PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPC 5

Case Nos. DP-2110-B9054 / DP-2110-B9060

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

And

(1) Fullerton Healthcare Group Pte Limited

(2) Agape CP Holdings Pte. Ltd.

... Organisations

DECISION

Data Protection *– Protection obligation – Unauthorised access to personal data – Unauthorised disclosure of personal data – Insufficient security arrangements - Failure to conduct reasonable periodic security review – Inadequate password policy*

Data Protection *– Protection obligation – Data intermediary – Obligations of organisation and data intermediary - Failure to exercise reasonable oversight over data intermediary*

Data Protection *– Protection Obligation – Financial penalty – Social enterprise*

(1) Fullerton Healthcare Group Pte Limited

(2) Agape CP Holdings Pte. Ltd.

Lew Chuen Hong, Commissioner — Case Nos. DP-2110-B9054 / DP-2110-B9060

23 March 2023

Introduction

1 On 19 October 2021 and 21 October 2021, Fullerton Healthcare Group Pte Limited ("**FHG**") and Agape CP Holdings Pte. Ltd. ("**Agape**") respectively notified the Personal Data Protection Commission (the "**Commission**") that the personal data of FHG's customers had been accessed, exfiltrated, and offered for sale on the dark web (the "**Incident**"). The Commission commenced investigations to determine whether the Incident disclosed any breaches of the Personal Data Protection Act 2012 ("**PDPA"**) by FHG and Agape.

2 On 11 January 2022 and 12 January 2022 respectively, FHG and Agape requested for the investigations to be handled under the Commission's Expedited Decision Procedure. In this regard, FHG and Agape voluntarily provided and admitted to the facts set out below and admitted that they had failed to implement reasonable security arrangements to protect the personal data accessed and exfiltrated in the Incident in breach of section 24 of the PDPA (the **"Protection Obligation"**).

Facts of the Case

3 FHG is an enterprise healthcare service provider which provides healthcare services to individuals and employees of its corporate clients. In 2018, FHG engaged Agape, a business process outsourcing provider and social enterprise, to provide call centre and appointment booking services for its customers (the "**Services**"). As part of its social enterprise initiatives, Agape engaged inmates from Changi Women's Prison (the "**Agents**") to assist in provision of the Services for FHG's customers.

4 In order to carry out the Services, FHG provided Agape with access to the personal data of its customers via Microsoft SharePoint, a cloud-based document management system. A single Agape personal computer (the **"Computer**") was authorised to access FHG's SharePoint platform via an FHG-assigned SharePoint account.

5 In order to facilitate Agents' access to FHG's customer data from within Changi Women's Prison, Agape downloaded FHG's customer data onto the Computer, and re-uploaded the customer data onto an internet-facing file server ("**the Online Drive"**). The Online Drive was then white-listed for access by the Agents from within Changi Women's Prison.

The Incident

6 On 15 October 2021, FHG became aware that its customer data was being offered for sale on a dark web forum. FHG engaged cybersecurity consultants to investigate. On 18 October 2021, FHG's cybersecurity consultants made contact with the purported seller who

claimed that he had exfiltrated FHG's customer data from Agape's Online Drive. By 22 October 2021, the post on the dark web forum advertising the sale had been removed.

7 FHG's cybersecurity consultants confirmed that the Incident solely involved and affected Agape's Online Drive. FHG's own systems and servers were not affected in the Incident.

8 The personal data of 156,900 FHG customers (133,866 direct patients and 23,034 employees of FHG's corporate clients) was accessed without authorisation in the Incident, although the exact volume of exfiltrated personal data was unknown. The affected personal data comprised the following datasets:

Direct patients

(a) Name;

(b) NRIC number / FIN;

(c) Date of birth;

(d) Gender;

(e) Email address;

(f) Telephone number;

(g) Financial information (Bank account numbers and bank codes);

(h) Health information (International Classification of Diseases codes that pertain to an individual's diagnosis information, and codes for surgical procedures done in hospitals);

Employees of FHG's corporate clients

(i) Name;

(j) NRIC number / FIN / Passport number;

(k) Date of birth;

(l) Email address;

(m) Financial information; and

(n) Health, and other information (Information relating to the utilisation of health benefits by individual members, which include details of clinic names and claim amount

(collectively, the "**Customer Data**").

Remedial actions

9 As part of remedial measures following the Incident, FHG informed affected clients and individuals promptly via SMS, email, and an FAQ page on its website, advising on appropriate steps which could be taken to guard against potential risks. FHG also engaged Credit Bureau (Singapore) Pte Ltd to provide free credit monitoring services to affected individuals for 6 months.

10 Agape suspended use of the Online Drive with effect from 19 October 2021, and, with the assistance of a forensic team, conducted internal checks on the Computer and Online Drive for other indicators of compromise.

11 FHG in coordination with Agape also:

(a) restricted Agape's access to its SharePoint to "view-only";

(b) deleted SharePoint files and folders that Agape did not need as part of data minimisation efforts;

(c) ceased synchronisation of data between SharePoint and the Computer;

(d) changed all passwords for Agape's access to FHG's SharePoint; and

(e) deleted the Customer Data from the Online Drive upon completion of Agape's investigations into the Incident.

Findings and Basis for Determination

Whether Agape had contravened the Protection Obligation

12 As a data intermediary of FHG, Agape is subject to the Protection Obligation pursuant to section 4(2) of the PDPA. For the reasons set out below, Agape was determined to have breached the Protection Obligation in relation to the Customer Data affected in the Incident.

Failure to conduct reasonable periodic security reviews

13 In previous enforcement decisions, the Commission has emphasised the need for organisations to conduct periodic security reviews of their IT systems. Such reviews enable organisations to detect vulnerabilities, assess security implications and risks, and ensure that reasonable security arrangements are implemented to eliminate or mitigate such risks. Periodic security reviews should be scoped based on the organisation's assessment of its data protection needs, for example, taking into account the type of personal data to be protected.[1]

14 In *Quoine Pte Ltd* [2022] SGPDPC 2 ("***Quoine***"), while the organisation had conducted periodic security reviews, these security reviews were improperly scoped and failed to include a particular account. The organisation explained that its current staff were not aware of the reasons for the affected account's set-up and security arrangements, as the account had been created "*at some time in the past (so legacy)*". This explanation did not excuse the

[1] *Everlast Projects Pte Ltd and others* [2020] SGPDPC 20 (at [21]).

organisation's breach of the Protection Obligation. The Commission found that it was incumbent on the organisation to have implemented the necessary systems and processes to ensure that critical information about its systems, including legacy systems, survived the turnover of its staff (*Quoine* at [23]).

15 Similarly, while Agape had carried out periodic security reviews, these reviews failed to cover the Internet-facing Online Drive. Agape admitted that this omission was because the use of the Online Drive had been a legacy feature unique to Agape's engagement by FHG, which was not implemented for any of Agape's other clients. As a result of this omission, Agape failed to review and assess the Online Drive's security implications and risks.

16 When the Online Drive was installed in December 2017, it was protected by a password which met Agape's password complexity policy (i.e. 8 to 10 characters with a mix of upper and lower-case characters, numbers and symbols). However, at the time of the Incident, the password for Agape's Online Drive had been inadvertently disabled for an estimated 20 months (since December 2019), the cause of which could not be established. Agape admitted that this caused the Online Drive to become an open directory listing on the Internet with no password protection, and highly vulnerable to unauthorised access, modification and similar risks over an excessive period of time.

17 If Agape's periodic reviews had been properly scoped to cover all of the IT components under its Services rendered to FHG (including the Online Drive), this lapse could have been detected and rectified timeously.

Inadequate password policy and management

18 In the course of investigations, Agape also admitted that prior to the password being disabled in December 2019, it had been shared by Agents to access the Online Drive. In *Terra Systems Pte. Ltd*. [2021] SGPDPC 7[2], the Commission highlighted the data protection risks associated with multiple users sharing a common password, including greater risks of unauthorised access by ex-staff and inadvertent disclosure to threat actors through social engineering, among others.

19 The use of a common password among all Agents was exacerbated by the fact that there was no expiry date set for the password. The failure to implement and enforce reasonable password management policies increased the vulnerability of the Customer Data on the Online Drive to unauthorised access and other similar risks, even before the password had been disabled.

20 For the above reasons, Agape was determined to have breached the Protection Obligation.

Whether FHG had contravened Section 24 of the PDPA

Failure to exercise reasonable oversight of vendor

21 Under Section 4(3) of the PDPA, an organisation that engages a data intermediary to process personal data on its behalf, bears the same obligations under the PDPA as if the personal data was processed by the organisation itself. This is so, even where the organisation

[2] This decision was subsequently subjected to reconsideration by the Commission. In *Terra Systems Pte Ltd* [2022] SGPCPCR 1, the Commissioner affirmed the finding of the organisation's breach of Section 24 of the PDPA and the financial penalty imposed.

engages the data intermediary to implement the necessary data protection measures in relation to the personal data (*Social Metric Pte Ltd* [2017] SGPDPC 17 at [15]).

22 The Commission has reiterated in past decisions, such as *SCAL Academy Pte. Ltd.* [2020] SGPDPC 2, that the Protection Obligation requires organisations to exercise reasonable oversight of their vendors.

23 Specifically in the context of an organisation's relationship with its data intermediary, the organisation (i.e. the data controller) has a supervisory or general role for the protection of the personal data, while the data intermediary has a more direct and specific role in the protection of personal data arising from its direct possession or control over the personal data. This means that a data controller may be found in breach of the Protection Obligation, even though its data intermediary may not be found in breach, and vice versa (*Social Metric Pte Ltd* [2017] SGPDPC 17 at [16]).

24 In this case, FHG engaged Agape as its data intermediary to carry out the Services using the personal data provided by FHG. Under the Protection Obligation, FHG was required to exercise reasonable oversight of Agape's data processing activities.

25 In *SCAL Academy Pte. Ltd.* [2020] SGPDPC 2 (at [8]), even though the organisation in question had instructed its vendor to prevent certain documents from being 'leaked' online, it did not check what security arrangements the vendor had implemented to ensure this. This hindered the organisation and vendor from being able to identify any data protection risks and

agree on the measures to be implemented to protect against unauthorised disclosure of the personal data in the documents.

26 In this case, due consideration is given to the fact that FHG had conducted a high-level IT due diligence review of Agape prior to its decision to onboard Agape as a vendor, and that FHG's written agreement with Agape required the latter to comply with the PDPA including, among others, obligations to take all appropriate and reasonable administrative, physical and technical safeguards, and security arrangements. Nevertheless, FHG's failed to exercise reasonable oversight through regular monitoring of Agape's personal data handling processes throughout the engagement, including how Agape stored and granted Agents' access to the Customer Data.

27 In this regard, there was a point of contention between the parties over whether FHG was aware of and permitted the uploading of the Customer Data from Agape's Computer to the Internet-facing Online Drive.

28 According to FHG, its understanding with Agape was that the local copy of the Customer Data on the Computer was only to be used for emergency or exceptional situations such as when Agape was unable to connect to FHG's SharePoint during any system downtime or disruptive event. No other copies of the Customer Data were to be made by Agape, whether from the SharePoint or the local copy on the Computer. FHG stated that it did not provide Agape with permission to upload the Customer Data from Agape's Computer to the Online Drive.

29 In contrast, Agape asserted that FHG was aware that the Agents were inmates operating from inside Changi Women's Prison, and that there were IT restrictions preventing them from accessing the Customer Data directly from FHG's Sharepoint. As such, Agape had downloaded and uploaded the Customer Data onto its Online Drive for the Agents to access and use. Agape asserted that FHG was aware of Agape's process of sharing Customer Data with the Agents as FHG's representatives had been present during "dry runs".

30 While there was insufficient contemporaneous evidence to support either party's version of events, the fact remains that FHG was aware that Agape was engaging inmates from inside Changi Women's Prison to carry out the Services, and the Commission's findings regarding FHG's breach of the Protection Obligation are not dependent on whether FHG permitted Agape to upload the Customer Data to the Online Drive or not.

31 Given that FHG was aware that access to the Customer Data would have to be granted to a third party that was offsite for the provision of the Services, FHG should have made reasonable enquiries to ascertain how the Customer Data was to be stored and transmitted, and how access to the Customer Data would be controlled. Had FHG made these enquiries and discovered the true state of affairs, they would have no doubt required Agape to implement stricter controls to regulate Agents' access and use of the Customer Data. By failing to make such enquiries, FHG failed to appreciate the reality of how Agape was storing, transmitting, and retaining the Customer Data, and failed to exercise reasonable oversight over Agape's data processing activities.

Unnecessary disclosure of sensitive personal data

32 Separately, FHG inadvertently disclosed personal data only intended for its employees' internal use, onto the SharePoint system shared with Agape. This included sensitive financial information such as bank account numbers and bank codes, and health information such as ICD codes and codes for surgical procedures done in hospitals. These datasets were not required by Agape for the performance of the Services, and this inadvertent disclosure ultimately led to a greater loss of personal data during the Incident.

33 When an organisation discloses more personal data than is needed for its purposes, this creates unnecessary data security risks, particularly where such data is more sensitive in nature[3].

34 In the Commission's Guide to Data Protection Practices for ICT Systems[4] (at page 11), data minimisation has been encouraged as a good way for organisations to examine what personal data is really needed. It should be a basic data protection practice for organisations to collect, use, or disclose only the least sensitive types of personal data if different types of personal data can be used to achieve the same purpose.

35 FHG should have implemented robust measures to ensure that only personal data necessary for performance of the Services was shared with Agape, and in particular, that sensitive personal data was not inadvertently disclosed.

[3] *Habitat for Humanity Singapore Ltd* [2018] SGPDPC 9 (at [19]-[20])
[4] Published on 14 September 2021. The Guide compiles data protection practices from past Advisory Guidelines, Guides and data breach cases that should be adopted by organisations in their ICT policies, systems and processes.

36 In view of the above, FHG was determined to have breached the Protection Obligation in respect of the Customer Data.

Voluntary measures implemented by FHG and Agape

37 Following the Incident, FHG and Agape have voluntarily taken or will be taking the following steps to prevent a recurrence of the Incident or similar events:

FHG

(a) Agents will now access FHG's customer data directly from FHG's SharePoint via individual user accounts with multi-factor authentication;

(b) FHG's SharePoint has been reconfigured to grant "view-only" access to only the specific files required by vendors for the services to be provided, with clear segregation between the vendor's SharePoint files and FHG's internal SharePoint files;

(c) FHG will formally communicate its internal personal data protection policies and processes to vendors in order for them to be applied to the vendors' processing of personal data on FHG's behalf;

(d) FHG will enhance its contracts with vendors to include additional data protection obligations, such as the requirement for vendors to undergo regular vulnerability assessments and penetration testing, rights for FHG to audit the vendor's data processing practices, and requirements for vendors to have in place reasonable data breach response management processes;

Agape

(e) With the assistance of external cybersecurity consultants, Agape has refreshed its data protection and IT policies; and

(f) Agape has increased data protection awareness by requiring employees to go through the assessment tools provided on the Commission's website, enrolling employees in Workforce Skills Qualifications PDPA courses for certification, and regularly conducting internal communications to maintain cybersecurity vigilance.

The Commissioner's Decision

38 In determining whether any directions should be imposed on FHG and Agape under Section 48I of the PDPA, and/or whether they should be required to pay a financial penalty under Section 48J of the PDPA, the factors listed at Section 48J(6) of the PDPA and the following mitigating factors were taken into account:

Mitigating Factors

(a) FHG and Agape were cooperative during the investigations;

(b) FHG and Agape voluntarily admitted to their breaches of the Protection Obligation under the Commission's Expedited Decision Procedure; and

(c) FHG and Agape took prompt remedial actions following discovery of the Incident.

39 While Agape's breaches of the Protection Obligation were more causally proximate to the unauthorised access and disclosure of personal data in the Incident, FHG's inadvertent disclosure of financial and health related data resulted in the impact of the Incident being

amplified. As the data controller, FHG also bore the ultimate responsibility to exercise due diligence and reasonable supervision over Agape. For the purposes of assessing what amount of financial penalty would be proportionate and effective as a deterrent, it was also taken into consideration that FHG's annual turnover based on its latest available audited accounts, was almost 50 times higher than that of Agape's.

40 Having carefully considered all the relevant circumstances, the Commissioner hereby requires that:

(a) FHG pay a financial penalty of $58,000; and

(b) Agape pay a financial penalty of S$10,000;

within 30 days of the date of the relevant notices 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.

41 In quantifying the financial penalties imposed, no weight was placed on Agape's status as a social enterprise. The standard of security arrangements expected under the Protection Obligation will depend on the volume and nature of personal data in the organisation's possession or control, regardless of whether the organisation is a for-profit business, a charity, or a social enterprise[5].

42 In addition to the financial penalties imposed, FHG and Agape are also directed to do the following:

[5] See *Singapore Red Cross Society* [2020] SGPDPC 16 at [10]

FHG

(a) Within 60 days from the date of this decision:

i. Review processes and contractual obligations with Agape and existing vendors processing personal data on behalf of FHG, to ensure that such vendors have sufficiently robust data handling processes to protect personal data in their possession and/or control;

ii. Review existing internal processes to ensure that only personal data necessary for fulfilling contractual obligations is disclosed to vendors via secured channels and with reasonable access controls considering the type and volume of personal data being disclosed; and

(b) Notify the Commission within 14 days of the completion of the reviews above, with an outline of their scope.

Agape

(c) Within 60 days from the date of this decision:

i. Ensure that the scope of its periodic security reviews and any security audits include the protection of personal data handled in all of Agape's systems and processes;

ii. Resolve and record in writing with FHG the data protection requirements and job specifications for the processing of personal data on behalf of FHG, including arrangements for the exercise of regular oversight by FHG to verify that the requirements and specifications are being met; and

(d) Notify the Commission within 14 days of the completion of the reviews above, with an outline of their scope.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION