(1) MSIG Insurance (Singapore) Pte Ltd

(2) Globalsign.in Pte Ltd

[2019] SGPDPC 43

Mr Tan Kiat How, Commissioner – Case Nos. DP-1708-B1066; DP-1708-B1086

Data protection – Protection obligation – Disclosure of personal data – Insufficient security arrangements

Data Protection – Retention limitation obligation – Purpose for which the personal data was collected is no longer served by retaining data – Retention is no longer necessary for legal or business purposes

19 November 2019

Introduction and Material Facts

1. MSIG Insurance (Singapore) Pte Ltd ("**MSIG**") notified the Personal Data Protection Commission (the "**Commission**") on 22 August 2017 that the mass emailing system of its service provider, Globalsign.in Pte Ltd's ("**GSI**"), had been accessed without authorisation and used to send spam emails (the "**Incident**") to 149,172 email addresses which belonged to MSIG's customers ("**Impacted Customers**").

2. GSI runs and hosts an email marketing platform known as "Global2Mail Online Marketing Web Application" (the "**G2M**" platform). GSI uses the G2M platform to send mass marketing emails to email addresses supplied by its clients.

3. MSIG, an insurance provider, had engaged GSI to send marketing emails to its customers via the G2M platform. For this purpose, MSIG and GSI had entered into an agreement dated 1 October 2013. An addendum to the said agreement was entered into on 16 May 2014 to take into consideration the obligations of both organisations under the Personal Data Protection Act 2012 (the "**PDPA**"). GSI's services were renewed by MSIG, with MSIG and GSI entering into a new agreement on 1 August 2017 (the "**Agreements**").

4. MSIG provided GSI with a list of email addresses of its customers each time an email marketing campaign was launched. For some of the email addresses, MSIG also provided the first and last names to GSI and these would be captured in the G2M platform. According to MSIG, the email addresses and names (where applicable) provided to GSI were password-protected.

5. Although no specific retention period for the email addresses provided by MSIG to GSI was stated in the Agreements, MSIG required GSI to delete and purge the email addresses and other personal data from its server after each marketing campaign. This is seen from emails sent by MSIG to GSI on 9 December 2016, 30 May 2017 and 5 June 2017 where MSIG asked GSI to confirm that it had purged the email addresses which had been provided by MSIG to GSI for specific marketing campaigns.

6. On 18 August 2017, the administrator account of the G2M platform was accessed without authorisation. By accessing the administrator account, the intruder was also able to access the email addresses and, in certain instances, names of individuals (the "**Compromised Data**") that were stored on the G2M platform.

7. On 19 August 2017, the G2M platform sent spam emails to 359,364 email addresses that were stored on the G2M platform (the "**Spam Emails**"). 149,172 of these email addresses were email addresses of MSIG's Impacted Customers (which MSIG had provided to GSI) and 201,192 were email addresses of customers ("**Other Impacted Individuals**") provided to GSI by three of GSI's other clients for use with the G2M platform. Each of the Spam Emails:
   (a) purported to provide tips on how to win a lottery;
   (b) contained a link under "clickbank.net" that redirected its users to a video on "lotterydominator.com";
   (c) appeared be sent from "MSIG Insurance" with the address "service@sg.msig-asia.com";
   (d) was only sent to one email address; and
   (e) contained no other personal data other than the email address of the recipient.

8. After MSIG informed the Commission about the Incident on 22 August 2017, MSIG and GSI jointly engaged a cyber-security consultancy to investigate into the data breach.

9. The cyber-security consultancy's investigations concluded that the Spam Emails did not contain phishing or malware content. It would appear that the end users who clicked on the links in the Spam Emails were simply redirected to the video on the "lotterydominator.com" website and there were no complaints from the users of any further negative consequences from clicking the links.

10. MSIG took the following remedial action after the Incident:
    (a) On 21 August 2017, MSIG posted an alert on the Spam Emails on its corporate website and Facebook page.
    (b) On 22 August 2017, MSIG instructed GSI to purge all email addresses and names of its customers in GSI's database, save for those customers that were affected, as they wanted to send out an apology email;
    (c) FAQs were included from 28 August 2017. MSIG also instructed GSI to deactivate its email account service@sg.msig-asia.com which had been used to send the Spam Emails;
    (d) On 24 August 2017, MSIG worked with GSI on an email sent by the latter to all 149,172 affected MSIG customers to apologise for the breach. The email included instructions on removing any malware from the link in the Spam Email. It provided a point of contact for any queries. MSIG instructed GSI to purge the email addresses and names of its affected customers thereafter.

11. Between 21 to 30 August 2017, MSIG addressed queries from 92 customers who had been affected by the Incident.

12. Separately, GSI took the following remedial action after the Incident:
    (a) Blocked the Spam Email link at server level to prevent recipients being re-directed to the site;
    (b) Immediately disabled the compromised administrator account to ensure no data would be exported and subsequently restored the account after putting in place additional security measures;
    (c) Changed password to the administrator account before restoring the account and implemented two-factor authentication (2FA) for all accounts whereby users would have to key in a one-time password sent either sent to their mobile number by SMS or Google Authenticator Application;
    (d) Transferred the application database to a new server, hosted in Amazon Web Services in Singapore in an encrypted database;

(e) Enforced HTTPS so that all traffic from end-users to GSI's website would be encrypted;

(f) Improved logging of access, whereby I.P. addresses used to access G2M would be properly logged at application server level, and added logging of web attacks that had been blocked by the server firewall; and

(g) Engaged a consulting company to assist GSI in implementing policies that meet the ISO 27001 standards.

Findings and Basis for Determination

Whether the Compromised Data included Personal Data

13. The personal data found in the Compromised Data included (i) the first and last names of some MSIG customers, (ii) the email addresses of those customers (i.e. which were stored with the names of the customers) and (iii) the email addresses of other customers which contained their full or partial names (the "**Compromised Personal Data**"). In relation to the latter set of email addresses, as set out in *Re Credit Counselling* [2017] SGPDPC 18 at [9], email addresses are personal data if they disclose the full name or partial name of individuals which allows for the identification of such individuals.

14. The Compromised Data also included other email addresses which were not linked to, or did not contain, the name of the customer ("**Other Email Addresses**"). It was also noted in *Re Credit Counselling* (at [10]) that an email address coupled with other information which enables identification of an individual, such as information obtained from a search on the Internet, is personal data.

Whether MSIG or GSI had breached section 24 of the PDPA

15. The main issue in this case is whether MSIG and GSI had done enough to protect the Compromised Personal Data which was in their possession or under their control. Section 24 of the PDPA requires organisations to make reasonable security arrangements to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or similar risks.

16. As MSIG had provided the personal data relating to MSIG's Impacted Customers to GSI in order to make use of the G2M platform for its purposes, both MSIG and GSI are required to comply with section 24 of the PDPA. However, the scope of their respective obligations under that section differs. In addition, GSI would be required to comply with section 24 in respect of all Compromised Personal Data (that is, personal data relating to MSIG's Impacted Customers and the Other Impacted Customers).

17. In relation to MSIG, as they had engaged GSI to send marketing emails using the G2M platform, the scope of their obligations would relate to the arrangements MSIG established in order to ensure that GSI protected the personal data in the G2M platform. In respect of MSIG, the Commissioner found that MSIG had complied with its obligations under section 24 of the PDPA for the following reasons:
    (a) MSIG imposed security requirements on GSI under the Agreements to protect personal data. An express clause in the Agreements provides that GSI shall *"implement sufficient and appropriate measures to guard against accidental or unauthorised access, collection, use, disclosure, misuse, loss, destruction, deletion, alteration, modification and processing of the Personal Data"*;
    (b) MSIG also had the right under the Agreements to inspect and audit GSI; and
    (c) There was evidence that MSIG followed through with these contractual obligations with operational processes, for example, there were emails showing that MSIG required GSI to purge the personal data it provided after each marketing campaign. In this regard, MSIG had sent emails to GSI on at least three separate occasions between December 2016 and June 2017 asking GSI to purge email addresses provided by MSIG from its system.

18. In relation to GSI, as GSI was operating the G2M platform, it was required to put in place reasonable security arrangements in the form of technical or administrative measures to protect the personal data in the G2M platform. In this regard, the Commissioner found that GSI had not made the appropriate security arrangements and was therefore in contravention of section 24 of the PDPA for the following reasons:
    (a) GSI had not implemented administrative or technical measures to require a regular change to the passwords to its administrator and client accounts in the G2M platform. In addition, GSI recognised that there was a risk that if accounts of staff who had left the employment of GSI were not disabled, these former staff may continue to have access to its applications. The need for an effective

password expiry mechanism has been discussed in past decisions such as *Re Orchard Turn Developments Pte Ltd* [2017] SGPDPC 12;

(b) When the administrator account changed hands, there were no logs to record the fact that passwords had been changed;

(c) Users were encouraged to choose strong passwords but GSI did not enforce any password strength requirements. The need for strong passwords is discussed in *Re Singhealth and anor [2019] SGPDPC 3*;

(d) All the users of the administrator account shared the same administrator account and the same set of login credentials. This made it difficult to determine which staff had accessed the account or identify who had made changes to the system during each log-in session. *Re Orchard Turn Developments Pte. Ltd.* [2017] SGPDPC 12 explains why the sharing of administrator account credentials can give rise to an increased risk of data breaches;

(e) It was found that no security scans were carried out over the 12 months before the Incident. Security scans are important in light of the type of personal data likely to be held by MSIG as an insurer. In *Re Courts (Singapore) Pte Ltd* [2019] SGPDPC 4, the Respondent's lack of regular testing and scanning for security issues were taken into account as factors to find a breach of section 24 of the PDPA.

(f) GSI claimed that it had complied with MSIG's express instructions to "delete and purge the data after each marketing campaign". However, this cannot be true as the G2M platform still retained at least 149,172 email addresses provided by MSIG which had been used in this Incident.

Whether GSI had complied with section 25 of the PDPA

19. As noted above, it appeared that GSI had not deleted 149,172 email addresses provided by MSIG after the relevant marketing campaigns were completed and notwithstanding email reminders from MSIG. Section 25 of the PDPA requires an organisation to cease retaining documents containing personal data, or to remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that:

(a) The purpose for which that personal data was collected is no longer being served by retention of the personal data; and

(b) Retention is no longer necessary for legal or business purposes.

20. As GSI was required to delete email addresses provided by MSIG once the relevant marketing campaigns were completed, GSI *ipso facto* ceased to have any purpose for retaining the email addresses in the G2M platform once the relevant marketing campaigns were completed. Accordingly, the Commissioner found that GSI was in contravention of section 25 of the PDPA.

GSI's Representations

21. After the Commissioner's preliminary decision was issued to MSIG and GSI, GSI submitted representations in relation to the quantum of financial penalty which the Commissioner proposed to impose in relation to its breach of section 24 of the PDPA and against the Commissioner's determination that it had breached section 25 of the PDPA. However, GSI did not disagree with, or make any representations relating to, the Commissioner's findings that it had breached section 24 of the PDPA.

22. First, GSI raised the following points as to why certain numbers of email addresses should not be taken into consideration in determining the number of affected individuals:
    (a) 4,488 of the email addresses which were stored on the G2M platform and which received the Spam Emails did not include the name or any other identifier of the individuals;
    (b) approximately 12,000 Spam Emails sent to the email addresses stored on the G2M platform had bounced;
    (c) approximately 145,338 Spam Emails were sent to GSI's overseas based clients; and
    (d) Only 18,113 recipients opened the Spam Emails and, of these, only 339 recipients clicked on the link contained within the Spam Emails.

23. In relation to sub-paragraph (a) above, the Commissioner accepts GSI's representation and has taken the reduced number of impacted individuals into account in determining the financial penalty quantum specified below. In relation to (b), the fact that the Spam Emails bounced is not conclusive that the email addresses were invalid as the emails may have bounced due to other reasons, such as the recipient's email inbox being full at that time. In relation to (c), GSI is required to protect personal data in its possession or under its control and it is immaterial whether the relevant individuals were resident in Singapore or overseas. Finally, in relation to (d), it has already been taken into account that there was no harm suffered by the recipients (see paragraph 32 below) and the Organisation's point at (d) above does not provide further mitigation of the Organisation's breach

24. Secondly, GSI represented that MSIG had access to the G2M platform and could exercise functions such as verifying the content of the platform, creating and sending out email campaigns and deleting content and emails. However, the fact that MSIG had access to the G2M platform does not absolve GSI from its obligations under the PDPA. The fact remains that MSIG had engaged GSI to send marketing emails using the G2M platform and GSI was obliged under the PDPA to protect the personal data that was in its possession or under its control for the purposes of this engagement. Furthermore, MSIG had specifically instructed GSI to delete the email addresses after each marketing campaign and this is something that GSI is contractually bound to do.

25. Thirdly, GSI raised the following additional points as mitigating factors for the Commission's consideration:

    (a) GSI had been fully cooperative during the Commission's investigations;
    (b) There was no evidence of exfiltration, further disclosure or modification of the Compromised Data;
    (c) The Spam Emails sent to the Impacted Customers did not contain any personal data;
    (d) There was no evidence of actual loss or damage suffered by any of the Impacted Customers;
    (e) GSI has also sent an email notification to all Impacted Customers of the Spam Emails;
    (f) GSI has in place internal data protection policies prior to the Incident; and
    (g) GSI has since taken further steps to tighten and strengthen its data protection policies and mechanisms, including sending additional employees for further PDPA training, engaging external vendors to conduct advisory sessions and gap analysis, completing a surveillance audit and implementing various internal programs and workshops to promote data responsibility.

26. The matters in sub-paragraphs (a) to (d) above had already been taken into consideration in determining the financial penalty (see paragraph 32 below). With regards to (f), organisations are required under the PDPA to implement policies and practices necessary for them to meet their obligations under the PDPA, and mere compliance with the PDPA is not a mitigating factor.

27. GSI's notification of the affected individuals is a relevant consideration and the further steps set out in (g) are relevant mitigating factors and the quantum of the final financial penalty set out below has been reduced.

28. Fourthly, GSI sought to compare the facts of this case with prior decisions such as *Re Avant Logistic Service Pte Ltd* [2019] SGPDPC 28, *Re AIA Singapore Private Limited* [2019] SGPDPC 20, Re *InfoCorp Technologies Pte Ltd* [2019] SGPDPC 17, *Re Option Gift Pte Ltd* [2019] SGPDPC 10 and *Re AIG Asia Pacific Insurance Pte Ltd & Toppan Forms (S) Pte Ltd* [2019] SGPDPC 2. It should be borne in mind, that none of these cited cases dealt with a similar scale of breach and cannot be relied upon to argue for a lower financial penalty.

29. GSI also made the following representations against the Commissioner's determination that it had breached section 25 of the PDPA:

(a) GSI sent an email to MSIG on 5 June 2017 confirming the deletion or purging of data from previous campaigns. This email read as follows:

> *"Yes, we are in the midst of purging the most recent campaigns. The older ones have been purged."*

The above email does not confirm that all completed campaigns have been purged, and only indicated that GSI was in the midst of doing so, and shows that some email addresses from recently concluded campaigns had not been removed from the system. This is, at best, evidence that GSI was trying to purge customer data after each campaign, but was not particularly prompt.

(b) GSI asserted that MSIG was an active client and, hence, the G2M platform retained 149,172 email addresses of MSIG's customers even after data from previous campaigns had been purged. However, this is contrary to the evidence which shows that MSIG had requested GSI to delete all email addresses after each email marketing campaign; and GSI's representations that it was putting in effort to do so (albeit with some delays).

In the final analysis, the representations in relation to the breach of section 25 of the PDPA did not warrant a review of the Commissioner's findings.

Outcome

30. After considering the facts of this case, the Commissioner hereby directs GSI to pay a financial penalty of $34,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty at such rate as specified in the Rules of Court.

31. In determining the amount of the financial penalty set out above, the Commissioner recognised that not all of the 359,364 email addresses targeted by the Spam Emails in the Incident constituted personal data and it was not possible for the Commission to determine the exact number of email addresses which did constitute personal data. Nevertheless, taking into account the GSI lapses and the other facts of the case detailed above, the Commissioner considered that a financial penalty of $34,000 would be appropriate.

32. In coming to this decision, the Commissioner also had regard to the following mitigating factors:

(a) GSI was cooperative in the course of the Commission's investigation and had provided prompt responses to the Commission's requests for information;
(b) GSI implemented the remedial actions set out paragraphs 10 to 12 above to address the Incident quickly, including notifying the affected individuals; and
(c) There was no harm caused by the disclosure of the Compromised Personal Data.

33. The Commissioner was of the view that no further directions are required given the remedial actions already taken by MSIG and GSI.
