PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 11

Case No DP-1712-B1471

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

And

Ncode Consultant Pte Ltd

… *Organisation*

DECISION

Ncode Consultant Pte Ltd

Tan Kiat How, Commissioner — Case No DP-1712-B1471

6 June 2019

Background

1 This is a case of 6 students using teachers' login credentials to access Victoria School's NTRIX School Management system ("**NTRIX**"). The students were able to obtain the login credentials of teachers by exploiting a SQL vulnerability found in NTRIX (the **"Incident"**). Ncode Consultant Pte Ltd ("**Ncode**") supplied NTRIX to various schools, including Victoria School. Victoria School is a school organised and conducted directly by the Ministry of Education ("**MOE**").

2 On 5 December 2017, the Government Technology Agency of Singapore on behalf of MOE reported to the Personal Data Protection Commission (the "**Commission**") that the NTRIX system for Victoria School suffered a total of 84 unauthorised logins (the "**Unauthorised Logins**") between 3 August to 17 October 2017.

3 Following an investigation into the matter, the Commissioner found Ncode in breach of section 24 of Personal Data Protection Act 2012 ("**PDPA**").

Material Facts

4 Ncode is a school administrative system developer, and has been working with schools since 1994. NTRIX is a web application/portal managed by Ncode. There were 3 levels of users (i) student/parent; (ii) teaching/non-teaching employees; and (iii) administrator. By logging in with their respective passwords, teachers could enter examination scores and comments. Students and parents could also login to view results.

5 At the time of the Incident and Unauthorised Logins, there were 2792 records of students' personal data stored as part of Victoria School's instance of NTRIX. In each record, the students' personal data may include all or some of the following information: student name, admission number, residential address, mobile number, parents' names and contact details, subject proficiency rating at primary 6, current examination scores at Victoria School and examination summary ratings (collectively, "**Personal Data**").

6 The Incident and the Unauthorised Logins exposed the Personal Data to risk of unauthorised access, use and modification. In addition, the unauthorised users could view confidential data of the students (e.g. examination results before it is published). There were also 11 instances of modification of examination results for 10 students. The investigations revealed no evidence of mass data exfiltration. The unauthorised modifications to the examination results were rectified by Victoria School, and there was no impact on the students' grades.

7 Ncode took the following remedial actions after discovery of the unauthorised access on 11 October 2017:

(a) 12 to 13 October 2017: Two factor authorisation (2FA) was introduced for Victoria School's employee logins to NTRIX;

(b) 14 to 17 October 2017: Ncode identified and fixed the SQL injection[1] vulnerability that led to the Unauthorised Logins;

(c) 21 October 2017: Ncode fixed all high risk items found using OWASP ZAP[2] active scan;

(d) February 2018: Ncode informed all of its developers of the proper use of the security scanning tools VCG[3] and OWASP ZAP. Ncode also installed automatic security scans and committed to conduct penetration testing as scheduled. In addition, Ncode's Data Protection Officer was instructed to review Ncode's data protection policies; and

(e) March 2018: Ncode initiated the use of the correct features of automatic testing tools to actively test NTRIX for vulnerabilities

The Commissioner's Findings and Basis for Determination

8 It is not disputed that the Personal Data is "personal data" as defined in section 2(1) of the PDPA. There is no question or dispute that Ncode falls within PDPA's definition of "organisation". In the course of investigations, it was

---

1 SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

2 OWASP ZAP (short for Zed Attack Proxy) is an open-source web application security scanner.

3 VCG (short for Visual Code Grepper) is an automated security review tool that handles C/C++, C#, Java, VB and PL/SQL.

determined that Ncode was at all material times an independent third party service provider to, and therefore was not acting on behalf of, MOE. Neither did Ncode raise the applicability of section 4(1)(c) at any time. In the circumstances, section 4(1)(c)[4] of the PDPA does not apply.

Whether Ncode complied with its obligations under section 24 of the PDPA

9 Ncode was appointed to supply NTRIX to Victoria School as well as to set up, host and maintain NTRIX for Victoria School for the period 1 January 2017 to 31 December 2017 pursuant to an Invitation to Quote ("**ITQ**") and the annexed Quotation Conditions of Contract read together with Ncode's ITQ Submission dated 14 December 2016 (collectively referred to as the "**Contract**"). Pursuant to the Contract, Ncode assisted Victoria School to upload the relevant databases containing the Personal Data for use with NTRIX and was obliged to comply with MOE IT Security Specifications for School-managed Systems ("**MOE IT Security Specs**").

10 It is not disputed that Ncode's scope of work in the Contract included processing Personal Data in NTRIX nor that it was in possession or control of the Personal Data. The Commissioner therefore finds that Ncode was acting as a data intermediary of Victoria School.

---

[4] Section 4(1)(c) of the PDPA provides that "any public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data is not subject to the obligations under Parts III to VI of the PDPA"

11 In the circumstances, Ncode had an obligation to put in place reasonable security arrangements to protect the Personal Data which was in its possession and/or under its control.[5]

12 Based on the investigations, there were 2 causes of the Incident and the Unauthorised Logins:

(a) The exploitation, by one of the students, of the NITRIX' SQL injection vulnerability using a publicly available SQLMap tool to discover usernames and encoded passwords stored as part of NTRIX for employee and administrator logins. The passwords were then decoded and shared with other unauthorised users. This allowed the unauthorised users to gain access to the Personal Data and make changes.

(b) The passwords found in the NITRIX system were not encrypted or hashed but were merely encoded in Base 64. The passwords were easily decoded with a publicly available online decoder. Once this was done, they were linked to the usernames of the account holders. The decoded passwords could then be used to access the web application with a legitimate existing user account.

13 SQL injection vulnerability was, at the material time, and still is, a common and well known information technology security threat used by hackers to access computer systems without authorisation. The SQLMap injection program used in the Incident did not require sophisticated knowledge in order to exploit the SQL injection vulnerability found in NTRIX. Detecting and fixing such a basic form of SQL injection vulnerability did not require

[5] See Section 4(2) read together with section 24 of the PDPA

specialist IT security skills but is within the expertise of the average software developer.

14 Further, paragraph 16.4(g) of the MOE IT Security Specs specifically highlighted SQL injection vulnerability flaws and required such flaws to be rectified in the application system by Ncode before deployment. Regular security vulnerability scanning was also required under paragraph 21.13 of the MOE IT Security Specs. Security scanners would have detected the SQL injection vulnerability found in NTRIX if used with the correct settings and features. However, Ncode failed to use the features available in security scanning tools like VCG and OWASP ZAP to actively detect common software vulnerabilities like the SQL injection vulnerability in this case.

15 Also, encoding passwords using Base64 is not a reasonable security arrangement to protect the Personal Data, as these may be easily reversed with publicly available online decoder as was done in this case. In the case of *ComGateway (S) Pte Ltd* [2017] SGPDPC 19, the Commissioner found that encoding a Shipment ID using Base64 is not an actual means of encryption. Base64 is a common and simple encoding scheme, easily decoded through publicly available decoding tools. ComGateway was found in breach of Section 24 of the PDPA because the URL of the Shipping Webpage unique to each customer (by virtue of the Shipment ID encoded in Base 64) could be easily manipulated and ComGateway did not put in place security measures to address this vulnerability.

16 Investigations showed that the 2 causes of the Incident as well as the Unauthorised Logins were due to the inexperience of Ncode's engineers in IT security. An engineer with reasonable IT security knowledge would have (i)

detected and fixed the basic form SQL injection vulnerability; and (ii) applied adequate password protection measures for all passwords.

17 In responses to Notices to Produce, Ncode admitted that its engineers were unfamiliar with IT security and lacked basic understanding of the correct settings/features of security scanners needed to detect SQL injection vulnerability. These engineers also did not understand the basic features of encoding, hashing and encrypting to protect passwords properly. In fact, paragraph 8.4 of the MOE IT Security Specs required Ncode to ensure its technical and security personnel are trained in IT security and are aware of the security implications of the work performed. There is no excuse for Ncode's failure to train the relevant employees in IT security.

