PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 8

Case No. DP-2001-B5645

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

And

Stylez Pte Ltd

… *Organisation*

DECISION

Stylez Pte. Ltd.

[2021] SGPDPC 8

Lew Chuen Hong, Commissioner — Case No. DP-2001-B5645

4 August 2021

Introduction

1 On 25 December 2019, a local newspaper reported that data from a quotation and service comparison portal, iCompare.sg ("**the Portal**"), had been uploaded onto the Dark Web (the "**Incident**")[1]. The Personal Data Protection Commission ("**the Commission**") commenced investigations into the Incident thereafter.

Facts of the Case

2 The Portal was created and operated by Stylez Pte Ltd ("**Organisation**") at the material time. In July 2016, the Organisation created a new database containing data from the Portal for the purposes of testing a new function for the Portal in a separate test environment (the "**Testing Database**"). The Testing Database was a text file comprising records of the Portal's renovation and interior design clients from 2009 to 2016 and was hosted on a cloud server leased from a cloud storage service provider ("**the Server**").

3 Investigations revealed that the data exposed in the Incident was accessed and exfiltrated from the Testing Database some time before December 2019. A total of 9,983 individuals' personal data, comprising their name, email address, and phone number were exposed in the Incident.

4 The Portal's production and backup databases were hosted on servers leased from a different cloud service provider and were unaffected in the Incident.

[1] https://www.straitstimes.com/singapore/local-renovation-database-exposed-on-dark-web

Remedial actions

5 Following the Incident, the Organisation took the following remedial actions:

a. The Testing Database and the account from which it was hosted were deleted;

b. A malware scan was run on the Server, and all unnecessary files were removed;

c. The operating system of the Server was updated and the root password was changed;

d. A website security scanning tool was installed to conduct security scanning of the Portal; and

e. The individuals affected in the Incident were notified.

Findings and Basis for Determination

Whether the Organisation contravened the Protection Obligation

6 Section 24 of the Personal Data Protection Act 2012 ("**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 or similar risks (the "**Protection Obligation**"). For the reasons set out below, the Organisation failed to implement reasonable security arrangements to protect the personal data in the Testing Database.

7 Firstly, the Testing Database was stored in a publicly accessible directory in the Server without any access controls. This resulted in the Testing Database being directly accessible from the Internet and crawled and indexed by search engines. This was a serious breach considering the volume of personal data contained in the Testing Database.

8 In the course of investigations, the Organisation characterised this as a failure to activate an anti-indexing function in the Server's software, which could have prevented the

Testing Database's URL from being indexed by search engines. This is incorrect. Even if the anti-indexing function had been activated, this would only have prevented the Server's directory contents from being listed. The actual contents of any publicly listed directory on the Server could still have been crawled and indexed by search engines. Crucially, anti-indexing is not the same as access control and even if the Testing Database's URL was not indexed, it could have been accessed directly without the need for authentication. This failure to appreciate the difference between anti-indexing and access control is a fundamental failing on the Organisation's part. Proper authentication measures (e.g. password protection, access whitelisting) should have been implemented to control access to the Testing Database.

9 Secondly, privileged access to the Server (and in turn the Testing Database) was also not adequately secured. Though the password for the IT administrator's account was strong (16 characters with upper and lower alphabets, numeric and special symbols), there was no limit imposed on the number of unsuccessful login attempts which could be made. This made the account vulnerable to brute-force attacks. The password to the IT administrator's account was also stored in his email account in clear-text without the need for any two-factor authentication. This significantly weakened the protection accorded to the Server by strong login credentials.

10 Thirdly, the Testing Data was stored in the Server in an unencrypted format for more than two and a half years (i.e. from July 2016 to December 2019). While the Organisation claimed that the Testing Data was subsequently used for other business purposes, in general, production data (i.e. actual personal data) should not be held in less secure development environments for extended periods of time. This is discussed further below in relation to the Organisation's breach of the Retention Limitation Obligation.

11 For the above reasons, it was determined that the Organisation breached the Protection Obligation in respect of the personal data in the Testing Database.

Whether the Organisation contravened the Accountability Obligation

12 Section 12(a) 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 (the "**Accountability Obligation**").

13 While the Organisation had developed an *external* data protection policy which communicated its purported data protection standards to customers and prospective customers, it failed to develop and implement any corresponding *internal* data protection policies to give effect to these externally communicated standards.

14 By way of illustration, the Organisation's external data protection policy stated:

> "*We have developed guidelines and implemented procedures to govern the destruction of personal data that are no longer required to fulfil the identified purposes*."

15 In fact, no such guidelines or procedures were implemented, and this made what was communicated to the Organisation's customers and prospective customers effectively an empty promise. While the Organisation claimed that it had relied on verbal reminders to inform its staff on the importance of data protection, these reminders were undocumented, and in any event, inadequate.

16 An organisation will not be taken to have complied with the Accountability Obligation merely because it publishes and communicates a data protection policy to external parties. Any externally communicated data protection policy must be given the weight of the necessary *internal* policies and documented practices to guide an Organisation's employees on how to comply with the PDPA in carrying out their work functions.

17 For this reason, the Organisation was determined to have breached the Accountability Obligation.

Whether the Organisation contravened the Retention Limitation Obligation

18 Section 25 of the PDPA requires an organisation to cease retaining data in a form that can identify the individual if the purpose of collection no longer exists, and if no business or legal reason exists for retention (the "**Retention Limitation Obligation**").

19 In this case, the explicit purpose of creating the Testing Database was to test a particular new function for the Portal in a separate environment. That purpose no longer existed once the testing had been completed, and it was for the Organisation to justify why it continued to retain the Testing Database for any legal or business reasons.

20 The Organisation claimed that it had continued to retain the Testing Database for the purposes of business analysis, namely, to analyse (i) users' requirements to improve the Organisation's marketing strategy (i.e. specifications listed by users for their renovation or interior design jobs such as property type, room type, budget etc); and (ii) details on when users made enquiries via the Portal in order to optimise the timing of online advertising. The Organisation claimed that it could not have used other sources of data (such as their production or regular backup databases) for these purposes as there was a risk of causing inadvertent contamination of those databases if so used.

21 This justification was not accepted. Simply put, the business analysis described by the Organisation did not require retention of data that could identify individuals. Even if the Organisation wanted to retain the data in the Testing Database for these new business purposes, the data could have been aggregated or anonymised (i.e. with any personal identifiers removed) which would have taken the data outside the scope of regulated personal data, and allowed it to be used as unregulated anonymised data.

22 It was also doubted that the Organisation would have relied on historical data from as early as 2009 to conduct customer behaviour and preference studies when it would have been more commercially useful to conduct such studies based on more recent data. In any event, no

weight was placed on this factor in determining that the Organisation had failed to comply with the Retention Limitation Obligation in respect of the personal data in the Testing Database.

23 Had the Organisation carried out what it claimed that it would do in its external data protection policy (see [14] above), it may well have ceased retention of or at least anonymised the data in the Testing Database before the Incident.

The Commissioner's Directions

24 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and if so, the amount of such financial penalty, the factors listed at section 48J(6) of the PDPA were taken into account, as well as the following aggravating and mitigating factors:

Aggravating Factors

(a) The personal data of almost 10,000 individuals was publicly exposed in the Incident;

(b) The Testing Database contained records that were 10 years old at the time of the Incident;

(c) The Organisation misrepresented the standard of its internal data protection policies and practices to external parties;

Mitigating Factors

(d) The Organisation took prompt remedial actions after being notified of the Incident; and

(e) The Organisation was cooperative during the investigations.

25 Having considered all the relevant factors of this case including representations made by the Organisation on 5 July 2021 after being notified of the Commissioner's Preliminary Decision, the Commissioner hereby:

(a) Requires the Organisation to pay a financial penalty of $37,500 in 12 monthly instalments by the due dates as set out in the notice accompanying this decision, 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;

(b) Directs the Organisation to develop and implement internal data protection policies and practices to comply with the PDPA within 60 days of the relevant direction accompanying this decision, and to notify the Commission within 1 week of the completion of this direction.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION