PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 30

Case No DP-1806-B2237

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

And

Executive Link Services Pte. Ltd.

…Organisation(s)

DECISION

Executive Link Services Pte. Ltd.

[2019] SGPDPC 30

Mr Yeong Zee Kin, Deputy Commissioner – Case No DP-1806-B2237

23 August 2019

Background

1. On 11 June 2018, Executive Link Services Pte. Ltd. (the "**Organisation**") reported a data breach to the Personal Data Protection Commission (the "**Commission**") concerning the unintended disclosure of personal data of individuals that were stored on the Organisation's server ("**Incident**"). The Commission investigated the Incident and determined that the Organisation had breached its obligations under the Personal Data Protection Act 2012 ("**PDPA**").

Material facts

2. The Organisation is an employment agency. Sometime before 8 June 2018, one of the Organisation's clients engaged a cybersecurity company to scan the Internet for information relating to the client. During this scan, the cybersecurity company was able to gain access and retrieve copies of draft contracts of job candidates from the Organisation's server. The Organisation was alerted on 8 June 2018. In total, resumes of 367 individuals (the "**Affected Individuals**") and around 150 draft contracts relating to some of those individuals, together with the personal data therein (the "**Compromised Personal Data**"), were exposed to unauthorised disclosure in this manner.

3. The Compromised Personal Data included the following:

(a) the individual's name, address, contact number, email address(es), education level, salary expectation and employment history (in relation to the resumes); and

(b) the individual's name, address and salary information (in relation to the draft contracts).

Events leading to the Incident

4. The Organisation had implemented remote access for staff to access internal files stored on its data storage server. This required the use of a Virtual Private Network ("**VPN**") service. The server was supplied by Blumm Technology Pte. Ltd. ("**Blumm**") and installed and set up by the Organisation's information technology ("**IT**") vendor, SShang Systems ("**SShang**"). SShang provided IT support services to the Organisation, eg upgrading and configuration of hardware, and general IT troubleshooting. When staff had difficulties with VPN access, the Organisation approached SShang for assistance. SShang was, in turn, advised by Blumm to adopt a workaround, by opening and enabling file access through the server's file transport protocol ("**FTP**") port (the "**VPN Workaround**"). Blumm also advised SShang to password-protect the folders within the server after the FTP port was opened.

5. When SShang implemented the VPN Workaround, it did not advise the Organisation about password-protecting the folders on the server because it assessed that there was little or no risk of unauthorised access to the folders since remote access was limited to staff. Although the Organisation had only intended to test the VPN Workaround for a few days, it was during this period that its client discovered the Compromised Personal Data on its server.

6. In the course of the Commission's investigation, the Organisation also admitted that it had not appointed a DPO and that it did not have any policies, internal guidelines or procedures on the collection, use and disclosure of personal data and other matters required under the PDPA.

Findings and Basis for Determination

Issues for determination

7. Based on the facts of the case, the issues to be determined are as follows:

(a) Whether the Organisation had complied with its obligation to protect personal data under section 24 of the PDPA; and

(b) Whether the Organisation had complied with the obligations to appoint a data protection officer ("**DPO**") and develop and implement data protection policies and practices under sections 11(3) and 12 respectively of the PDPA;

Whether the Organisation complied with its obligation under section 24 of the PDPA

8. At all material times, the Compromised Personal Data was in the Organisation's sole possession and control. SShang was engaged to provide IT support services but was not engaged to process personal data. Blumm supplied the server and had assisted to open the server's FTP port to enable the VPN Workaround, but it was not engaged to process personal data. Hence, both SShang and Blumm were not data intermediaries. Hence, the responsibility to protect the Compromised Personal Data fell squarely and solely on the Organisation.

9. The question is whether the Organisation had failed to take reasonable steps to protect the Compromised Personal Data. It should be noted from the outset that this was not a case involving a server hosting a website that was meant to be accessible on the World Wide Web. It was an internal server that was meant to be accessed by staff remotely through the Internet. There are subtle but significant differences between the two. A website on the World Wide Web is by its nature intended to be more easily linked from other websites, and to be discovered by search engines and directories. Remote access to a server via the Internet requires the member of staff to use VPN software or know the precise Internet Protocol ("**IP**") address. It is not usually crawled by online search engines. But that is not to say that it cannot be discovered. It can be, by using the right tool to scan a known set of IP address range, as was done in this case by the cybersecurity company. The footprint is smaller and the risk is lower, but that does not in any way mean that the risk does not exist.

10. The Organisation did not have requisite IT knowledge and depended on its outsourced IT support services provider. Its duties as owner of the server and controller of the Compromised Personal Data include making its requirements known to SShang and asking the right questions from the perspective of a business owner. It can rely on SShang's technical know-how. In this case, the Organisation was aware of the risks and had implemented VPN access for its staff. When there were difficulties with the VPN access and SShang was called upon to troubleshoot, it was a natural and reasonable expectation that any workaround recommended would not materially compromise its requirement for security. It is not unreasonable for the Organisation to have expected that any such material deviation– particularly when the security level is lowered – would be drawn to its attention.

11. Of course, the Organisation could have asked about the security of VPN Workaround. But is it reasonable to expect this level of pedantry? I am mindful that when troubleshooting IT issues, there is a degree of urgency and need for speed to implement workarounds, identify root causes and implement permanent solutions.

In these circumstances, the operating assumption should be that existing business rules continue to be relevant. However, I am of the view that since the VPN Workaround touched on secured remote access, the Organisation could have sought clarification of the impact of the VPN Workaround on its requirements for security.

12. In this case, SShang had been advised by Blumm to enable password protection. SShang had assessed that there was no need to do so as remote access was limited to staff and there was little or no risk of unauthorised access to the folders. We do not know what SShang would have informed the Organisation had the Organisation sought clarification. However, even if SShang shared its assessment and maintained its advice that it was not necessary to enable password protection, the Organisation would not have known better and would have relied on the advice. In light of these circumstances, I am giving the Organisation the benefit of doubt and will not make a finding of breach of its protection obligation under section 24 of the PDPA.

Whether the Organisation complied with its obligations under sections 11(3) and 12 of the PDPA

13. The remaining two issues are straightforward. Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA. This individual is typically referred to as the DPO. Further, section 12 of the PDPA requires organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, and to communicate information about such policies and practices to its employees (among other obligations). The importance of these requirements have been emphasized multiple times in previous decisions.[1]

[1] See *Re Aviva Ltd* [2017] SGPDPC 14 at [32]; *Re M Stars Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 at [31] to [37]; *Re Singapore Taekwondo Federation* [2018] SGPDPC 17 at [39] to [42]; *Re AgcDesign Pte Ltd* [2019] SGPDPC 23 at [4] to [5].

14. In view of the Organisation's admissions that it had not appointed a DPO and had not developed and implemented any policies, internal guidelines or procedures on the collection, use and disclosure of personal data, I find the Organisation in breach of sections 11(3) and 12 of the PDPA.

Remedial Actions by the Organisation

15. After being informed of the Incident by its client, the Organisation closed the FTP port on the same day. The Organisation also took the following additional steps:

a. Shut down the server permanently and replaced it with a new server;

b. Installed a firewall for the new server and implemented access to the new server via VPN, which requires the use of passwords (thereby limiting access to the data stored on the server);

c. Implemented password policies for its employees for the use of the VPN;

d. Engaged a cyber-security firm to conduct a network vulnerability assessment on its new server, which found no vulnerabilities;

e. Appointed a data protection officer;

f. Drafted and implemented policies on the handling of personal data; and

g. Provided data protection training for its employees.

The Deputy Commissioner's Directions

16. In assessing the breach, I took into account the following mitigating factors:

a. The Organisation was cooperative with the Commission during its investigation and was prompt and forthcoming in its responses to queries posed by the Commission;

b. The Organisation took swift and extensive remedial action following the Incident;

c. The duration that the Compromised Personal Data was at risk was only for a limited time period. The Organisation was alerted to the Incident only a few days after the FTP port was opened to enable the VPN Workaround, and the Organisation took swift action thereafter to remove such access; and

d. The VPN Workaround was only intended to be a temporary measure, and the Organisation had intended to revert back to the use of the VPN. Thus, the potential for unauthorised disclosure of the Compromised Personal data would have been limited in any event.

17. Having considered the facts of this case and the factors outlined above, I hereby direct the Organisation to pay a financial penalty of $5,000 within 30 days from the date of this direction, failing which interest at the rate specified in the Rules of Court[2] 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

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