18 The investigations also revealed that the NTRIX system had other vulnerabilities which were undetected. These included Broken Session Management[6] and Cross-site scripting[7]. While these vulnerabilities were not exploited in the Incident or in respect of the Unauthorised Logins, they exposed the Personal Data stored in NTRIX to unauthorised access.

19 In addition, the Incident not only resulted in unauthorised access, but also unauthorised modification of students' examination results. While there was no harm suffered by the students as Victoria School managed to rectify the unauthorised modifications, this will not always be the case. The Commissioner would like to emphasize that the failure to put in place reasonable security

---

6 A weakness that allows a hacker to either capture or bypass authentication methods due to improper management of sessions

7 Enables a hacker to inject client side scripts allowing the hacker to bypass access controls

arrangements to prevent unauthorised modification is a serious breach of an organisation's obligation to protect personal data. Changes to examination results could have had an impact on the academic performance of the students affected.[8] In this regard, an attacker may stealthily make unauthorised modifications which may be difficult to detect, and consequentially cause significant harm. Possible security arrangements to prevent unauthorised modification include automatic notification when changes are made to static historical personal data or the need for a higher level of access rights to make any changes to such personal data, given the significance of examination results to students' academic performance.

20 For the reasons above, the Commissioner finds Ncode in breach of section 24 of the PDPA.

The Commissioner's Directions

21 Given the Commissioner's findings that Ncode is in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to issue Ncode such directions as it deems fit to ensure compliance with the PDPA. This may include directing Ncode to pay a financial penalty of such amount not exceeding S$1 million.

22 In assessing the breach and determining the directions, if any, to be imposed on Ncode in this case, the Commissioner took into account the following aggravating factors:

---

[8] See "ASEAN Scholar at SMU jailed 16 weeks for hacking into professor's computer and changing grades" (The Straits Times, 8 November 2017), where changes were made by the accused person to give himself better grades.

(a) Ncode's business includes processing of minors' personal data. It is therefore imperative that reasonable security arrangements ought to have been in place to protect the personal data of minors; and

(b) Ncode should have easily detected and rectified the well-known SQL injection vulnerability that existed in its basic form.

23 The Commissioner also took into account the following mitigating factors:

(a) Ncode cooperated fully with the investigations; and

(b) There was no evidence of mass exfiltration of personal data as a result of the Incident or the Unauthorised Logins.

24 Having considered all the relevant factors of this case, the Commissioner hereby directs Ncode to pay a financial penalty of S$30,000.00 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[9] in respect of judgment debts, shall accrue and be payable on the outstanding amount of the financial penalty until the financial penalty is paid in full.

Representations made by the Organisation

25 The Organisation in its letter to the Commission dated 19 December 2018 stated that while they concurred with the facts and findings set out in this Decision, they had requested for a reduction of the financial penalty quantum.

[9] Cap 322, R5, 2014 Rev Ed.

They made this request on the basis that they had cooperated fully with investigations as well as took prompt action to remediate the breach.

26 The Commissioner had already taken into consideration the above points in coming to its decision on the financial penalty.

27 The Organisation had also referred to the financial penalties imposed on other organisations. However, the facts in the decisions referred to by the Organisation were not identical to the facts in this case.

28 In particular, the Organisation cited 3 cases in which the organisations that were in breach of their obligations under the PDPA were imposed a financial penalty that was less than that imposed on the Organisation. The cases cited by the Organisation was *Re ComGateway (S) Pte Ltd* [2017] SGPDPC 19, *Re WTS Automotive Services Pte. Ltd.* [2018] SGPDPC 26 and *Re Propnex Realty Pte Ltd* [2017] SGPDPC 1. However, the major difference between these 3 cited cases and the current matter is that this matter, unlike the cases cited by the Organisation, included the personal data of minors. Organisations ought to protect the personal data of minors to a higher standard and the unauthorised access or disclosure of personal data of minors is an aggravating factor when the quantum of financial penalty to be imposed is determined.

29 The Commissioner is, therefore, of the view that the financial penalty imposed in this case is justified, in particular given the aggravating factors set out above at paragraph 22.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION