PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPC 12

Case No. DP-2205-B9761

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

And

PPLingo Pte Ltd

… *Organisation*

DECISION

PPLingo Pte. Ltd.

Lew Chuen Hong, Commissioner — Case No. DP-2205-B9761

24 October 2023

Introduction

1 On 8 May 2022, PPLingo Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a data breach incident involving unauthorised access to personal data contained within the Organisation's online education platform (the "**Incident**").

2 The Commission commenced investigations to determine the Organisation's compliance with the Personal Data Protection Act 2012 ("**PDPA**") in relation to the Incident.

3 The Organisation requested for this matter to be handled under the Expedited Breach Decision Procedure, which the Commission acceded to. To this end, the Organisation voluntarily and unequivocally admitted to all the facts set out in this decision, and also to contraventions of Sections 11(3) and 24 of the PDPA (as explained below).

Facts of the Case

4 The Organisation is a company incorporated in Singapore and operates an online Chinese and English language learning platform that offers virtual classes to its students aged 4 to 15 years old globally ("**LingoAce**").

5 The LingoAce platform incorporates an operations support system ("**OPS System**") which provides teacher management, student management and class scheduling management functions. The personal data of the Organisation's students, parents, teachers and other staff (including teachers and staff formerly employed by the Organisation) ("**Users**") was stored in the OPS System.

6 At the time of the Incident, the Organisation had in place a written data protection policy and had implemented certain security measures for the LingoAce platform, including network access control measures, and firewall protection for the OPS System. The Organisation had also organised two rounds of internal security awareness training for its IT development team in April 2022, one month before the Incident.

The Incident

7 The Organisation engaged a private forensic expert ("**PFE**") to ascertain the cause and extent of the Incident. The PFE's forensic investigations revealed that sometime between 26 April 2022 to 27 April 2022, the threat actor obtained the password of an administrator account of the Organisation's OPS System

("**Compromised Admin Account**") via brute force attacks[1]. The password of the Compromised Admin Account was "*lingoace123*".

8 Using the Compromised Admin Account, the threat actor created several new accounts with administrator privileges to the OPS System, and used these newly created accounts to access the personal data of the Users.

9 A total number of 557,144 Users were assessed to be affected by the Incident. The breakdown of the volume and type of personal data accessed by the threat actor is set out in the table below:

Category of Individuals	**Number of Individuals**	**Types of Personal Data Affected**
Students	303,238	Name, date of birth, gender, avatar link (including photos, where provided), native language, learning experience & skills
Parents	244,021	Name, username, mobile phone number, email address, nationality, country & region, residing country, avatar link (including photos, where provided), Whatsapp/Wechat ID, account class credit balance, address

[1] Brute force attacks also include dictionary attacks.

Teachers (including ex-teachers)	9,395	Name, username, mobile phone number, email address, nationality, gender, photo (where provided), country of residence, date of birth, teacher ID, salary, bank name and account number, signature, Chinese resident identity card number, labour agreement or independent contractor agreement, Whatsapp/Wechat ID, educational background
Other Staff (including ex-staff)	490	Name, username, mobile phone number, email address, Wechat ID
Total	**557,144**	

10 Although the threat actor had accessed the personal data of the Users, there was no evidence of any data modification or exfiltration.

11 On 5 May 2022, the threat actor gained unauthorised access to email accounts of the Organisation's employees through unidentified means. The threat actor accessed an email account belonging to one of the Organisation's employees and sent an email to the Organisation ("**Email**"). In the Email, the threat actor informed that he had accessed LingoAce platform's systems and set out the personal data of a few

Users in the text to prove this. Nonetheless, the threat actor did not follow up with any further communication or make any subsequent demands to the Organisation.

Remedial actions

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

Actions to mitigate and contain the Incident

(a) Engaged a third party PFE to assist in investigations and remedial measures;

(b) Inspected the servers related to the OPS System to detect any further intrusion;

(c) Reset passwords of all administrator accounts and removed unnecessary administrator accounts;

(d) Implemented two-factor authentication for all accounts accessing the OPS System;

(e) Implemented enhanced password strength/complexity requirements for accounts accessing the OPS System;

(f) Appointed a Data Protection Officer ("**DPO**"); and

(g) Notified all the affected Users.

Actions to prevent recurrence or similar incidents

(a) Implemented two-factor authentication for all email accounts of the Organisation;

(b) Signed up for services of a third-party platform to test for bugs of the OPS System and improve bug discovery capabilities;

(c) Adopted Data Full Life Cycle Security Specifications relating to the collection, transmission, storage, usage and destruction of data;

(d) Carried out audits and monitoring of the OPS System and enhanced the protection of the application firewall;

(e) Reset passwords to strengthen the passwords or implementing two-factor authentication for other related systems connected to the LingoAce platform; and

(f) Enhanced the Organisation's internal security and data protection training programme, and increased the frequency of security and data protection training for the Organisation's staff.

Findings and Basis for Determination

13 Based on the circumstances of the Incident, the Commission's investigation centred on whether the Organisation had breached its obligations under Section 24 of the PDPA 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**").

14 As the Organisation indicated that it had not appointed a DPO when notifying the Commission of the Incident, the Organisation's compliance with Section 11(3) of the PDPA (the "**Accountability Obligation**") was also investigated.

Breach of the Protection Obligation by the Organisation

15 To comply with the Protection Obligation, an organisation must implement security arrangements that are reasonable and appropriate in the circumstances. This includes the nature of the personal data in the Organisation's possession and control, as well as the potential impact that unauthorised disclosure of the personal data might have on the affected persons[2].

16 Given the high volume and sensitivity of the personal data contained in the OPS System (including financial information such as bank name and account number and students/minors), the onus was on the Organisation to implement an appropriately robust level of security arrangements to discharge its obligation under the Protection Obligation.

[2] See the Commission's Advisory Guidelines on Key Concepts in the PDPA (Revised 16 May 2022), at [17.2].

Inadequate password policy

17 As a necessary measure of data protection, organisations must adopt, implement, and enforce a strong password policy[3]. A password policy that mandates a minimum level of password complexity, and a fixed period of password validity or regular change of passwords, amongst others, are basic practices of proper authentication and authorisation processes[4]. This can include implementing password controls such as (i) requiring a change of password upon first logon, (ii) minimum password length, (iii) restricting reuse of previous passwords, and (iv) mandating a minimum level of password complexity. A robust password policy is a key security measure that an organisation must have in place to ensure that its IT systems are not vulnerable to common hacking attempts such as brute force attacks[5].

18 Investigations disclosed that the Organisation did not have any password policy for the Compromised Admin Account, other than requiring a minimum length of 8 characters for passwords. Given the Compromised Admin Account granted privileged access to the Organisation's OPS System, this was an inadequate security arrangement to safeguard the personal data contained in the OPS System.

i. No expiry / requirement to change passwords

19 The use of the OPS system commenced in March 2020. The password

[3] See *Congita Asia Holdings Pte Ltd* [2022] SGPDPCS 14.
[4] See the Commission's Guide to Data Protection Practices for ICT systems.
[5] See *LoveBonito Singapore Pte Ltd* [2022] SGPDPC 3, at [18].

"*lingoace123*" was in use since then and remained unchanged for more than 2 years prior to the Incident.

20 This was a serious lapse in the Organisation's password management practices, which failed to provide for a fixed period of password validity or require regular change of passwords to mitigate risks of unauthorised access. The absence of such security arrangements meant that the OPS System was vulnerable to brute force attacks.

ii. No requirements on password complexity

21 Further, the Organisation failed to implement requirements to provide for an adequate level of password complexity. This would have contributed to the ease of brute force attempts by the threat actor to gain access to the Compromised Admin Account.

22 The PFE's forensic investigations support the Commission's findings, as it identified that the password for the Compromised Admin Account did not meet typical industry best practices for password strength, in terms of appropriate length, and combination of numbers, symbols, and/or uppercase and lowercase characters.

Guessable phrases / components in the password

23 The password "*lingoace123*" was also a weak password due to its incorporation of both the Organisation's name and a common sequence of numbers (i.e. "123"). Such a password would be vulnerable to brute force attacks by threat actors.

24 In *Re Chizzle Pte Ltd* [2020] SGPDPCR 1, the password "Chi!zzle@2018" which complied with the organisation's password complexity rules was nevertheless held to be a weak password as it incorporated the organisation's name as well as the year "2018". The same concern has been repeated in the Commission's Guide to Data Protection Practices for ICT systems ("**Guide**"), stating that the use of an organisation's name as a component of the password is not recommended because it is not difficult to guess and be cracked by hackers.

25 The Organisation accepted that the password was a weak one, which left the OPS system vulnerable to brute force attacks.

26 As a result of the above weaknesses, the threat actor successfully obtained the password of the Compromised Admin Account of the OPS System, via brute force attacks.

27 For the above reasons, the Organisation is found to have negligently breached the Protection Obligation by failing to implement adequate security arrangements in respect of the Compromised Admin Account.

Two-factor / multi-factor authentication ("2FA / MFA")

28 At the time of the Incident, the Organisation had not implemented a password policy requiring two-factor ("**2FA**") or multi-factor authentication ("**MFA**") in respect of the Compromised Admin Account. As the Incident happened shortly before the Commission's decision in *Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 ("*Lovebonito*") was published, this will not be taken into account as a basis for breach of the Protection Obligation in this case. However, the baseline standard described by the Commission at [51] of *Lovebonito* bears repeating:

> *"(a) First, 2FA / MFA should be implemented as* ***a baseline requirement for administrative accounts to systems that hold personal data of a confidential or sensitive nature, or large volumes of personal data****: see [46]-[47] above. Failure to do so can ipso facto amount to a breach, unless the organisation can show that its omission is reasonable or implementation of 2FA is disproportionate.*
>
> *(b) Second,* ***remote access by privileged accounts to information systems that host confidential or sensitive personal data, or large volumes of personal data, should a fortiori be secured by 2FA / MFA****. The risks concerning remote access are higher, thus the expectation to implement 2FA / MFA will correspondingly increase.*
>
> *(c) Third, organisations using IT systems to host confidential or sensitive personal data, or large volumes of personal data, are expected to enable and*

configure 2FA / MFA, if this is a feature that is available out-of-the-box. Omission to do so may be considered an aggravating factor."

[emphasis added]

29 As 2FA / MFA becomes more readily available at lower cost, organisations should expect the baseline standard described in *Lovebonito* to rise. An organisation choosing not to implement 2FA / MFA will have to explain why this is reasonable, considering for example, costs, the organisation's circumstances, and the level of data protection risks.

Other enhanced data protection practices

30 The Commission's Guide recommends two tiers of (i) basic and (ii) enhanced data protection practices for organisations to adopt in different circumstances.

31 While the Organisation is not faulted for not implementing enhanced data protection practices (and this has not been taken into account in determining the enforcement action in this case), it is observed that implementing the other enhanced data protection practices in the Commission's handbook on *How to Guard against Common Types of Data Breaches*[6] could have prevented or slowed down brute force attacks. For example, the Compromised Admin Account could have been locked after

[6] See the Commission's recent release of the handbook on common causes of data breaches in *How to Guard against Common Types of Data Breaches* published on 24 May 2021 (at page 13).

a pre-defined number of failed login attempts, or CAPTCHAs could have been implemented to deter automated login attempts.

32 In any event, organisations must assess whether enhanced data protection practices should be implemented[7] in respect of their security arrangements to protect the personal data (having regard to the volume and sensitivity of such personal data and the possible impact of a data breach) in their possession or control.

Breach of the Accountability Obligation by the Organisation

33 Investigations revealed that the Organisation did not appoint a DPO since its incorporation in 2016.

34 Under Section 11(3) of the PDPA, all organisations are required to designate an individual to be responsible for compliance with the PDPA. Appointing a DPO is a basic requirement of the PDPA.

35 As emphasised in previous decisions of the Commission[8], a DPO plays a vital role in ensuring an organisation's compliance with the PDPA, and the proper implementation of an organisation's data protection policies and practices. The responsibilities of a DPO include, but are not limited to:

(a) Ensuring compliance with the PDPA when developing and implementing policies and processes for handling personal data;

[7] See the Commission's Guide to Data Protection Practices for ICT systems (at page 8).
[8] *Re AgcDesign Pte Ltd* [2019] SGPDPC at [5] & *Re M Stars Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 at [31] to [37].

(b) Fostering a data protection culture and accountability among employees and communicating personal data protection policies to stakeholders;

(c) Handling and managing personal data protection related queries and complaints from the public;

(d) Alerting management to any risks that might arise with regard to personal data; and

(e) Liaising with the Commission on data protection matters, if necessary.

36 A DPO was appointed after the Incident on 18 May 2022, more than 5 years after the Organisation's incorporation.

37 In the circumstances, it is determined that the Organisation had negligently breached the Accountability Obligation for failing to designate a DPO to be responsible for ensuring that the Organisation complies with the PDPA.

The Commissioner's Preliminary Decision

38 In determining whether to give directions (if any) to the Organisation pursuant to Section 48I of the PDPA, and/or whether to impose a financial penalty pursuant to Section 48J of the PDPA, the Commission took into account the relevant facts and circumstances of the case and the factors listed at Section 48J(6) of the PDPA.

39 The Commission noted that the Organisation had been negligent in not complying with its obligations under the PDPA, namely the Protection Obligation and the Accountability Obligation.

40 The Commission also noted that the Incident involved a high volume of personal data, which affected 557,144 individuals. The type of datasets affected were of a higher sensitivity, including personal data of a financial nature and approximately 303,238 minors.

41 The Commission nonetheless recognised the following mitigating factors:

(a) There was no evidence of any exfiltration or misuse of the personal data of the Users;

(b) The Organisation took prompt remedial actions in response to the Incident, including notifying the affected Users;

(c) The Organisation voluntarily admitted that it had breached the Accountability Obligation and the Protection Obligation; and

(d) The Organisation was cooperative during investigations.

42 The Organisation's early admission of liability for its breaches of the Accountability Obligation and Protection Obligation was considered a significant mitigating factor. An organisation that voluntarily accepts responsibility for its non-compliance with the PDPA is an organisation that demonstrates its commitment to its

obligations under the PDPA and shows that it can be responsible for the personal data in its possession or under its control[9].

43 Having considered the above factors and circumstances, the Commissioner preliminarily determined that a financial penalty of $74,000 would be imposed in respect of the Organisation's negligent contraventions of the Accountability Obligation and Protection Obligation. On 27 July 2023, the Organisation was notified of the Commissioner's preliminary decision, including the full findings set out above, and given 14 days to make written representations.

Representations by the Organisation

44 While the Organisation did not challenge the findings and bases of both contraventions, the Organisation made representations seeking that a financial penalty of not more than $35,000 be imposed, for the following reasons:

(a) The Organisation had spent significant capital on its remedial actions and wanted to implement further improvements of IT systems and processes. Any reduction of the financial penalty could be used to fund these further improvements;

(b) The Organisation, in full compliance with its obligations globally, had made voluntary notifications regarding the Incident to other data protection authorities in over 40 other affected locations. These other data protection authorities may also impose financial penalties on the Organisation. To avoid

[9] See Section 11(2) of the PDPA.

"double counting", the Commission should only consider the Singapore-based individuals when assessing the total number of affected individuals rather than the global figures;

(c) Lower financial penalties had been imposed in previous enforcement decisions[10] involving similarly high volumes of personal data.

45 After careful consideration, the Organisation's representations were not accepted for the reasons outlined below:

(a) Under Section 11(2) of the PDPA, the Organisation is responsible for all personal data in its possession or under its control. This is not limited to the personal data of affected individuals / data subjects located within Singapore;

(b) The Commission's enforcement jurisdiction is not fettered by potential enforcement proceedings abroad by other data protection authorities. In any event, the Organisation has not shown how or any evidence that there would be any "double counting"; In any event, as a matter of principle, claiming that the amount that goes towards payment of a financial penalty could be spent on further improvements is not a relevant factor;

(c) Every case is decided on its specific facts and circumstances. In this case, the Organisation had committed two contraventions of the PDPA, and a large volume of minors' personal data was affected which distinguished it from the cases cited.

[10] GeniusU [2022] SGPDPC 1, Eatigo International Pte Ltd [2022] SGPDPC 9, and Redmart Limited [2022] SGPDPC 8.

46 Having considered all the relevant circumstances of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of $74,000 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.

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

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION