloud).

(b) Whether the financial penalty imposed on the Organisation should be reduced

8 The Organisation also raised the following matters, which (they assert) should be taken into consideration in reducing the quantum of the financial penalty imposed:

(a) The Organisation is an early stage start up earning insignificant revenues;

(b) The Organisation promptly notified the Commission and its consumers of the breach;

(c) The Organisation took immediate steps to investigate and restrict access to the utility which caused the breach;

(d) The Organisation has complied with the directives of the Commission during the investigation in a timely manner;

(e) The Organisation is committed to investing in the required actions as advised by the Commission;

(f) The Organisation was a victim of a hacking and ransom attempt; and

(g) The financial penalty imposed is likely to force the Organisation into closing down its business and it would not be able to raise funding for its platforms.

9 The matters raised in [8(a), 8(b), 8(g)] were previously raised by the Organisation in its representations to the Commission in the course of settling the Decision. They had already been taken into account and the financial penalty was reduced to the amount stated in the Decision. The Commissioner had also already taken into consideration the matters in [8(c) and (d)] and they do not warrant a further reduction in the financial penalty.

10 With respect to the matters in 8(e) and 8(f)], these are not mitigating factors which warrant a reduction in the financial penalty. The Organisation is required to comply with the PDPA and any directions issued thereunder. Further, as stated at [5(b)] above, the Organisation is not absolved of its obligations to comply with the PDPA merely because it suffered a deliberate security breach.

Conclusion

11 Given the foregoing, the Commissioner affirms the directions in the Decision. The Organisation is required to comply with the Directions set out in the Grounds of Decision save that the timelines for the Organisation to comply with the directions shall take effect from the date of this Reconsideration Decision.

———————————