# PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2312-C1857

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

And

Air Sino-Euro Associates Travel Pte. Ltd.

… *Organisation*

---

## DECISION

---

# Air Sino-Euro Associates Travel Pte. Ltd.

# [2025] SGPDPC [5]

Lew Chuen Hong, Commissioner — Case No. DP-2312-C1857

31 October 2025

## Introduction

1 Air Sino-Euro Associates Travel Pte Ltd (the "**Organisation**") is a Singapore travel agency that offers outbound travel services to destinations worldwide. On 21 December 2023, the Personal Data Protection Commission (the "**Commission**") was notified of an online news article reporting that a threat actor ("**TA**") had targeted the Organisation and allegedly extracted data from the Organisation during the cyberattack (the "**Incident**"), publicising the incident online. No ransom was sought from the Organisation.

2 The Commission reached out to the Organisation, who confirmed the Incident. The Commission thereafter 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 Decision Procedure ("**EDP**"), which the Commission acceded to.

**The Facts**

4 The Organisation collects personal data of customers for tour group and air ticket bookings for the purpose of making travel arrangements, which are keyed into and stored in its legacy booking system (the "**OB System**"). The Organisation engages a few third-party vendors ("**Vendors**"), one vendor who had developed and maintains the OB System ("**OB Vendor**"), and other vendors who maintain the IT equipment, internet connectivity and security for its servers (collectively, the "**IT Vendors**"). The IT Vendors did not process personal data on behalf of the Organisation.

5 During the material time of the Incident, the Organisation had in place an external facing privacy and data protection policy, but no internal data protection practices or policies. The Organisation had also implemented some security measures, such as firewall protection and administrative access controls, for its servers and endpoint security for its employees' laptops/desktops.

*The Incident*

6 On 20 December 2023, three (3) employees of the Organisation were locked out of their company-issued laptops at separate periods during the same evening and were unable to access their laptops using their login credentials. These were reported to the IT Vendors, who assisted to reset the respective employees' login credentials and performed scans on the affected laptops. Subsequently, the IT Vendors conducted scans on the servers (which included the OB System) and as a precautionary measure, reset the administrative passwords for the servers. No forms of malware, ransomware or abnormalities were detected by the IT Vendors.

7 On 21 December 2023, despite having not discovered malware, ransomware or abnormalities, the IT Vendors reformatted the three affected laptops to completely remove any possible malware, which also removed the past event logs. Separately, on the same day, the Organisation received a media inquiry in relation to an online news article which alleged that there was a successful exfiltration of the Organisation's data, potentially including human resources data, customer information, and company financials.

8 Following from its internal investigations, including engaging a private forensic expert to conduct a review and analysis of the information available on the dark web, the Organisation accepted that the TA had accessed the OB System without authorisation, likely through remote desktop protocol, and that the personal data of 336,759 unique individuals were stored in the OB System and subject to the unauthorised access by the TA. The Organisation also accepted that there was data exfiltration of some personal data. Nonetheless, the TA did not follow up with any subsequent demands to the Organisation in relation to the exfiltrated personal data.

9 The Organisation reported that the OB System contained the following types of personal data from 336,759 individuals in the Organisation's possession or control listed below. The affected data included the following (in various combinations):

(a) Names;

(b) Addresses;

(c) NRIC numbers;

(d) Email addresses;

(e) Dates of Birth;

(f) Phone numbers;

(g) Full images of NRICs / passports / birth certificates (which includes information such as gender, nationality and photograph(s) of the individual); and

(h) Transaction information which includes details such as the amount of money paid to the Organisation, the mode of payment, masked credit card numbers (i.e. only the last 4 out of the 16 numbers are shown), amongst others.

*Remedial actions*

10 In addition to the steps taken at [6] and [7] above to mitigate and contain the Incident, the Organisation also took the following additional remedial actions to prevent recurrence or similar incidents which included:

(a) Disabling of Remote Desktop Protocol ("**RDP**") access for all servers;

(b) Hardening of firewall rules;

(c) Upgrading of its laptop/desktop operating systems from Windows 10 to Windows 11;

(d) Changing of all account passwords; and

(e) Implementation of multi-factor authentication ("**MFA**") for its administrative accounts.

## Findings and Basis for Determination

11 Based on the circumstances of the Incident, the Commission's investigation centered on whether the Organisation had breached its obligations under (a) Sections 11 and 12 of the PDPA (collectively the "**Accountability Obligation**") and (b) 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**").

*Breach of the Accountability Obligation by the Organisation*

12 The Accountability Obligation requires organisations to undertake measures in order to ensure that they meet their obligations under the PDPA and, importantly, demonstrate that they can do so when required[1]. Section 12 of the PDPA is explicit about the specific requirements that the Organisation must develop and implement with respect to its obligations under the PDPA, which states that an organisation must:

(a) develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA;

(b) develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA;

(c) communicate to its staff information about the organisation's policies and practices mentioned in paragraph (a) above; and

[1] See the Commission's Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Revised 16 May 2022) at [21.2].

(d) make information available on request about –

(i) the policies and practices mentioned in paragraph (a) above; and

(ii) the complaint process mentioned in paragraph (b) above.

13 At the time of the Incident, the Organisation only had an external customer-facing privacy and data protection policy. The Organisation accepted that apart from the external-facing privacy policy, it did not put in place any internal processes and/or practices (i.e. complaint-handling process, and data handling policies) to meet its data protection obligations and/or communicate such processes/policies to its employees. The Accountability Obligation requires Organisations to put in place such internal processes or practices to give external data protection policies and practices practical effect.

14 To this end, there are parallels with *Stylez Pte Ltd* [2021] SGPDPC 8, whereby the Commission had found at [13] to [17] that:

> "*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." [emphasis ours as underlined]*

15 Similarly, even though the Organisation had an external facing privacy & data protection policy for its customers, its internal data handling policies and processes were absent and there were no communications of any data protection policies to the Organisation's employees on how to comply with PDPA. The foregoing was inadequate for the Organisation to meet the Accountability Obligation.

16 For the above reasons, the Commission finds that the Organisation has failed to meet its obligations under Section 12 of the PDPA.

17 In addition, the Organisation did not appoint a Data Protection Officer ("DPO") until 15 April 2024, after the Incident. Section 11(3) of the PDPA requires Organisations to designate one or more individuals to have the responsibility for ensuring an Organisation complies with its obligations under the PDPA. The appointment of a DPO is a basic requirement, and part of the Accountability Obligation. The Commission reiterates its previous decisions[2] that a DPO plays an important role, undertaking activities such as guiding an organisation to develop data protection policies, a personal data inventory, and reporting personal data protection risks. A diligent DPO could have alerted the organisation to the risks of storing a large volume of personal data in the OB server.

18 In addition to its finding at [16], the Commission also finds that the Organisation has failed to meet its obligation under Section 11(3) of the PDPA. In the circumstances, the Commission determines that the Organisation has negligently breached the Accountability Obligation.

*Breach of the Protection Obligation by the Organisation*

19 To comply with the Protection Obligation, an organisation must implement security arrangements that are reasonable and appropriate in the circumstances (e.g. such as administrative, physical and technical measures or a combination of these[3]).

[2] *PPLingo Pte Ltd* [2023] SGPDPC 12 at [35], *Re AgcDesign Pte Ltd* [2019] SGPDPC at [5] & *Re M Stars Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 at [31] to [37].
[3] See the Commission's Advisory Guidelines on Key Concepts in the PDPA (Revised 16 May 2022), at [17.5].

The Organisation accepted that it was in possession of the personal data on the OB server, although the IT management was outsourced to an IT vendor. In the present case, as the Organisation is in possession of a high volume of personal data (including sensitive personal data such as the photograph(s) of individuals and full information found in the full images of NRICs / passports / birth certificates), the onus was on the Organisation to implement an appropriately robust level of security arrangements to discharge its obligation under the Protection Obligation.

20 Investigations revealed that the following lapses increased the risks of unauthorised access to the personal data in the Organisation's possession and contributed to the Incident, which the Organisation has admitted to:

(a) The Organisation did not have any contractual clauses with its IT Vendors on the scope of their responsibilities in relation to patch management, maintenance of the OB server or data protection, including the supervision / monitoring of its IT Vendors. Thus, the Organisation did not conduct any security reviews of the affected OB server prior to the Incident;

(b) The Organisation's server was using Windows Server 2012, which reached its end-of-life on 10 October 2023 with no further support[4], an outdated operating system which the TA could have exploited to gain access; and

[4] https://learn.microsoft.com/en-us/lifecycle/announcements/windows-server-2012-r2-end-of-support

(c) The Organisation did not employ multi-factor authentication ("**MFA**") or require sufficient password complexity for its administrative and user accounts.

*Failure to conduct regular security reviews*

21 Although the Organisation had engaged IT Vendors, the Organisation did not put in place written contracts that set out the respective obligations and responsibilities of the vendors to protect personal data or get the IT Vendors to carry out regular security reviews of its systems.

22 Where an organisation relies on vendors to perform IT security maintenance and/or review, the Protection Obligation requires that the organisation ensures that the scope of the vendor's services and security requirements are clearly stipulated in writing in the vendor contract. This forms part of the duty of a data controller under the Protection Obligation[5]. Additionally, an Organisation should follow through with operational procedures and checks to ensure that its vendor/data intermediary carried out its functions to protect personal data in accordance with any specific instructions or contractual requirements[6]. In this regard, the Commission has repeatedly reiterated that the Protection Obligation requires organisations to exercise reasonable oversight of their vendors[7].

23 In this case, the Organisation claimed that the affected server was maintained by its OB Vendor, and it could not have patched any vulnerabilities in the server.

[5] *See Academy of Medicine Singapore* [2024] SGPDPCS 4 at [10(c)].
[6] *Re Tech Mahindra (Singapore) Pte Ltd* [2017] SGPDPC 4 at [15].
[7] *See Fullerton Heathcare Group and Agape CP Holdings* [2023] SGPDPC 5 at [22], citing *SCAL Academy Pte. Ltd.* [2020] SGPDPC 2.

However, there were no written contracts or documents that clearly stated the duties and responsibilities of the OB Vendor concerning the affected server, including responsibilities related to the security of personal data in the Organisation's possession and / or control. There was also a lack of documented processes and records for the supervision / monitoring of its Vendors. If the Organisation intended its vendor to take on the responsibility to maintain the affected server, it should have documented contractual stipulations to this effect.

24 Flowing from this, the Organisation failed to, whether by itself or through its engaged IT vendors, conduct any periodic security reviews prior to the Incident. Periodic security reviews should be conducted to a reasonable standard to identify and remedy any vulnerabilities in an organisation's IT systems and network[8]. This is especially crucial for the Organisation as it possesses large volumes of personal data from its business operations.

25 In this instance, performing security reviews could have identified, amongst others, the need to upgrade its server operating system, Windows Server 2012, which was no longer supported by Microsoft, and the need to introduce MFA for its administrative accounts accessing the server which stored the customers' data[9].

*Use of end-of-life, outdated computer system*

26 Further, using outdated or unsupported software versions can leave systems vulnerable to security risks[10]. The Organisation's server was running Windows Server

[8] See *CH Offshore Ltd* [2024] SGPDPC 2 ("**CH Offshore**") at [13].
[9] The need to introduce MFA was also an issue identified in *CH Offshore* at [13(c)].
[10] See the Commission's Guide on managing and notifying data breaches under the Personal Protection Act (revised on 15 March 2021) at page 8 and Annex A, on computer system weaknesses.

2012, an outdated OS that was no longer supported by Microsoft at the time of the Incident. This was assessed to be a vulnerability through which the TA could have obtained access to the Organisation's server through the RDP.

27 After gaining access to the Organisation's server, the TA would likely be able to gain access and exfiltrate the personal data stored in the OB System. Thus, it is possible that the outdated OS could have given the TA entry into the Organisation's environment.

*Lack of password complexity and two-factor / multi-factor authentication*

28 Third, the Organisation had not implemented MFA for administrative and user accounts or sufficient password complexity prior to the date of the Incident. In the Commission's decision of *Lovebonito Singapore Pte. Ltd.* [2022] SGPDPC 3 ("***Lovebonito***"), the Commission had made clear that MFA was to be implemented as a baseline requirement for administrative accounts with privileged access to confidential or sensitive personal data or large volumes of personal data[11].

29 The Organisation has, in its possession, large volumes of personal data and should have implemented MFA for the administrative accounts which were connected to the OB System which stored the customers' data.

30 The Commission reiterates that organisations must adopt, implement and enforce a strong password policy, including a minimum level of password complexity,

[11] See *Lovebonito* at [48].

and regular password changes[12]. This is a basic security measure that Organisations are expected to put in place, which the Organisation did not have.

31 From the foregoing, the Commission finds that the Organisation has negligently contravened the Protection Obligation.

**Observations on other data protection practices**

32 Separate to the above findings, the Commission notes that the Organisation had reformatted the affected laptops without keeping a backup copy of any audit or system logs. The Commission accepts that the Organisation reformatted the affected laptops as it did not reasonably know at the time that it was the subject of a ransomware attack. Nevertheless, it could have retained system logs as backup when it reformatted the affected laptops, such that all available information about its systems would not have been completely wiped out.

33 The Commission had stated that the maintenance of audit and system logs are important to determining the cause of security incidents and monitoring the overall health of ICT systems. Organisations that maintain system logs are also able to review them regularly for security violations and possible breaches[13]. Had the Organisation retained a backup of the logs in the aftermath of the Incident, it would have been in a better position to determine the causes of the data breach and take more effective remediation measures.

[12] *PPLingo Pte Ltd* [2023] SGPDPC 12 at [22], *Congita Asia Holdings Pte Ltd* [2022] SGPDPCS 14. See also the Commission's Guide to Data Protection Practices for ICT Systems ("**ICT Guide**"), on the basic practices for ICT Controls.
[13] ICT Guide at pg 27, points c and d.

34 In this case, it was not necessary for the Commission to make findings in relation to the above data protection practice. However, organisations should note that the Commission will not hesitate to take action against any organisations which have deliberately deleted forensic evidence of data breaches to hide the fact that personal data was exposed and accessed.

**The Commissioner's Preliminary Decision**

35 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.

36 From the Incident, a high volume of personal data amounting to 336,759 unique individuals were affected. A fair number of different types of datasets were involved, which included full images of some of the affected individuals' NRIC / passport / birth certificates, including ID photographs (at least 100 affected individuals). As the Commission has highlighted before in *Keppel Telecommunications & Transportation Ltd* [2024] SGPDPC 3, where the personal data affected includes full images of identification documents, individuals may be exposed to greater risks of identity theft or actual financial losses. Full images of identification documents differ from collection of only the NRIC or passport numbers. Identification documents are composites of several pieces of personal data, and such images are often used to identify customers to a high degree of fidelity for financial transactions as part of know-your-customer processes. The exposure of such personal data presents significant harm. There was also exfiltration of some of the affected personal data, because of the Incident. The nature and gravity of the non-compliance is high.

37 Having considered the facts relating to the Organisation's failure to implement reasonable security arrangements to protect the personal data in its possession and/or control and failure to demonstrate accountability, the Commission is satisfied that the breaches were systemic. The Commission finds the Organisation to be negligent in contravening the Protection Obligation and the Accountability Obligation, and a financial penalty is warranted under Section 48J(1)(a) of the PDPA.

38 Having decided that the imposition of a financial penalty is warranted, the Commission considered the relevant facts and circumstances in determining the appropriate quantum of the financial penalty to be imposed, including the Organisation's annual turnover. The Commission considers that a proportionate financial penalty would serve as an effective deterrent to both the Organisation, and other organisations with turnovers of similar size.

39 In turn, the Commission recognises the following factors warranting a reduction in the quantum of the financial penalty imposed, which includes:

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

(b) The Organisation took prompt and effective remedial actions in response to the Incident.

40 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[14].

41 Having considered the above factors and circumstances, the Commissioner preliminarily determined that a financial penalty of $47,000 would be imposed in respect of the Organisation's negligent contraventions of the Accountability Obligation and Protection Obligation. On 1 September 2025, 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**

42 While the Organisation accepted the findings of contraventions under Sections 11(3), 12 and 24 of the PDPA, the Organisation made various representations, amongst others, in seeking a reduction of the financial penalty to be imposed:

(a) It was the Organisation's first instance of non-compliance with the PDPA;

(b) The Organisation had taken prompt and substantial remedial action to mitigate the effects of the Incident;

(c) The Organisation had voluntarily admitted to its breaches of the PDPA under the Expedited Decision Procedure;

(d) Not all of the records in the affected OB System/server had been established to be compromised, with many records being historical, outdated or duplicative;

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

(e) The Organisation is still recovering from its considerable losses during the Covid-19 period. In support, the Organisation cited the Commission's decision in *Commeasure Pte Ltd* [2021] SGPDPC 11 (*"**Commeasure**"*), where the Commission took into account that the organisation, which operates in the hospitality industry, had been severely impacted by the COVID-19 pandemic when deciding the financial penalty quantum to be imposed[15];

(f) The Organisation had commenced key security upgrades prior to the Incident. A reduction in financial penalty would allow the Organisation to reallocate these resources to enhance IT security and strengthen protection of its clients' personal data; and

(g) The proposed financial penalty of $47,000 appears disproportionate, as the Organisation is not an IT service provider, initiated substantial IT security upgrades and referring to the Commission's decision to impose a financial penalty of $17,500 for a breach involving the exfiltration of 190,589 individual's personal data in *Ezynetic Pte Ltd* ([2025] SGPDPCS 2) ("**Ezynetic**").

43 After careful consideration, the Organisation's representations were not accepted for the main reasons outlined below.

*Considerations already taken into account in the preliminary decision*

[15] See *Commeasure* at [20].

44 The representations at paragraphs 42(a)[16], (b) and (c) do not provide any new considerations to merit a reduction in the financial penalty.

*Scope of harm caused by the Incident*

45 The representation at paragraph 42(d) above is not accepted. The Organisation had admitted that the Incident affected a high volume of personal data that totalled 336,759 unique individuals at paragraph 36 above. Unless the personal data in question are contained in records that have been in existence for at least 100 years (under Section 4(4) of the PDPA), it is irrelevant whether the records of the 336,759 affected individuals were historical or outdated as they are still subject to the PDPA. Further, the Organisation has not submitted any evidence to substantiate its representation that these records were duplicative.

*COVID-19-related financial hardships*

46 The representation at paragraph 42(e) above does not merit a reduction in the financial penalty. When deciding the financial penalty to be imposed, the Commission has consistently taken into account the financial circumstances or the organisation or person involved, bearing in mind that the financial penalty imposed should avoid imposing a crushing burden or cause undue hardship on the organisation or person[17]. In this case, the purported financial hardship is not borne out by the Organisation's latest financial statements[18] and do not show that the proposed financial penalty would be ruinous to its financial situation. From 2023 to 2024 (after the receding of the

[16] See the Commission's decision in *RedMart Ltd* [2002] SGPDPC 8 at [35].
[17] *Re Jigyasa* [2021] SGPDPCR 1; *Commeasure*; *Neo Yong Xiang (trading as Yoshi Mobile)* [2021] SGPDPC 12 and *Eatigo International Pte Ltd* [2022] SGPDPC 9.
[18] See Section 48J(5A) of the PDPA, where the annual turnover is based on the most recent audited accounts of the organisation available at the time the financial penalty is imposed on that organisation.

COVID-19 pandemic), the Organisation's revenue increased substantially and it recorded net profits for both years.

47 The Commission's decision in *Commeasure* does not assist the Organisation in this regard. The decision was issued on 15 September 2021 which was closer to the height of the COVID-19 pandemic, and where Governmental measures to curb its spread was still in place. Since the effects of COVID-19 on the hospitality sector was more severe at that time, it had a greater bearing on the Commission's assessment of the impact that the financial penalty would have on the organisation's financial situation compared to the present case.

*Remedial measures implemented by the Organisation*

48 The representation at paragraph 42(f) above does not merit a reduction in the financial penalty quantum. While the Commission notes that the Organisation has carried out some security upgrades prior to the Incident, it is not mitigating for the Organisation to claim that it had taken certain security measures to protect the personal data, as the Organisation was simply fulfilling its statutory obligation under the Protection Obligation. In any case, there was no economic reason or excuse for the Organisation to not have had a DPO or data protection policies in place for a prolonged period of time prior to the Incident.

49 The Commission also cannot accede to the Organisation's request for a reduction in financial penalty so that it can allocate those resources to strengthening its IT security, as this would paradoxically reward organisations that had not strengthened its data protection measures prior to the occurrence of data breaches. A

financial penalty needs to also send an effective deterrent message against errant organisations, as is the case with the Organisation.

*Comparison with the Commission's decision in Ezynetic*

50 The representation at paragraph 42(g) above is not accepted. In arriving at the appropriate financial penalty, each case has to be decided on its specific facts and circumstances. In this case, amongst others, the Organisation had committed multiple contraventions of the PDPA and its turnover was substantially higher which distinguished it from *Ezynetic.*

51 Having considered all the relevant circumstances of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of $47,000 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 2021 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.

52 In addition, the Commissioner directs the Organisation to within 90 days of the relevant notice accompanying this Decision:

(a) develop and implement relevant data protection policies necessary to meet the Organisation's obligations under the PDPA, including a password policy requiring password complexity and other good password practices;

(b) review or put in place contracts with existing vendors to include relevant clauses related to cybersecurity (regular security reviews, IT

infrastructure maintenance, patch management and monitoring) and data protection necessary to meet the Organisation's obligations under the PDPA;

(c) engage a Cyber Security Agency (CSA) licensed cybersecurity service provider to conduct a vulnerability assessment and penetration testing and to remediate any vulnerabilities identified including using MFA for administrative and user accounts; and

(d) provide the Commission with the supporting documents evidencing the above, upon completion and within the stated period.

**WONG HUIWEN DENISE**
**DEPUTY COMMISSIONER**
**FOR COMMISSIONER FOR PERSONAL DATA PROTECTION**