PERSONAL DATA PROTECTION COMMISSION

[2018] SGPDPC 26

Case No DP-1706-B0834

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

And

WTS Automotive Services Pte. Ltd.

... Organisation

GROUNDS OF DECISION

WTS Automotive Services Pte. Ltd.

[2018] SGPDPC 26

Tan Kiat How, Commissioner – Case No DP-1706-B0834

13 December 2018

Background

1 This matter involves WTS Automotive Services Pte. Ltd. (the "**Organisation**"), a company which provides vehicle repair and maintenance services at Kaki Bukit and Gul Circle in Singapore. On 9 June 2017, a complaint was lodged by a member of the public ("**Complainant**") with the Personal Data Protection Commission ("**Commission**"), alleging that a URL link to the Organisation's customer database, which contained the personal data of the Organisation's customers, was publicly accessible over the Internet (the "**Incident"**). The Commissioner sets out below his findings and grounds of decision based on the investigations carried out in this matter.

Material Facts

2 The Complainant had been searching for a company address via Google's search engine, when he chanced upon the URL link to the Organisation's Kaki Bukit customer database, which contained the personal data of 2,472 of its Kaki Bukit customers. The personal data that was disclosed included the names, NRIC and FIN numbers, residential addresses, contact numbers, email addresses and car plate registration numbers of the Organisation's Kaki Bukit customers. The Complainant proceeded to lodge a complaint with the Commission on 9 June 2017. Upon receiving the complaint, the Commission commenced an investigation into this matter.

3 During the course of the investigation, the Organisation represented that it had implemented a Backend Electronic Job Card System ("**Backend System**") which ran as a web

application over the Internet since December 2013. The Backend System was set up for internal use only and was meant to allow the Organisation's staff to, amongst other things, store and access the personal data of the Organisation's customers. The Backend System was developed and maintained by ZNO International (Pte.) Limited ("**ZNO**") from October 2013. Subsequently, QGrids was responsible for the maintenance of the Backend System from March 2016. The Organisation represented that the publicly accessible URL link to the Organisation's Kaki Bukit customer database was part of the Backend System.

4 During the course of the investigation, the Commission also found that there were two other databases that were part of the Backend System, which similarly contained personal data and were also publicly accessible, as follows:

(a) the Organisation's Gul Circle customer database, which contained the names, NRIC and FIN numbers, residential addresses, contact numbers, email addresses and car plate registration numbers of 2,223 of the Organisation's Gul Circle customers; and

(b) the Organisation's master car database, which contained 3,764 records with the names of car owners, and the details of their cars, such as a car's make, model, plate number, colour, chassis number, registration number, transmission type and mileage.

5 All three URL links to the Organisation's three databases will collectively be referred to as the "**Compromised URL Links**". The Compromised URL Links were all webpages which provided data export functions, i.e. they allowed data to be exported into Microsoft Excel spreadsheets. By clicking on any of the Compromised URL Links, the corresponding Microsoft Excel spreadsheet would be generated and provided to a user. As the Microsoft Excel spreadsheets would subsequently be saved in the backend server, the Microsoft Excel spreadsheets could be discovered and indexed by search engines.

6 Notably, the Organisation admitted during the course of the investigation that the webpages of the Backend System were all secured by authentication mechanisms, save for the Compromised URL Links. The Organisation represented that the authentication mechanisms for the Compromised URL Links were "*left out by ZNO unintentionally*" during the development of the Backend System. With no authentication mechanisms to limit access to the

Compromised URL Links, search engines were able to discover and index these Compromised URL Links, rendering the respective databases publicly accessible over the Internet.

7 After the Organisation was notified by the Commission of the unauthorised disclosure of its Kaki Bukit customers database on 15 June 2017, the Organisation represented that it had taken the following steps to prevent the reoccurrence of the unauthorised disclosure of personal data:

(a) added Robots.txt to discourage search engines from crawling webpages of the Organisation's Backend System;

(b) secured all webpages in the Organisation's Backend System with login mechanisms;

(c) removed the Compromised URL Links from Google and Bing search engines; and

(d) migrated the Backend System to a local server and configured it to be only accessible within the Organisation's Local Area Network instead of the Internet.

Findings and Basis for Determination

8 At the outset, the information that was disclosed via the Compromised URL Links (names, NRIC and FIN numbers, residential addresses, contact numbers, email addresses, car plate registration numbers and details of cars, such as a car's make, model, plate number, colour, chassis number, registration number, transmission type and mileage) constitutes personal data as defined in section 2(1) of the Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**"), as the Organisation's customers and/or car owners could be identified from such information disclosed or is information that is about these identified customers and/or car owners.

9 The issue for determination is whether each of the Organisation, ZNO and QGrids had complied with the obligation under section 24 of the PDPA to implement reasonable security arrangements to protect personal data in its possession or under its control.

10 Section 24 of the PDPA provides:

> "*An organisation shall 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 or similar risks.*"
>
> [Emphases added.]

As a preliminary issue, the meaning of the terms "possession" and "control" under section 24 of the PDPA is considered. Whilst the definition of "possession" is not defined in the PDPA, the distinction between "possession" and "control" had been explained in *Re Cellar Door Pte Ltd [2016] SGPDPC 22* at [17] as:

> "it is possible for the same dataset of personal data to be in the possession of one organisation, and under the control of another. For example, in a situation where the organisation transfers personal data to its data intermediary, the organisation could remain in control of the personal data set while, simultaneously, the data intermediary may have possession of the same personal data set."

11 Notably, in *Re Cellar Door Pte Ltd*, it was found that even though the organisation was not in direct possession of the personal data that was held in the data intermediary's servers, it was still obliged to implement reasonable security arrangements to protect the personal data as it had control over such data.

12 As to the definition of "control", *AIG Asia Pacific Insurance Pte. Ltd.* [2018] SGPDPC 8 at [18] states that:

> "[w]hile there is no definition of "control" in the PDPA, the meaning of control in the context of data protection is generally understood to cover *the ability, right or authority to determine (i) the purposes for; and/or (ii) the manner in which, personal data is processed, used or disclosed.*"
>
> [Emphasis added.]

13 Against this backdrop, the issue for determination is whether each of the Organisation, ZNO and QGrids had possession or control of the personal data contained in the Compromised URL Links, so as to trigger the obligation to implement reasonable security arrangements to prevent its unauthorised disclosure under section 24 of the PDPA.

Whether ZNO had the obligation to protect personal data under section 24 of the PDPA

14 ZNO was the IT vendor engaged by the Organisation to develop, host and maintain the Backend System. While the Organisation claims that it had asked ZNO to include authentication mechanisms to limit access to the data found in the Compromised Links, the only evidence that the Organisation relied upon was the statement of its General Manager. Even if we take the Organisation's case at its highest and it is found that ZNO was indeed asked to implement authentication mechanisms, ZNO would not be in breach of the PDPA given that it had delivered the Backend System (save for one module which was not relevant to the Incident) in 2013. After the relevant PDPA provisions came into force on 2 July 2014, the onus is on the Organisation to review its existing systems and to put in place enhancements to ensure that the standards of protection under the PDPA are met. In this regard, the Commissioner finds that ZNO did not have the obligation under section 24 of the PDPA.

Whether QGrids had the obligation to protect personal data under section 24 of the PDPA

15 As of March 2016, QGrids had been engaged by the Organisation for the purposes of application and data migration from ZNO's web hosting services to Vodien Internet Solutions Pte. Ltd. ("Vodien"), a third party Singapore-based web hosting company which provides, amongst other services, domain registration and web hosting services, and subsequently, to take over the maintenance of the Backend System from ZNO. QGrids had possession of the personal data which is the subject of this decision in migrating the Backend Server to Vodien, and would have had to ensure that such personal data was protected. However, the data breach that occurred in this case was not a result of the migration of the Backend Server or QGrids role with respect to this. In this regard, the Commissioner finds that QGrids does not have the obligation under section 24 of the PDPA to implement reasonable security arrangements to protect the personal data contained in the Compromised URL Links.

Whether the Organisation had the obligation to protect personal data under section 24 of the PDPA

16 With regards to the development of the Backend System, the Organisation represented that it had "[specified] to ZNO that the website and system should be protected with login mechanism and role-based authorisation feature; however, these requirements were given verbally during requirement analysis and were not recorded in any document". Also, while the Organisation represented that it had tested the Backend System before it was delivered to the Organisation by ZNO, the user acceptance test was not documented by either the Organisation or ZNO.

17 The Commissioner takes this opportunity to reiterate the importance of clarifying the obligations of an organisation and a service provider and thereafter documenting these in writing and 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."

18 Presently, there is an absence of objective evidence showing that the Organisation had given specific requirements that login mechanism and role-based authorization was required. Equally, there is no evidence that this requirement was communicated, documented or – crucially – included within the scope of User Acceptance Tests. Post 2 July 2014 when the PDPA came into full force, the Organisation should have reviewed its systems to ensure that the standards of protection expected under the PDPA are met. The Commission also recognises that "personal data of individuals may be exposed if the website or database in which it is stored contains vulnerabilities. There needs to be a regular review to ensure that the website collecting personal data and the electronic database storing the personal data has reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks".[1] The Commission considers that it is good practice for an organisation to "conduct regular ICT security audits, scans and tests to detect

[1] PDPC, *Guide to Data Protection Impact Assessments* (published 1 November 2017), at [8.3].

vulnerabilities".[2] Against the above backdrop, the Organisation retained full responsibility for implementing reasonable security arrangements to protect the personal data contained in the Compromised URL Links. The Commission found that the Organisation did not take any steps towards protecting the personal data in its possession or under its control to prevent any unauthorised disclosure of the personal data contained in the Compromised URL Links. Additionally, it should have conducted regular IT security checks to ensure that the Backend System did "not contain any web application vulnerabilities that could expose the personal data of individuals collected, stored or accessed via the website through the Internet".[3]

19 Although access to the Backend System was only intended for staff of the Organisation, considering how the Backend System was accessible from the Internet, it would have been important for the Organisation to conduct IT security checks to detect vulnerabilities in the Backend System. The Commission takes the view that "[t]esting 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)."[4] In this regard, the Organisation represented that "there [was no] penetration testing performed prior to [the Commission notifying the Organisation about the unauthorised disclosure of personal data on 15 June 2018]".

20 Given the absence of any security arrangements to protect personal data against unauthorised disclosure, the Commissioner finds that the Organisation has contravened section 24 of the PDPA.

Representations

21 The Organisation made representations following the issuance of a preliminary Grounds of Decision. The Commissioner has considered the representations made and is of the view that the representations made do not justify any change in his decision or the directions

[2] PDPC, *Guide to Securing Personal Data in Electronic Medium* (revised 20 January 2017) at [6.1].
[3] PDPC, *Guide on Building Websites for SMEs* (revised on 20 January 2017), at [4.2.1].
[4] PDPC, *Guide on Building Websites for SMEs* (revised on 20 January 2017), at [5.6.1].

made. The Commissioner sets out below the points raised in the representations together and the reasons for rejecting the representations.

22 The Organisation in its representation states that they implemented a role based authorisation feature and a login mechanism. These facts have already been taken into consideration. The Organisation's claims that it had instructed its vendor to protect the system with a login mechanism and a role based authorisation feature are considered in paragraph 18 above. Even on the assumption that instructions for a role based authorisation feature and a login mechanism was properly given, the authentication mechanisms were not implemented with respect to the Compromised URL Links and any alleged instructions were not documented. As stated in paragraph 17, such instructions should be documented in writing to clarify the obligations of an organisation and a service provider.

23 The Organisation also states in its representations that they had expected its vendor ZNO to conduct all the necessary audits as it was still developing the backend system even after the relevant data protection provisions under the PDPA came into force on July 2014 and that the disclosure resulted from a programming flaw. This has already been considered at paragraph 14 above. Further, organisations should take note that while they may delegate work to vendors to comply with the PDPA, the organisations' responsibility for complying with statutory obligations under the PDPA may not be delegated. In this case, the Organisation simply did not put in place any security arrangements to ensure that it complies with its obligations under section 24 of the PDPA.

24 The final point made by the Organisation in its representations is that it had no technical expertise to identify technical flaws and had no reason to suspect that the compromised URL links would be published on the Internet. In the present case, the gravamen lies in the lack of awareness and initiative on the part of the Organisation, as owner of the system, to take its obligations and responsibilities under the PDPA seriously. It is unrealistic to expect all organisations to have the requisite level of technical expertise to manage increasingly complex IT systems. But a responsible organisation would have made genuine attempts to engage competent service providers and give proper instructions. In this case, it is the paucity of evidence of such instructions, purportedly made by the Organisation, that stands out. Likewise, there was no evidence that it had conducted adequate testing of the system. Pertinently, while these lapses may have been more excusable before 1 July 2014, there is no excuse for the

Organisation not to have initiated (and properly documented) a review of the system for compliance with the PDPA. The responsibilities of ownership do not require technical expertise.

Directions

25 Having found that the Organisation is in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

26 In assessing the breach and determining the directions to be imposed on the Organisation, the Commissioner took into account the following mitigating factors:

(a) the Organisation was generally cooperative, forthcoming and prompt in providing responses to the Commission during the investigation; and

(b) the Organisation took immediate remedial actions to rectify and prevent the recurrence of the data breach.

27 The Commissioner also took into account the aggravating factor that the Organisation showed a lack of accountability with respect to the Backend System and its obligation to protect the personal data that was stored on it. Not only did the Organisation fail to document the instructions given to ZNO to implement login mechanism and role-based authorisation features for the Backend System, the Organisation had also failed to document the user acceptance test. While the system was developed and delivered before the PDPA came into full force, the Organisation knowing full well that its practices left a lot to be desired from a security standpoint, ought to have audited its systems before 2 July 2014 to ensure that its practices are PDPA compliant. The failure to do so reflected the Organisation's lack of accountability in ensuring that it had made reasonable security arrangements to protect the personal data on the Backend System, as well as to prevent any unauthorized disclosure or similar risks to such data.

28 In consideration of the relevant facts and circumstances of the present case, the Commissioner hereby directs the Organisation to pay a financial penalty of S$20,000 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 be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION