DS Human Resource Pte. Ltd.

[2019] SGPDPC 16

Tan Kiat How, Commissioner — Case No DP-1802-B1756

Data protection – Openness obligation – Lack of data protection policies and practices

Data protection – Protection obligation – Unauthorised access to, and deletion of, personal data – Insufficient security arrangements

13 June 2019.

Background

1 Open source software is increasing in popularity and prevalence. This case illustrates the risks to companies in using default settings of open source software without any assessment of the security features. On 25 February 2018, DS Human Resource Pte. Ltd. ("**DSHR**") informed the Personal Data Protection Commission (the "**Commission**") of a data breach involving unauthorised access and deletion of its database by a hacker. Following an investigation into the matter, the Commissioner found DSHR in breach of sections 12 and 24 of Personal Data Protection Act 2012 ("**PDPA**").

Material Facts

2 DSHR specialises in the outsourcing of part-time staff to the food and beverage industry in Singapore. Individuals interested in applying for a part-

time job would enter their personal data into DSHR's mobile application. The personal data collected by DSHR's mobile application was stored on MongoDB database, an open source database software used by DSHR since April 2017 ("**Database**").

3 The Database is hosted on Amazon Web Services ("**AWS**") server. The source code used by DSHR to perform specific functions on the Database was stored in Github, an online code repository. The administration of DSHR's Database was handled mainly by DSHR's director. At the material time, the Database stored personal data of approximately 2,100 individuals, including:

(a) Name;

(b) NRIC Number;

(c) Date of Birth;

(d) Gender;

(e) Emergency Contact;

(f) Bank Account Details;

(g) Work Experience;

(h) Educational Qualification; and

(i) Image of front and back of NRIC.

(collectively, "**DSHR's Data**")

4 On 24 February 2018, DSHR discovered unauthorised access to the Database and deletion of DSHR's Data. The hacker demanded payment of 0.25

bitcoins in exchange for restoring the Database. Notwithstanding DSHR's payment on the same day, the hacker did not restore the Database (collectively, the "**Incident**"). DSHR did not have a backup and was unable to recover the deleted DSHR's Data.

5 DSHR took the following remedial actions after the Incident:

(a) Changed all of the passwords of its AWS account;

(b) Restricted connections to DSHR's AWS server to DSHR's IP addresses only;

(c) Disabled remote access to the MongoDB server software;

(d) Engaged consultants to perform vulnerability and penetration testing, and remedied the issues found in the tests, such as an issue concerning session management;

(e) Installed HTTPS at www.dshradmin.com;

(f) Changed the username of it AWS account; and

(g) Notified all affected individuals via SMS.

The Commissioner's Findings and Basis for Determination

6 It is not disputed that the DSHR's Data is "personal data" as defined in section 2(1) of the PDPA. There is also no dispute that the PDPA applies to DSHR as it falls within PDPA's definition of "organisation".

7 The issues to be determined by the Commissioner in this case are as follows:

(a) Whether DSHR had complied with its obligations under Section 24 of the PDPA; and

(b) Whether DSHR had complied with its obligations under Section 12 of the PDPA.

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

8 Section 24 of the PDPA provides that an organisation shall 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. It is not disputed that DSHR had possession and control of DSHR's Data stored in the Database, and hosted on the AWS Server.

9 The investigations found that DSHR failed to put in place reasonable security arrangements to protect the DSHR's Data for the following reasons:

(a) The default settings of the MongoDB open source database software allowed remote connections through the internet. By using the default settings, DSHR's Data stored on the Database was exposed. DSHR used the default settings without any assessment of whether this was a reasonable security arrangement to protect DSHR's Data stored on the Database. In this regard, DSHR admitted that it focused on the installation and functional use of the MongoDB database software rather than its security.

(b) There was readily available information and documents on security of the MongoDB software (e.g. steps to take to enable access control and limit network exposure). This included MongoDB's blog

post on 6 January 2017 referring to a Security Manual and Checklist which DSHR should have referred to when installing the MongoDB software in April 2017. DSHR failed to do so. As highlighted in the Commission's Guide to Securing Personal Data in Electronic Medium, organisations need to put in place adequate protection for databases that contain personal data, and consider their security requirements when selecting a database product.[1]

(c) DSHR's Data included bank account details which is personal data of a sensitive nature.[2] As highlighted in *Re Credit Counselling Singapore* [2017] SGPDPC 18 at [25], when it comes to the protection of sensitive personal data, there is a need to put in place stronger security measures because of the actual or potential harm, and the severity of such harm, that may befall an individual from a misuse or unauthorised use of such data. In the circumstances, it was completely inexcusable for DSHR to use the default settings in the MongoDB open source database software without addressing its mind to the questions whether remote access to DSHR's Data was necessary and, if not, ensuring that the remote access functionality of MongoDB was disabled.

(d) More fundamentally, MongoDB did not have an administrator password by default. It is necessary for all organisations making use of IT solutions to secure the administrator account by changing its default password to something unique and not easily guessable.

---

[1] PDPC, *Guide to Securing Personal Data in Electronic Medium* at [13.1]-[13.2].

[2] *Re AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [19].

(e) The Commissioner finds that DSHR failed to put in place any security or access controls to the Database (e.g. through password protection), resulting in DSHR's Data being exposed to the Internet. This case is analogous to the case *Re Propnex Realty Pte Ltd* [2017] SGPDPC 1, where it was found that the organisation failed to properly protect personal data as it did not have any security controls or restrictions (i.e. proper authentication system) to prevent access from the Internet over the webpages that were stored on the server.

10 The investigations also revealed that DSHR had inadequate patch management processes. At the material time, notwithstanding GitHub had published documentation on its website advising periodic manual review by users, DSHR relied completely on GitHub for MongoDB patch alerts. GitHub is a portal for collaborative storage and management of source code in the developer community. Its features include providing security alerts of common vulnerabilities. However, it is not a complete substitute for monitoring IT security portals (eg Common Vulnerabilities and Exposures system, or CVE) and the security and patch information feed direct from the software solution provider (ie MongoDB). DSHR ought to have actively monitored for new patches released for software components and from the correct sources. Cyber attackers are well aware of vulnerabilities available for exploiting. It is important for organisations to keep their software updated or patched regularly to minimise their vulnerabilities.[3]

Whether DSHR complied with its obligations under section 12 of the PDPA

[3] PDPC, *Guide to Securing Personal Data in Electronic Medium* at [16.3]-[16.4].

11 DSHR admitted that it did not have any policies or internal guidelines which specify the rules and procedures on the collection, use and disclosure of personal data. DSHR's omission to do so and consequential failure to communicate such policies and internal guidelines to its employees amounts to a breach of section 12 of the PDPA.

Representations by DSHR

12 In the course of settling this decision, DHSR made representations on the amount of financial penalty which the Commissioner intended to impose, while agreeing with the Commissioner's findings and basis of determination set out above.

13 In its representations on the amount of financial penalty, DSHR requested that the Commissioner consider the following factors:

(a) DSHR asserted that the Incident arose due to its director's negligence but hopes that the director's lack of technical knowledge may be taken into account;

(b) The popularity of MongoDB database software and the fact that it was used by many big companies worldwide led DSHR's director to believe that the database would have reasonable security reliability; and

(c) DSHR's determination to proceed with automation of its business processes notwithstanding difficulties faced, including hiring a full time developer moving forward;

14 Having considered representations, the Commissioner acknowledges DSHR's determination to automate its business processes and its director's initiative to do so in response to the Government's push for small and medium

enterprises ("**SMEs**") go digital, particularly when difficulties in hiring technically skilled staff would have discouraged others. The Commissioner would like to take this opportunity to highlight that good data management and protection practices need to be adopted from the onset of the digitalisation process, and these can be proportionate without being too costly. SMEs are urged to tap on available Government funding and support programmes to assist SMEs in their digitalisation efforts.

15 The Commissioner has decided to maintain the financial penalty set out in paragraph 19 for the following reasons:

(a) An organisation's lack of technical knowledge cannot be a mitigating factor. As explained in *WTS Automotive Services Pte Ltd* [2018] SGPDPC 26 at [24], the responsibilities of ownership do not require technical expertise. In this regard, if an organisation does not have the requisite level of technical expertise to manage its IT system, the organisation may either procure technical expertise internally (e.g. by training its existing employees or hiring individuals with relevant expertise) or engage competent service providers and give proper instructions; and

(b) The security features or reliability of the MongoDB database software were not the issue. It was DSHR's failure to ensure that the appropriate security settings were configured to protect DSHR's Data. This is therefore not a mitigating factor.

The Commissioner's Directions

16 Given the Commissioner's findings that DSHR is in breach of sections 12 and 24 of the PDPA, the Commissioner is empowered under section 29 of

the PDPA to issue DSHR such directions as it deems fit to ensure compliance with the PDPA. This may include directing DSHR to pay a financial penalty of such amount not exceeding $1 million.

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

(a) There was actual loss of DSHR's Data as the hacker managed to access and delete the entire Database;

(b) There was also the risk of DSHR's Data being misused (e.g. the front and back image of affected individuals' NRIC could be used to commit identity theft); and

(c) DSHR's failure to password protect the Database was a serious lapse of a basic and integral IT security arrangement.

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

(a) DSHR implemented reasonable corrective measures to address the technical flaws that resulted in the Incident. DSHR also notified all affected individuals via SMS; and

(b) DSHR cooperated with the investigations.

19 Having considered all the relevant factors of this case, the Commissioner hereby directs DSHR to pay a financial penalty of $33,000.00 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[4] 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.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION

---

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