SearchAsia Consulting Pte. Ltd.

[2019] SGPDPC 40

Yeong Zee Kin, Deputy Commissioner — Case No DP-1809-B2790

Data Protection – Protection obligation – Unauthorised access to personal data – Insufficient security arrangements

24 October 2019

Introduction and Material Facts

1. SearchAsia Consulting Pte. Ltd. (the "**Organisation**") is a recruitment company established in Singapore which matches job seekers with organisations that are looking to recruit employees for a specific role. On 26 September 2018, the Organisation notified the Personal Data Protection Commission (the "**Commission**") of a data breach incident involving the inadvertent disclosure of résumés (the "**Incident**") which were uploaded by individual job seekers to the Organisation's website, www.searchasia.com.sg (the "**Website**"). Specifically, when a search was conducted on the names or email addresses of affected individuals using an Internet search engine, the search results would include links to the affected individuals' résumés which had been uploaded to the Website. These résumés were accessible by clicking on the listed links.

2. The Organisation provided job seekers with the ability to upload their résumés on the Website so that the Organisation could assess their suitability for roles which the Organisation has been engaged to fill. The résumés would generally include personal data such as the name, phone numbers, employment history, educational qualifications, achievements and skillset of the job seekers. In one instance, it was discovered that a job seeker included additional information such as nationality, date of birth, marital status and current salary. (The personal data on the affected individuals' résumés is collectively referred to as the "**Personal Data**".)

3. The résumés uploaded to the Website were intended to only be accessible by recruitment agents employed by the Organisation. However, in practice résumés which were uploaded to the Website were stored in a folder ("**the Folder**") on the Website's server which was not secured by access controls. As a result, these résumés were indexed by bot crawlers and could be found and accessed by the general public when a search was done via an Internet search engine.

4. The Organisation asserted to the Commission that it had instructed its third party web developer (the "**Developer**") to restrict access to the Folder to only 1 of the Organisation's employees. However, the Organisation did not provide the Commission with any documentary evidence supporting its assertion and the Developer, in its statement to the Commission, denied receiving any specifications on security from the Organisation. Further, the Organisation had not conducted any checks or tests to ensure that access to the Folder was restricted or that the data in the Folder was encrypted. The Organisation admitted that the Developer had not processed any personal data on its behalf.

5. In its representations to the Commission, the Organisation stated that it had asked the Developer whether the résumés uploaded to the Website would be encrypted and the Developer responded saying that "it was safe". This does not detract from the fact that the Organisation did not set out its instructions to the developer in writing. As stated in *Re WTS Automotive Services Pte Ltd* [2018] SGPDPC 26 (at [17]), when engaging a service provider, it is important for the organisation to clarify their obligations and thereafter documenting them in writing prior to the provision of services. As set out in *Re Smiling Orchid (S) Pte Ltd and others* [2016] SGPDPC 19 at [51]:

> *"[t]here must be a clear meeting of minds as to the services that the service provider has agreed to undertake, and this should be properly documented. Data controllers should follow through with the procedures to check that the outsourced provider is indeed delivering the services."*

6. Further, the Organisation's failure to conduct any checks on whether or not access controls were put in place was in itself a breach of its protection obligations: see *Re Tutor City* [2019] SGPDPC 5 at [16].

7. The Organisation also asserted that it had relied on its web hosting and technical support services provider ("**Web Host**"), to ensure that the Website had adequate security features. However, the Organisation had not informed the Web Host that the contents of the Folder were meant to be protected. Hence, while the Web Host had performed some security reviews on the Website, they had not been engaged to advise on or implement measures to protect the personal data stored in the Folder.

8. After being informed of the Incident, the Organisation undertook the following remedial actions:

a. The Organisation requested the Web Host to assist in disabling the directory listing function of the Website;

b. The Organisation also engaged an external web developer to add a mechanism to the Website to help prevent future indexing by search engine crawlers;

c. Public access permissions were removed from sensitive file directories to avoid similar incidents from reoccurring; and

d. The Organisation requested Google to remove the existing cached copies of the affected individuals' résumés from its search engine results.

Findings and Basis for Determination

9. Section 24 of the Personal Data Protection Act 2012 ("**PDPA**") requires organisations to make reasonable security arrangements to protect personal data in its possession or under its control from unauthorised access, disclosure and similar risks. While the Organisation had outsourced the hosting of the Website to the Web Host, it remained in control of the Personal Data. Accordingly, the Organisation was responsible for making reasonable security arrangements to protect the Personal Data.

10. The facts of this case, as set out above, clearly show the Organisation's failure to make reasonable security arrangements to protect the Personal Data The cause of the Incident was that the Folder was set to allow access to documents within the folder to the public without

restrictions and the Organisation had not given the appropriate instructions to its contractors, including the Developer and the Web Host, to protect the Personal Data in the Folder.

11. As has been set out in numerous previous decisions issued by the PDPC (see for example *Re Tutor City*), one of the fundamental actions an organisation is required to undertake towards fulfilling its obligation to make reasonable security arrangements to protect personal data in its possession or under its control is to conduct relevant tests of their IT environment, including websites, to ensure that personal data has been adequately protected.

12. In the circumstances, I find the Organisation in breach of section 24 of the PDPA.

Outcome

13. Having found the Organisation in breach of section 24, I have decided to direct the Organisation to pay a financial penalty of $7,000 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. Given the Organisation's remediation actions as set out above at paragraph 8, I have decided not to issue any other directions.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION