PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPC 10

Case No. DP-2209-C0193 / DP-2209-C0217

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

And

Ascentis Pte. Ltd.

… Organisation

DECISION

Data Protection *– Protection Obligation – Unauthorised disclosure of personal data – Insufficient administrative and technical security arrangements*

Data Protection *– Data intermediary – Obligations of organisation and data intermediary*

Ascentis Pte. Ltd.

Wong Huiwen Denise, Deputy Commissioner - Case No. DP-2209-C0193 / DP-2209-C0217

12 September 2023

Introduction

1 On 13 September 2022, the Personal Data Protection Commission (the **"Commission**") was notified by the Singapore Computer Emergency Response Team that the personal data of 332,774 individuals had been exfiltrated from an eCommerce platform (the "**Platform**") owned by Starbucks Coffee Singapore Pte Ltd ("**Starbucks SG**") and offered for sale online (the "**Incident**").

2 The Commission commenced investigations to determine whether the circumstances of the Incident disclosed any contraventions of the Personal Data Protection Act 2012 ("**PDPA**"). For the reasons set out below, the Commission determined that the developer of the Platform, Ascentis Pte Ltd ("**the Organisation**") had contravened section 24 of the PDPA ("**the Protection Obligation**") in the context of the Incident.

3 The Organisation requested and agreed for the investigation to be handled under the Commission's Expedited Breach Decision Procedure, and voluntarily provided and admitted to the facts set out below. The Organisation also admitted that it had failed to implement reasonable security arrangements to protect the personal data exfiltrated during the Incident, in breach of the Protection Obligation.

4 The Commission also accepted a voluntary undertaking from Starbucks SG pursuant to section 48L(1)(a) of the PDPA for Starbucks SG to implement enhanced security arrangements to improve its compliance with the PDPA[1]. No further enforcement action was taken against Starbucks SG.

Facts of the Case

The CRM System and CRM Database

5 The Organisation is in the business of developing, providing and integrating software solutions for Customer Relationship Management and eCommerce.

6 On 19 December 2014, Starbucks SG engaged the Organisation to develop, implement, support, and host a Customer Relationship Management system (the "**CRM System**") to support Starbucks SG's "My Starbucks Rewards" loyalty program (the "**Rewards Program**").

7 When an individual signed up as a member of the Rewards Program, their personal data including name, email address, telephone number, and birth date was collected and stored on a cloud database (the "**CRM Database**").

The Project for development of the Platform

8 On 14 September 2020, Starbucks SG engaged the Organisation to separately develop and provide, as well as render ongoing technical support for, the Platform, an online store for the sale and purchase of products offered by Starbucks SG ("the **Project**").

[1] A copy of Starbucks SG's voluntary undertaking is available at https://www.pdpc.gov.sg/Undertakings.

9 In turn, on 1 January 2021, the Organisation engaged one Kyanon Digital Co. Ltd ("**Kyanon**"), a company based in Vietnam in the business of software development and provision, to provide additional manpower and software development support to the Organisation for its execution of the Project.

10 One of Starbucks SG's requirements for the Project was for a Rewards Program member's personal data to be auto-completed in electronic forms on the Platform, such that the member would not have to manually key in his/her personal data to complete a transaction on the Platform.

11 The personal data of Rewards Program members was originally only stored on the CRM Database (and not on the Platform). In order to make it more convenient for members to use the Platform, the Organisation implemented a process to automatically synchronise a member's personal data from the CRM Database to the Platform whenever an individual logged in as a member on the Starbucks SG website and then visited the Platform. This synchronisation occurred in real-time. Once the synchronisation was complete, the member's personal data would exist separately in a database within the Platform. Both the CRM Database and the database within the Platform were hosted and operated independently.

Kyanon's involvement in the Project

12 Despite Kyanon's engagement, the Organisation maintained control and management of, and had direct involvement in, the Project. The leader of the team delivering the Project (the "**Project Team**"), was an employee of the Organisation, while the remaining personnel comprising the Project Team were employees of Kyanon (the "**Kyanon Employees**")

13 The Kyanon Employees were provided with accounts to the Platform with full administrative privileges (the "**Admin Accounts**"). These enabled the Kyanon Employees to support, check and perform configuration of the Platform, troubleshoot any technical problems, and check if data received on the Platform had been synchronised correctly. The Admin Accounts also granted rights to Kyanon Employees to export data from the Platform (the significance of which is discussed below). Prior to the Incident, the Admin Accounts did not require multi-factor authentication ("**MFA**").

14 One of the Kyanon Employees, "Peter", left the employ of Kyanon in May 2022. He handed over the credentials to his Admin Account ("**Peter's Admin Account**") to the remaining members of the Project Team via a shared Google Sheet. Despite the cessation of Peter's employment with Kyanon, Peter's Admin Account was not disabled. Rather, the Kyanon Employees changed the password of Peter's Admin Account to "Kyanon@123456", updated the shared Google Sheet with the new password, and continued using Peter's Admin Account among themselves.

The Incident

15 Sometime between 10 and 13 September 2022, a malicious actor used Peter's Admin Account to gain access to the Platform, where the personal data of those Rewards Program members who had previously logged into the Platform was stored. The Organisation was not able to determine the exact method by which the malicious actor gained access to Peter's Admin Account; it was possibly through the abovementioned shared Google Sheet. The malicious actor granted other accounts administrative privileges, performed data gathering, and exported the gathered data to an external email address.

16 In total, the personal data of 332,774 individuals stored in the Platform comprising names, email addresses, dates of birth, membership details relating to the Rewards Program, last login dates to the Platform, the physical addresses of 181,875 individuals, and the telephone numbers of 310,560 individuals ("**Subject Data**") was exfiltrated in the Incident.

17 The Subject Data was subsequently advertised for sale on an online forum on the dark web. The Commission was notified of the same by the Singapore Computer Emergency Response Team on 13 September 2022. Starbucks SG and the Organisation submitted data breach notifications to the Commission on 15 and 16 September 2022, respectively.

Remedial Actions

18 After being notified of the Incident, the Organisation took remedial actions which included:

(a) Activating an emergency response team and establishing an investigation team (including an external cybersecurity firm) to investigate the Incident;

(b) Disabling access to the Platform by all accounts, validating all Platform accounts, and resetting all administrator accounts;

(c) Blocking the malicious actor's IP address in the Platform firewall;

(d) Mandating that all vendors, including Kyanon, perform full anti-virus and malware scans, and provide reports of these scans to the Organisation before resuming work; and

(e) Implemented MFA for all its accounts

Findings and Basis for Determination

Whether the Organisation had contravened the Protection Obligation

19 Under the Protection Obligation, an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks.

20 The Protection Obligation also applies to data intermediaries[2]. A data intermediary is defined under section 2(1) of the PDPA as "*an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation*". In turn, the "*processing*" of personal data is defined as:

> "*in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:*
>
> *(a) recording;*
>
> *(b) holding;*
>
> *(c) organisation, adaptation or alteration;*
>
> *(d) retrieval;*
>
> *(e) combination;*
>
> *(f) transmission;*
>
> *(g) erasure or destruction;"*[3]

21 As the developer and host of the CRM System and the Platform, the Organisation processed personal data (including the Subject Data) in the CRM Database and the Platform

[2] Section 4(2) of the PDPA.
[3] Section 2(1) of the PDPA.

on Starbucks SG's behalf. Accordingly the Organisation was a data intermediary of Starbucks SG and was subject to the Protection Obligation in respect of the Subject Data.

22 The reasonableness of an organisation's security arrangements would be assessed having regard to the volume and sensitivity of such personal data and the possible impact of a data breach. As stated in the Commission's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 16 May 2022) ("**Advisory Guidelines**") at paragraphs 17.3(a) and (b), an organisation should:

> *"a) design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;*
>
> *...*
>
> *c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of security*
>
> *..."*

23 Additionally, as stated in the Commission's *Guide to Data Protection Practices for ICT Systems* ("**ICT Systems Guide**") at page 8:

> *"For organisations that hold large quantities of different types of personal data or data that might be more sensitive to the individuals or the organisations, they should additionally implement the relevant enhanced practices suggested in each section. The design and implementation of these protection measures should always take into consideration the extent of the sensitivity of the data based on the nature of business and types of services offered."*

24 In the present case, having regard to the large volume of personal data hosted in the Platform, reasonable security arrangements to protect the Subject Data were not implemented. The Commission sets out the reasons for this finding in the paragraphs below. In particular, the Organisation failed to disable Peter's Admin Account after he was no longer working on the Project.

25 In the ICT Systems Guide, the Commission recommends at page 15 that organisations should, as a basic practice, conduct "*Regular review of user accounts to ensure that all the accounts are active and the* ***rights assigned are necessary*** *(i.e****. remove user accounts when a user has left the organisation or update the user's rights when he/she has changed his/her role within the organisation****).*" (emphasis added in bold).

26 In this case however, the Organisation did not disable Peter's Admin Account after he left the employ of Kyanon but permitted its continued use by Kyanon Employees. While Peter was an ex-employee of Kyanon and not of the Organisation, it was nevertheless (by the Organisation's own admission) the Organisation itself which retained responsibility for the development and management of the Platform, including the creation and management of administrator accounts. The Organisation admitted that the failure to disable Peter's Admin Account was a "*lapse*" on its part, and further admitted that it failed to create new accounts for the Kyanon Employees who took over Peter's duties.

27 The failure to disable Peter's Admin Account was exacerbated by the fact that the account was not protected with a sufficiently complex password. Having taken over Peter's Admin Account, the Kyanon Employees changed the password to "Kyanon@123456" (the "**New Password**"). The Organisation informed the Commission that the New Password met the

Platform's password complexity requirements, namely that passwords be at least 8 characters in length, have at least 1 upper and 1 lower case letter, at least 1 special character, and not be a repeat of the account's previous 5 passwords.

28 The Commission has made clear in previous enforcement decisions that mere technical compliance with password complexity requirements is not good enough if the password remains guessable[4]. Although the New Password complied with the Platform's password complexity requirements, it incorporated the name "Kyanon" and a sequential series of digits ("123456"). This made the New Password easily guessable and insecure.

29 Further, the sharing of credentials for Peter's Admin Account via a shared Google Sheet meant that anyone who obtained access to the said Google Sheet could gain access to Peter's Admin Account. As the Commission has stated in the ICT Systems Guide at page 16, an organisation should "*[h]ave clear policies that prohibit the sharing of passwords such as admin credentials*". Such sharing posed a heightened risk of unauthorised access especially if a malicious actor was familiar with Peter's user ID.

30 The Organisation stressed to the Commission that passwords for accounts to the Platform were hashed, and that the Organisation was unaware of the New Password. Further, the Organisation stated that Peter's Admin Account was used by Kyanon Employees and not the Organisation's employees, and that the New Password was set by the Kyanon Employees using Peter's Admin Account.

[4] *Re Chizzle Pte Ltd* [2020] SGPDPR 1 at [5(d)].

31 While the immediate cause for the weak New Password and insecure sharing of the credentials for Peter's Admin Account may have been the Kyanon Employees, the Organisation could have managed this better by specifying clearer data protection requirements to Kyanon as part of its involvement in the Project, including in relation to account management.

32 While the Master Services Agreement between the Organisation and Kyanon dated 1 January 2021 did impose broad data protection obligations on Kyanon, it did not mandate any specific measures in relation to account management, beyond stating that "*secure authentication and authorisation processes*" were to be implemented.

33 In addition, Kyanon had provided the Organisation with a signed Letter of Undertaking in which Kyanon undertook to comply with "*the standards in relation to personal data protection, including those required under the Personal Data Protection Act (No. 26 of 2012) of Singapore (the "PDPA Policy")*", the Organisation's Security and Services Guide, and the Organisation's Personal Data Handling and Measures. However, these documents did not specify any specific requirements for the disabling of ex-employee accounts.

34 Taking into consideration the above, the Commission finds the Organisation in breach of the Protection Obligation for failing to disable Peter's Admin Account after Peter was no longer a Kyanon employee.

Observations on other data protection practices

35 Separate to the above finding (which the Organisation admitted to), the Commission sets out observations on two other data protection practices which, if implemented, could have

prevented the unauthorised disclosure of personal data in the Incident even if Peter's Admin Account had not been disabled. For the avoidance of doubt, these observations are made solely to provide guidance, and (i) do not constitute additional findings of breaches of the Protection Obligation by the Organisation in this case, or (ii) factor in any way in the Commission's final decision in this case.

Scoping of rights assigned to Admin Accounts

36 All Admin Accounts assigned to Kyanon Employees were granted rights to export data from the Platform, even though such rights may not have been necessary for their work on the Project.

37 As stated in the ICT Systems Guide (page 15) and paragraph 25 above, the Commission recommends regular review of user accounts to ensure that only the necessary rights are assigned. The Commission has previously found organisations in breach for failing to carry out such review.[5]

Implementation of MFA for Admin Accounts

38 The level of privileges granted to all Admin Accounts created a heightened risk that large volumes of personal data could be exfiltrated from the Platform if an Admin Account was compromised. This risk was exacerbated by the fact that the Admin Account did not require MFA. In *Lovebonito Singapore Pte. Ltd.* [2022] SGPDPC 3, the Commission made clear that MFA should be implemented as ***a baseline requirement*** for administrative accounts with access to confidential or sensitive personal data or large volumes of personal data.[6]

[5] *RedMart Limited* [2022] SGPDPC 8 at [19].
[6] *Lovebonito Singapore Pte. Ltd.* [2022] SGPDPC 3 at [51].

39 In this case, the Organisation explained that while it had plans to implement MFA for the Admin Accounts (as part of unified access controls), these plans were delayed due to manpower shortages caused by the COVID-19 pandemic.

40 While the Commission recognises the business difficulties brought on by the COVID-19 pandemic, implementation of MFA for the Admin Accounts could nevertheless have been given greater priority considering the volume of personal data accessible from the Platform, and the associated heightened data protection risks.

41 It was not necessary for the Commission to make breach findings in relation to the above two data protection practices in this case. However, the Commission will not hesitate to find organisations in future enforcement cases in breach of the Protection Obligation for failing to implement the same – particularly in cases involving unauthorised use of administrative accounts with access to sensitive or large volumes of personal data.

The Commission's Decision

42 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 Commission took into account the factors listed at section 48J(6) of the PDPA.

43 The Commission notes that the personal data of 332,774 individuals was affected in the Incident and that this largely consisted of basic contact and account membership information.

44 The Commission also recognises that:

(a) the Organisation was cooperative with the Commission's investigations;

(b) the Organisation took prompt remedial actions to address the Incident;

(c) the Organisation has not previously been found to have breached the PDPA; and

(d) the Organisation had voluntarily accepted responsibility for the Incident, thus facilitating the expeditious investigation and resolution of this case through the Commission's expedited breach procedure.

45 Having considered all the relevant factors in this case, the Commission hereby requires the Organisation to pay a financial penalty of $10,000 within 30 days from the date of the relevant 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.

46 No further directions are necessary on account of the remedial measures already taken by the Organisation.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION