PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 32

Case No DP-1807-B2376

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

And

O2 Advertising Pte. Ltd.

… *Organisation*

DECISION

O2 Advertising Pte. Ltd.

[2019] SGPDPC 32

Tan Kiat How, Commissioner — Case No DP-1807-B2376

28 August 2019

Background

1 An individual found certain of his personal data accessible over the Internet without his consent. In particular, the individual found that when he conducted a search on Google using his name and National Registration Identification Card ("**NRIC**") number, the search results included a URL link (the "**URL Link**") to a database maintained by O2 Advertising Pte. Ltd. (the "**Organisation**"). The database contained the personal data of numerous individuals including the individual's (the "**Affected Individuals**"). On 10 July 2018, the individual lodged a complaint with the Personal Data Protection Commission ("**Commission**") over the incident.

Material Facts

2 The Organisation provides advertising and marketing services in Singapore. In 2015, the Organisation collected the Affected Individuals' personal data during an advertising campaign conducted on behalf of one of its clients. The Organisation stored the collected personal data in two databases.

3 The incident resulted in the following types of personal data of the Affected Individuals being either exposed to unauthorised access or at risk of unauthorised access (the "**Disclosed Data**") depending on which database the Disclosed Data was stored in:

(a) Name;

(b) NRIC number;

(c) email address;

(d) residential address;

(e) gender;

(f) date of birth;

(g) mobile number;

(h) age; and

(i) skin type.

4 The Disclosed Data of 403 Affected Individuals was stored in one database ("**Database A**") and exposed to unauthorised access through the URL Link found by the complainant. The Disclosed Data of 1,165 Affected Individuals was stored in another database ("**Database B**") which was at risk of unauthorised access. This was because after accessing Database A using the URL Link, a party with knowledge of how to navigate the root directory could possibly gain access to Database B. In addition, there was a risk of unauthorised access to 2 php files found in a directory containing user names and passwords to the Organisation's email system and another database ("**Exposed**

Credentials"). Using the same URL Link, a party with knowledge of how to navigate the root directory could also possibly gain access to the Exposed Credentials.

The Commissioner's Findings and Basis for Determination

5 The issues for determination are:

(a) whether the Organisation breached the Protection Obligation under section 24 of the PDPA;

(b) whether the Organisation complied with its Retention Limitation Obligation under section 25 of the PDPA; and

(c) whether the Organisation complied with its Accountability Obligation under sections 11(3) and 12 of the PDPA.

Whether the Organisation breached section 24 of the PDPA

6 Databases A and B which contained the Disclosed Data were maintained by the Organisation. Hence, the Organisation had possession and control of the Disclosed Data at all material times and therefore had an obligation to protect them. Database A was in the Public_HTML directory of a server, and was not secured with any form of access controls. This enabled internet search engines like Google to index the URL Link to Database A, resulting in it showing up in search results. As stated above, this also exposed Database B to risk of unauthorised access. The Organisation asserted that the server hosting Database A and Database B was password protected. However, this was not a security arrangement to restrict access to the databases which had been stored in the Public_HTML directory.

7 As observed in *Re Tutor City* [2019] SGPDPC 5 (at [21] to [23]), there are a number of technical security measures that can be implemented to prevent documents from being indexed by web crawlers:

(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).

8 Since its website went live over 5 years ago, the Organisation had not conducted any vulnerability scanning. The flaws in the security of its website that had been discovered during investigations would have been revealed in a vulnerability scan. Had one been conducted, the Organisation would have been in a position to put in place reasonable security arrangements mentioned in the preceding paragraph.

9 For the reasons above, the Commissioner finds the Organisation in breach of section 24 of the PDPA.

Whether the Organisation breached section 25 of the PDPA

10 Under section 25 of the PDPA, an organisation is obliged to cease retaining personal data once the purpose for which the personal data was collected has been served, unless further retention can be justified for legal or business purposes. The Organisation admitted that it had overlooked deleting the Disclosed Data and that there were no reasonable grounds to continue retaining them after the engagement with its client ceased in 2016. The Disclosed Data was only deleted by the Organisation after it was informed by the Commission of the complaint. The Commissioner therefore finds the Organisation in breach of section 25 of the PDPA.

Whether the Organisation breached sections 11(3) and 12 of the PDPA

11 Section 11(3) of the PDPA requires the Organisation to a data protection officer; Section 12 of the PDPA imposes an obligation on organisations to develop and implement data protection policies and practices. The Organisation admitted that at the material time, it did neither of these. In the circumstances, the Commissioner finds that the Organisation failed to meet its obligations under sections 11(3) and 12 of the PDPA.

Representations by the Organisation

12 In the course of settling this decision, the Organisation made representations on the amount of financial penalty which the Commissioner intended to impose. In the beginning of 2016, the Organisation discovered it was a victim of a fraud involving the misappropriation of company funds amounting to approximately $3.2 million, resulting in massive retrenchment and significant cash flow issues for the Organisation. Consequently, the

Organisation's financial performance for the past few years has been weak, and is currently in dire financial straits. The director is 72 years old and is the Organisation's sole employee since 1 March 2018. He intends to continue the Organisation's business on a significantly reduced scale.

13 Having carefully considered the representations, the Commissioner has decided to reduce the financial penalty to $10,000. The quantum of financial penalty has been determined after due consideration of the Organisation's finances and to avoid imposing a crushing burden on the Organisation given its present financial circumstances and future prospects. 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.

The Commissioner's Directions

14 Having found the Organisation in breach of sections 11(3), 12, 24 and 25 of the PDPA, the Commissioner hereby directs the Organisation:

(a) to pay a financial penalty of $10,000 within 30 days from the date of the Commissioner's direction, failing which, interest at the rate specified in the Rules of Court[1] 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;

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

(b) to appoint an individual responsible for ensuring the Organisation's compliance with the PDPA within 30 days from the date of the Commissioner's direction;

(c) to develop and implement policies and practices that are necessary for the Organisation to meet its obligations under the PDPA within 60 days from the date of the Commissioner's direction; and

(d) to inform the Commission of the completion of each of the above directions in (b) and (c) within 1 week of implementation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION