PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 5

Case No DP-1806-B2228

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

And

Tutor City

… *Organisation*

DECISION

Tutor City

[2019] SGPDPC 5

Yeong Zee Kin, Deputy Commissioner — Case No DP-1806-B2228

23 April 2019

Background

1 As more organisations conduct business over the Internet, the volume and sensitivity of personal data collected online likewise increases. This case shows that when collecting documents containing personal data via a website, organisations should have in place reasonable security arrangements in the form of access controls to prevent unauthorised access to these documents to third parties. In particular, organisations should ensure that these documents are not unwittingly saved in folders that are accessible by the public.

2 On 8 June 2018, the Personal Data Protection Commission (the "**Commission**") received a complaint from an individual (the "**Complainant**") in relation to the publication of personal data belonging to 50 individuals on the Organisation's website, www.tutorcity.com.sg (the "**Website**"). Specifically, images of the educational certificates of tutors using the Website were found to be publicly accessible by Internet users (the "**Incident**").

3 Following an investigation into the matter, I found the Organisation in breach of section 24 of Personal Data Protection Act 2012 ("**PDPA**"). I set out below my findings and grounds of decision based on the investigations carried out in this matter.

Material Facts

The Website

4 The Organisation is registered and managed by its sole proprietor (the "**Sole Proprietor**"). Through the Website, the Organisation provides matching services between

freelance tutors and its prospective clients (*e.g.* parents of students).

5 The Website lists freelance tutors and provides access to information about their educational qualifications, past experience and contact details. Freelance tutors agree to make such of their information publicly available and searchable on the Website when they sign on for the service. The Website also provides an interested student or her parent to request for additional educational details from a tutor that they have identified. In order to provide this feature, tutors could upload their educational certificates onto the Website. The intention was for the tutor to approve each request to view their educational certificates, and by dint of this workflow, there was no intention to make the educational certificates publicly available or searchable outside the Website. The optional nature of this feature explains the low number of tutors who were affected, *viz* 50 tutors out of a total of 13,283 tutors registered on the Website.

6 The Organisation had instructed a freelance web developer to design and develop the Website. Upon its completion in 2011, the Website was handed over to the Organisation and uploaded to a hosting server. It is admitted by the Sole Proprietor that:

(a) the Organisation has been the sole party in charge of the Website after the handover;

(b) the developer did not process any personal data on the Organisation's behalf for the development of the Website; and

(c) the developer did not have any further involvement in the Website after it was handed over to the Organisation.

The Incident

7 As part of the Website's features, tutors interested in using the Organisation's matching service are given the option of voluntarily uploading up to three different educational certificates onto the Website. These certificates assisted the Organisation in matching the needs of the student in question to suitable tutors. These certificates were not intended to be made publicly accessible.

8 Notwithstanding this, all uploaded certificates were stored in the /Public_html/directory

(the "**Public Directory**") of the Website's server within a sub-folder, Public_html\tutor\tutor_image (the "**Image Directory**"). Both directories were not secured with any form of access controls and were accessible by the public so long as the path to the relevant directory was known.

9 Investigations also revealed that the certificates were indexed by search engines like Google due to the lack of any measures taken to prevent automatic indexing of the Image Directory by web crawlers. This resulted in them showing up as search results on Google.

10 The Incident resulted in the disclosure of the following types of personal data of 50 individual tutors:

(a) name of the individual;

(b) NRIC number;

(c) educational institution the individual attended; and

(d) the grades the individual attained for each subject.

11 After being notified of the Incident, the Organisation took the following steps to prevent its reoccurrence:

(a) it added a .htaccess file to the Image Directory that would restrict access to only the administrator; and

(b) it deleted all the images stored in the Image Directory as of 8 June 2018.

Findings and Basis for Determination

12 The issue for determination is whether the Organisation breached section 24 of the PDPA. Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

13 As a preliminary point, I note that the Organisation, being the sole administrator of the Website, retained full possession and control over the personal data that the Website collected at all material times. Although a developer was previously engaged for website development, the Sole Proprietor admitted that the developer did not process any personal data on behalf of the Organisation. Accordingly, the developer was not a data intermediary and the Organisation retained full responsibility for the IT security of the Website as well as the personal data contained therein.

14 Notwithstanding that the Organisation retained full responsibility over the Website's security, other than instructing the developer to "*make it safe*", the Organisation had paid little to no attention to the security of the Website. In this regard, the Sole Proprietor had provided the following statement:

> From year 2011 to current, I did not implement any additional security measures to the website or its web directories as I am not tech-savvy and the current website had fulfilled my business needs. Therefore, even though the Personal Data Protection Act took effect in year 2014, I did not review my website to see if its security settings and measures are sufficient to protect the personal data of the tutors that had registered in my website. I did not think there was a need to review my website as I thought that Tutor City is a small business and no one would hack my website.
>
> As for the security measures for the web directory, I do not have the knowledge of the exact settings or measures taken as I had pointed out earlier that I am not tech-savvy. When I commission the web developer to design the website, I gave him the business requirements and just told him to make it safe. I did not question on what sort of technical measures were to be used for the website. Before the website was uploaded to the hosting server, I did some testing on whether the features of the website were working correctly as intended but the testing was from a functionality angle and not to examine the security of the website. I wish to state that I am not aware of how the folders in the web directory are protected.

15 While the Website was developed and handed over to the Organisation before the PDPA came into force on 2 July 2014 (the "**Appointed Day**"), the Organisation continued to use the Website to collect personal data after the Appointed Day. As such, it was incumbent on the Organisation to take proactive steps to comply with its obligations under the PDPA. The following passage in *Re Social Metric Pte Ltd* [2017] SGPDPC 17 (at [11]) is instructive:

> This means that, for example, if there were no security arrangements previously to protect the existing personal data the organisation was holding, the

> organisation has a positive duty to put in place security arrangements after the Appointed Day. It was not enough for the organisation to leave things *status quo*, if this would not enable the organisation to meet the requirements and standards of the Protection Obligation. As provided in Section 24 of the PDPA, the security arrangements must be "reasonable".

16 In this regard, as can be seen from paragraph 14 above, no steps were taken after the Appointed Day by the Organisation or the Sole Proprietor to review the standard of security of the Website. The facts demonstrate that, prior to the Incident, the Organisation did not attempt to equip itself with knowledge of its data protection obligations under the PDPA. As mentioned above, the Organisation showed a lack of knowledge of the security arrangements over its Website. It did not:

(a) communicate any specific security requirements to its developer to protect the personal data stored on the Website's server, including instructing the developer to ensure that the uploaded certificates would not be accessible to the public;

(b) make reasonable effort to find out and understand the security measures implemented by its developer for the Website;

(c) attempt to verify that security measures to "*make [the Website] safe*" were indeed implemented by its developer; and

(d) conduct any reasonable security testing (*e.g.* penetration tests).

These demonstrate a fundamental lack of care by the Organisation over the personal data in its possession and/or under its control.

17 Related to the above, I note that the Sole Proprietor's vague comment to its developer to make the Website safe does not constitute a security measure. The Organisation could not have reasonably expected its developer to implement security measures that were adequate for the Organisation's purposes merely based on the Sole Proprietor's vague comment. The developer would not have known that the Organisation intended to protect the tutors' certificates from public access without the Organisation specifying this requirement.

18 While this palpable lack of detail may have been the norm before the Appointed Date, this is surely not the standard after the Appointed Date. The standard that is expected from organisations contracting professional services to build their corporate websites or other online

portal is articulated in the *Guide to Building Websites for SMEs*. The Organisation ought to have reviewed the standard of security that had been implemented on the Website after the Appointed Date. In doing so, it should have delved into some degree of detail by providing its developer the intended use cases and identifying risks and abuse that it can foresee. These do not require deep technical knowledge but do require that the Organisation has an understanding of how the Website will be used by itself and its customers. Had it reviewed the security standard implemented on the Website, it would have realised that all the certificates provided by the tutors were accessible publicly, when this was not the intention. The Sole Proprietor's claim that he lacked IT knowledge or tech-savviness is also not a defence against the Organisation's failure to take any steps to comply with the Protection Obligation.

19 As observed in the *Guide to Building Websites for SMEs* at [5.5] to [5.6]:

> **5.5 Security Configuration Management**
>
> 5.5.1 ***Organisations should ensure, or require their vendor(s) to ensure, that the software and hardware components of the organisation's website are properly configured to prevent unauthorised access.*** This includes reviewing operating systems, checking if appropriate antivirus/anti-malware software are in place and setting firewall rules to only allow authorised traffic. The configuration of each component should also be fully documented, kept up to date, and reviewed regularly.
>
> 5.5.2 ***There should also be a plan for testing and applying patches and updates for the website's software and hardware components.*** This includes having a process and person responsible to monitor new patches and updates that become available.
>
> **5.6 Security Testing**
>
> 5.6.1 ***Testing the website for security vulnerabilities is an important aspect of ensuring the security of the website. Penetration testing or vulnerability assessments should be conducted prior to making the website accessible to the public, as well as on a periodical basis (e.g. annually).*** Any discovered vulnerabilities should be reviewed and promptly fixed to prevent data breaches.
>
> 5.6.2 Where organisations have outsourced the development of its website, they should require the IT vendor(s) to conduct the above security testing. As a baseline, organisations may wish to consider using the Open Web Application Security Project (OWASP) Testing Guide and the OWASP Application Security Verification Standard (ASVS) to verify that security requirements for the website have been met.
>
> [Emphasis added.]

20 The same guide goes on to add, amongst others, at [6.2.1], that:

> Access control is a critical part of the website's security arrangements. An effective access control scheme should be designed such that:
>
> - Only authorised users (usually staff of the organisation) are allowed to access the website's administrative functions and personal data handled by the website…
> - All users should only be able to see the website functions and data that they are allowed to access…

21 In the present case, I am advised that where documents containing personal data have to reside on web servers, folder or directory permissions and access controls are a common and direct way of preventing their unauthorised access by public users and web crawlers. Depending on its circumstances, the Organisation could therefore have implemented any of the following reasonable technical security measures to prevent its Image Directory from being indexed by web crawlers:

(a) First, the Organisation could have placed these documents in a folder of a non-public folder/directory. Access to such documents will then be controlled by the server's administrator. While this may not be ideal in complex servers with multiple web applications — given that it may not be practicable for the server administrator to control access to all these files — this is not the case for the present Website.

(b) Second, the Organisation could have placed these documents in a folder of a non-public folder or directory, with access to these documents being through web applications on the server. This could be done through PHP scripts. To access the data in the documents, users would have to first log into the web application.

(c) Third, the Organisation could have placed these documents in a sub-folder within the Public Directory but control access to files by creating a .htaccess file within that sub-folder. This .htaccess file may specify the access restrictions (*e.g.* implement a password requirement or an IP address restriction). An index.html file could also be created within that sub-folder to show a HTML page with no content or a denial of access message. Any unauthorised user would then need the specific URL to access a document in the sub-folder. However, given that the Public Directory is the web root directory containing all the content to be displayed on the Website, it should not have overly restrictive access rights. This may pose some challenges for organisations seeking to balance access restrictions to specific documents against retaining accessibility to website content that is intended to be public.

22 It is up to each organisation to determine which security arrangements are the most suitable for its purposes, taking into account factors such as sensitivity of the personal data, size of the database and operational realities. The above are merely three potential technical security measures that organisations may implement to protect personal data.

23 On an even more basic level, the Organisation could, and should, have done proper housekeeping to ensure that all its Website's publicly accessible folders did not contain files that are not meant to be publicly disclosed. Investigations disclosed that from the handover up till the occurrence of the Incident, the Organisation did not carry out any further updates or develop new security features for the Website. Although this did not contribute, in this case, to the Incident, it is nevertheless a separate breach of the Protection Obligation. I cannot emphasise enough the importance of putting in place maintenance processes to ensure regular security patching as a security measure; regular archival of old data will also reduce the size of any breach that may arise and is therefore also an important aspect of the Protection Obligation. Data protection threats are constantly evolving and patching is one of the common tasks that all IT system owners are required to perform in order to keep their security measures current against external threats.[1]

24 Besides the above, I note that the Organisation had taken the view that the security of the Website did not need to be reviewed because the Sole Proprietor did not think that it would be hacked. I would like to make it clear that the low likelihood of being hacked is not an acceptable reason for the failure to comply with the Protection Obligation. An organisation is required to put in place security arrangements to protect personal data in its possession or

[1] See also *Re Orchard Turn Developments Pte. Ltd.* [2017] SGPDPC 12 and *Re Cellar Door Pte Ltd* [2016] SGPDPC 22.

control whether or not they believe that there is a likelihood of being hacked on the basis that they are small organisations.

25 It is erroneous to think that the cyber security risk exposure of a business is commensurate with its business size. According to the *Singapore Cyber Landscape 2017* issued by the Cyber Security Agency of Singapore, almost 40% of the cyberattacks reported to SingCERT in 2017 targeted small medium enterprises ("**SMEs**").[2] A more recent study released in January 2019 by Chubb and YouGov has revealed that many SMEs in Singapore underestimate their exposure to cyber risks, and the existence of "*a significant gap between the hard reality of cyber risk and how well small companies are prepared to deal with it*".[3]. Crucially, the same study observes that:

> ... ***it is becoming increasingly likely that if an SME has a security weakness, it will be targeted sooner rather than later***. This is why, for cyber criminals, these businesses are the proverbial "low-hanging fruit". Not only are they easy targets, they also offer a substantial cumulative payoff. In fact, ***SMEs, with their low or no investment in cyber security measures, are actually the ideal, and subsequently the most common target for online crimes.***
>
> [Emphasis added.]

26 In the same vein, and as illustrated by the Incident as well as our previous decisions, data protection threats may not always come in the form of hacking incidents – the lack of access controls[4], which is something inherently within the Organisation's powers to implement, system design errors[5] and human error[6] can similarly lead to a personal data breach incident. Organisations should therefore not take the security of their website for granted simply because of the smaller scale of their businesses.

[2] https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecyberlandscape2017.pdf

[3] Out of the 300 SMEs in Singapore polled, 63% believed themselves to be less vulnerable than larger companies, yet 56% had experienced a cyber error or attack in the past 12 months; https://www.chubb.com/sg-en/_assets/documents/chubb-sg-sme-cyber-preparedness-report.pdf

[4] See, for example, *Re Dimsum Property Pte. Ltd.* [2018] SGPDPC 20 and *Re Singapore Management University Alumni Association* [2018] SGPDPC 6.

[5] See, for example, *Re COURTS (Singapore) Pte Ltd* [2019] SGPDPC 4, *Re Funding Societies Pte. Ltd.* [2018] SGPDPC 29 and *Re Jade E-Services Singapore Pte Ltd* [2018] SGPDPC 21.

[6] See, for example, *Re Aviva Ltd* [2018] SGPDPC 4, *Re SLF Green Maid Agency* [2018] SGPDPC 27 and *Re National University of Singapore* [2017] SGPDPC 5.

Conclusion

27 I find on the facts above that the Organisation did not make reasonable security arrangements to protect personal data in its possession or under its control against the risk of unauthorised access. The Organisation is therefore in breach of section 24 of the PDPA. I took into account the number of affected individuals, the type of personal data at risk of unauthorised access and the remedial action by the Organisation to prevent recurrence. I have decided to issue a warning to the Organisation for the breach of its obligation under section 24 of the PDPA as neither further directions nor a financial penalty is warranted in this case.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION