This decision is subject to final editorial corrections approved by the tribunal and/or redaction pursuant to the publisher's duty in compliance with the law, for publication in LawNet.

Advance Home Tutors

[2019] SGPDPC 35

Yeong Zee Kin, Deputy Commissioner — Case No DP-1806-B2218

Data protection – Protection obligation – Unauthorised disclosure of personal data – Insufficient security arrangements

Data protection – Protection obligation – Unauthorised disclosure of personal data – Lack of access controls

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

12 September 2019.

Facts of the case

1 On 7 June 2018, the Personal Data Protection Commission (the "**Commission**") received a complaint that personal data of many individuals had apparently been disclosed without authorisation on the Organisation's website, www.advancetutors.com.sg (the "**Website**"). Upon investigation, the Commission found the following facts leading to this apparent unauthorised disclosure of personal data.

2 The Organisation is a sole proprietor who provides "matching services" through the Website between freelance tutors and prospective clients seeking tuition services.

3 In January 2017, the Organisation engaged a freelance web developer based in the Philippines (the "**Developer**") to provide the following services:

(a) to design and develop the Website; and

(b) to migrate the existing databases and files of the Organisation's old website to the Website.

4 At that point in time, 834 freelance tutors had signed up with the Organisation and some of these tutors had chosen to upload their educational certificates to the Website's server (the "**Server**") via the Website. These certificates would be used by the Organisation to evaluate the suitability of the tutors for prospective jobs. In addition, copies of a tutor's certificates were to be disclosed on the tutor's public profile on the Website if the tutor consented to such disclosure. Out of the tutors who had uploaded educational certificates, a total of 152 tutors (the "**Affected Individuals**") had not consented to disclosure of their educational certificates on their public profile.

5 The Developer subsequently migrated the educational certificates of the tutors who had uploaded them to the Website and stored them in an image sub-directory of a public directory found on the Server (the "**Image Directory**"). These directories were not secured with any form of access controls and were accessible by the public via the Internet if the path to the relevant directory was typed into a web browser. Furthermore, no measures were taken to prevent automatic indexing of the Image Directory by Internet search engines. This resulted in the contents of the Image Directory, including the educational certificates of the Affected Individuals, showing up in search results on Google after the Website went live on 17 October 2017.

6 On 6 April 2018, the Organisation informed the Developer to make certain changes to the Website in order to disclose the education certificates of

consenting tutors on their public profile pages on the Website. The Organisation provided written instructions to the Developer to "*migrate all existing tutor profiles from the [old website] to the [Website]*", and to "*impose all pre-existing conditions in the [old website] to the [Website] when migrating the tutors*". According to the Organisation, one of the pre-existing conditions of the old website was to only disclose educational certificates of tutors who had consent. According to the Organisation, one of the pre-existing conditions of the old website was to only disclose educational certificates of tutors who had consent.

7 The Organisation also represented that it had provided the following verbal instructions to the Developer:

(a) to "*hide the educational certificates of tutors who did not give consent*";

(b) to "*respect and protect the privacy and confidentiality of all the data that is present in AHT website*";

(c) it "*should not disclose or share any of the personal data or AHT Admin user account details with a third party*"; and

(d) to "*ensure users' data is protected as AHT had entrusted them for the purpose of IT services*".

8 Acting on the Organisation's instructions, the Developer wrote a coding script to enable the retrieval and display of the educational certificates from the Image Directory. However, the coding script lacked a validation condition to ensure that only educational certificates of tutors who had consented to disclosure were disclosed on the tutors' profile pages on the Website. This resulted in all of the educational certificates found in the Image Directory, including those of the Affected Individuals, being retrieved and publicly disclosed on the Website through the tutors' respective profile pages.

9 The disclosure of the Affected Individuals’ educational certificates (described at [5] and [8] above) resulted in the unauthorised disclosure their personal data which were found on their respective educational certificates (the “**Incident**”). The disclosed personal data included data such as the individual’s name and NRIC number, educational institutions attended and grades attained for each subject (the “**Disclosed Data**”).

10 Separately, during the Commission’s investigations, the Organisation admitted that it had not developed or implemented any data protection policies relating to its compliance with the Personal Data Protection Act 2012 (the “**PDPA**”).

Remedial measures taken by the Organisation

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

(a) deleted all the educational certificates that were stored in the Image Directory;

(b) ceased retention of any educational certificates received from the tutors;

(c) requested Google to remove any cached copies of the educational certificates from the Image Directory;

(d) conducted a penetration test to discover and address any gaps in respect of its security arrangements in respect of the Website and its server;

(e) removed all front-end access to the “Search Tutor” and “Tutor Profile” pages of the Website;

(f) engaged an external system analyst to check the work which may be performed by the Developer in future; and

(g) developed a data protection policy.

Findings and Basis for Determination

Whether the Organisation had breached section 24 of the PDPA

12 Although the Organisation had engaged the Developer to provide various services, the Organisation retained possession and control over the Disclosed Data at all material times. It was responsible for the security arrangements to be implemented on the Website and its back-end system, as well as to protect the Disclosed Data.

13 Section 24 of the PDPA requires an organisation to 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 and similar risks.

14 To determine whether the Organisation was in breach of section 24, the relevant question is whether it had put in place reasonable security arrangements to safeguard the Disclosed Data hosted on the Website and its Server. As the Disclosed Data included the NRIC numbers of the tutors concerned, it should be borne in mind that NRIC numbers are of special concern as they are "*a permanent and irreplaceable identifier which can be used to unlock large amounts of information relating to the individual*".[1] Further, the Commission's

[1] *Re Habitat for Humanity Singapore Ltd* [2018] SGPDPC 9 at [19]

Advisory Guidelines on the PDPA for NRIC and Other National Identification Numbers (issued 31 August 2018) at [2.4], albeit not effective at the time of the breach, points to the risks and potential impact of any unauthorised use or disclosure of personal data associated with an individual's NRIC; and the expectation that organisations are to provide a greater level of security to protect NRIC numbers in its possession or control.

15 As the Organisation had engaged the Developer to develop the Website, the onus is on the Organisation to ensure that its security requirements for the Website and Server will be and have been met by the Developer. As part of this, the Organisation could have done the following[2]:

(a) emphasised the need for personal data protection to the Developer by making it part of the written contract;

(b) when discussing the Developer's scope of work, required that any changes the Developer made to the Website did not contain vulnerabilities that could expose the personal data, and to discuss whether the Developer had the necessary technical and non-technical processes in place to prevent the personal data from being exposed, accidentally or otherwise; and

(c) tested the Website before any new changes went live to ensure that the Organisation's instructions to the Developer were properly

[2] Further information on the steps that the Organisation should have taken when outsourcing the development of its Website may be found in the Commission's *Guide to Building Websites for SMEs*.

implemented and that the Website was sufficiently robust and comprehensive to guard against a possible cyberattack.

16 The Organisation admitted to the Commission that "there was a lack of technical expertise within Advance Home Tutor to protect personal data", including the lack of expertise "on how to make the technical assessment and ensure that the assessment is robust enough for adequate protection for personal data". This is also evident from the fact that the Organisation had required the Developer to migrate the information of its then-existing tutors from the old website to the Website "with the exact same conditions imposed" on the old website, without having any idea of how its old website had been configured.

17 Similar to *Re Tutor City* [2019] SGPDPC 5 ("***Tutor City***"), the Organisation also did not:

(a) communicate any specific security requirements to the Developer to protect the personal data stored on the Server;

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

(c) attempt to verify that the security measures implemented had indeed "*respect[ed] and protect[ed] the privacy and confidentiality of all the data that is present on the Website*" to the extent expected by the Organisation; and

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

18 To be clear, the lack of knowledge on the PDPA or expertise in the area of IT security is not a defence against the failure to take sufficient steps to comply with section 24 of the PDPA. There were resources, including the

guides published by the Commission, and skilled personnel available that the Organisation could have relied on to increase its knowledge in the relevant areas or to assist it in complying with its obligations under the PDPA.

19 Related to the above, I note that the Organisation's purported instruction to the Developer to "*respect and protect the privacy and confidentiality of all the data that is present on the Website*" does not constitute a security measure. The Organisation should have reviewed the security standard implemented on the Website and provided its Developer the intended use cases and identify foreseeable risks.[3]

20 More generally, although the Organisation asserted that it had provided verbal instructions to the Developer (see [7] above), these have not been substantiated by any evidence. According to the document entitled "Project Scope" entered into between the Organisation and the Developer, there was no specification relating to the security arrangements that the Developer was required to design into the Website and its back-end system. The Organisation ought to have entered into a written agreement with the Developer that clearly stated the standard of compliance that the Organisation expected its Website and Server to have with the PDPA, and the Developer's responsibilities in this regard.

21 As regards security testing, while the Organisation had conducted some testing of the Website from the functionality perspective, i.e., to verify that certificates of consenting tutors were disclosed on their profile pages, it did not check the profile pages of non-consenting tutors to ensure their certificates were

[3] *Re Tutor City* [2019] SGPDPC 5 at [18]

not disclosed. It also did not check if the Website contained any other vulnerabilities that posed a risk to the personal data hosted on the Server. Had the Organisation done a proper security test, the lack of access controls for the certificates hosted on the Image Directory and the unauthorised disclosure of the certificates of non-consenting tutors on their profiles would have been apparent. It would then have been able to take the necessary steps to rectify these security issues. That said, I understand that the Organisation has, since the Incident, procured the Developer to conduct a penetration test and resolve the high risk issues identified by it.

22 As regards the lack of access controls, it has been observed in *Tutor City* (at [21] to [23]) that technical measures are available that prevent indexing of images by web crawlers: viz,

(a) First, the Organisation could have placed these documents in a folder of a non-public folder/directory.

(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.

(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).

23 In view of the above, I find the Organisation in breach of section 24 of the PDPA.

Role of the Developer

24 The Developer's role in data migration constitutes "processing" within the meaning of the PDPA. One of the causes for the breach of the protection obligation may be traced to the migration of educational certificates to the Image Directory which was publicly accessible and could be indexed by search engines: see discussion at [4] above. As the Developer is in, and supplied the Services from, the Philippines, I intend to refer this aspect of the case to the Philippines National Privacy Commission.

Whether the Organisation had breached section 12 of the PDPA

25 Section 12 of the PDPA requires an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. Although the Organisation is a sole proprietorship with no employees, it collects a significant amount of personal data from the tutors and clients seeking tuition services via the Website. As such, it is required to have an external data protection policy which sets out its practices relating to such personal data and the purposes for which the tutors' and students' personal data are collected, used and disclosed by the Organisation.

26 In view of the Organisation's admission that it had not developed and implemented any such policies, I also find the Organisation in breach of section 12 of the PDPA.

Representations by the Organisation

27 In the course of settling this decision, the Organisation made representations to waive the imposition financial penalty for the following reasons:

(a) The Organisation is a small home business which does not generate much revenue. If the proposed financial penalty is imposed, the Organisation would take 5 to 6 years to recover the financial penalty amount based on its annual revenue;

(b) As a sole proprietor, the Organisation's director neglected operational duties of the business in order to assist the Commission with the investigations into the Incident. This resulted in a significant drop in the Organisation's annual revenue in 2018 and its revenue has yet to recover;

(c) The Organisation incurred significant costs in undertaking remedial and preventive actions following the Incident;

(d) This is the first time a data breach involving the Organisation has occurred; and

(e) The Organisation compared the present case to *Tutor City* with similar facts where only a warning had been issued taking into account the number of affected individuals, the type of and duration for which personal data was at risk, and the remedial actions taken.

28 While accepting full responsibility of its breach of Section 12, the Organisation also asserted in its representations that based on the grounds of decision of *Tutor City*, it "*…implicitly understood that [Tutor City] also had no policies and practices meeting the PDPA obligations set in place. However, they were not found in breach of the Section 12*".

29 With respect to the Organisation's representations comparing the present case to *Tutor City*, I would like to emphasize that my decision is based on the unique facts of each case. While the facts may appear similar in 2 cases, my decision in each case takes into consideration the specific facts of the case and the totality of the circumstances so as to ensure that the decision and direction(s) are fair and appropriate for that particular organisation. In this regard, I would highlight that Section 12 of the PDPA was never an issue of concern in *Tutor City* as the organisation in question did, in fact, have the requisite policies and processes. Accordingly, this is not a point that would need to be reflected in *Tutor City*. Unlike *Tutor City*, I have decided that a financial penalty is warranted in this case because the Organisation has been found in breach of Sections 12 and 24 of the PDPA, and there was a larger number of individuals' personal data at risk in the present case. I have also taken into consideration the fact that the duration for which personal data was at risk in the present case is significantly shorter than *Tutor City*.

30 Having carefully considered the representations, I have decided to reduce the financial penalty to $1,000. The quantum of financial penalty has been calibrated after due consideration of the Organisation's financial circumstances and to avoid imposing a crushing burden on the Organisation. Although a lower financial penalty has been imposed in this case, the quantum of financial penalty should be treated as exceptional and should not be taken as setting any precedent for future cases.

Outcome

31 In assessing the breaches and determining the directions to be imposed on the Organisation in this case, I also took into account the following mitigating factors:

(a) the Organisation fully cooperated with the Commission's investigations; and

(b) the Organisation took prompt action to mitigate the effects of the breaches and prevent reoccurrence of similar breaches.

32 In consideration of the relevant facts and circumstances of the present case, I hereby direct the Organisation:

(a) to put in place a data protection policy to comply with section 12 of the PDPA within 60 days of this direction;

(b) to inform the Commission within 7 days of implementing the above; and

(c) to pay a financial penalty of $1,000 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.

YEONG ZEE KIN
DEPUTY COMMISSIONER
[FOR COMMISSIONER] FOR PERSONAL DATA PROTECTION