DECISION OF THE
PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1607-B0129

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

And

(1) Tiger Airways Singapore Pte Ltd (UEN No. 200312665W)

(2) SATS Ltd (UEN No. 197201770G)

(3) Asia-Pacific Star Private Limited (UEN No. 199705514Z)

… Organisations

Decision Citation: [2017] SGPDPC 6

GROUNDS OF DECISION

31 May 2017

A. INTRODUCTION

1. On 27 July 2016, the Personal Data Protection Commission received a complaint that the passenger name list for Tiger Airways Singapore Pte Ltd ("**Tigerair**") flight TR2466 ("**Flight Manifest**") had been improperly disposed in a rubbish bin in the gate hold room at Changi Airport. The complainant alleged that the Flight Manifest could have been retrieved by anyone in the vicinity.

2. The Commission undertook an investigation into the matter and sets out its findings and grounds of decision below.

B. MATERIAL FACTS

3. Tigerair is a low cost carrier. SATS Ltd ("**SATS**") is an aviation ground handling service provider. SATS was engaged by Tigerair to provide ground handling services. In accordance with the terms of the ground handling services contract between SATS and Tigerair ("**Ground Handling Services Contract**"), SATS was responsible for the provision of the services by its subsidiaries as if it had been provided by SATS itself.

4. Asia-Pacific Star Private Limited ("**APS**") is a wholly-owned subsidiary of SATS. SATS sub-contracted the provision of ground handling services for Tigerair to APS pursuant to a Services Agreement dated 11 June 2014 ("**Services Agreement**").

5. Under the Services Agreement, APS was responsible for managing the boarding process, reconciling passenger numbers and verifying travel documents at the boarding gate. Among other things, APS was required to print a copy of the Flight Manifest at the boarding gate for the cabin crew to take on board the flight and submit to the immigration authority at the arrival destination.

6. On 26 July 2016, an APS employee who was on gate duty for flight TR2466 ran out of paper while printing a copy of the Flight Manifest. The APS employee disposed of the partially-printed Flight Manifest in the rubbish bin in the gate hold room for flight TR2466 and reprinted the Flight Manifest in full ("**Data Breach Incident**"). The gate hold room where the partially-printed Flight Manifest was discarded was only accessible to passengers and airport staff.

7. None of the Organisations (nor the complainant) could verify the exact number of passengers whose personal data was disclosed in the partially-printed Flight Manifest.

8. The partially-printed Flight Manifest contained passenger personal data such as the passenger's name, booking reference number (also known as PNR), fare class, sequence number of check-in, date of booking, seat number, destination and flight number.

9. Other personal data such as the passenger's full name, passport number, home address, phone number, email address and last four digits of the credit card used to pay for the plane ticket could have been retrieved by entering the passenger's name and the PNR into Tigerair's "Manage My Booking" portal. Special features or add-ons to the passenger's flight(s) and travels, such as hotel bookings and airport transfers or cars rentals would also have been reflected on the "Manage My Booking" portal. This information was only accessible up to the last travelling date of the passenger's itinerary.

C. COMMISSION'S FINDINGS AND BASIS FOR DETERMINATION

10. At the outset, the Commission finds that the partially-printed Flight Manifest constitutes personal data as defined in section 2(1) of the Personal Data Protection Act 2012 ("**PDPA**"). The Flight Manifest contained data about the passengers who could be identified either from that data alone or from that data and the data on Tigerair's "Manage My Booking" portal.

Issues for determination

11. The issues to be determined by the Commission are as follows:

    (a) whether SATS and APS were acting as data intermediaries for Tigerair in relation to the Tigerair passengers' personal data; and

    (b) whether each of the Organisations complied with its obligation under section 24 of the PDPA in respect of the Data Breach Incident.

Issue (a): Whether SATS and APS were acting as data intermediaries for Tigerair in relation to the Tigerair passengers' personal data

12. As mentioned at paragraph 3 above, SATS was engaged by Tigerair to provide services such as managing the boarding process, reconciliation of passenger numbers and verification of travel documents at the boarding gate. These are activities of "processing" personal data on behalf of Tigerair as defined in section 2(1) of the PDPA.

13. SATS had sub-contracted the provision of the services to APS but remained responsible for the provision of ground handling services as if they were performed by SATS itself. APS was granted access to Tigerair's "Departure Control System" which contained all the information related to a passenger's booking to carry out activities of "processing" on behalf of Tigerair. Accordingly, the Commission is satisfied that SATS and APS were both acting as data intermediaries of Tigerair.

14. A data intermediary has a duty to comply with the Protection Obligation under section 4(2) of the PDPA. An organisation has the same obligation in respect of personal data processed by a data intermediary on its behalf and for its purposes as if the personal data were processed by the organisation itself under section 4(3) of the PDPA. Accordingly, Tigerair, SATS and APS each have an obligation to make reasonable security arrangements to protect the personal data of Tigerair passengers in their possession and/or under their control.

Issue (b): Whether each of the Organisations complied with its obligation under section 24 of the PDPA in respect of the Data Breach Incident

15. It was not disputed that the partially-printed Flight Manifest was improperly disposed of by the APS employee at the gate hold room. However, the Organisations represented that they had adequate policies and processes regarding the protection of personal data. The Data Breach Incident was simply an isolated incident that occurred due to the oversight of the APS employee.

16. Section 24 of the PDPA places a positive obligation on an organisation to make reasonable security arrangements to protect the personal data

in its possession or under its control and to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

17. In accordance with section 11(1) of the PDPA, the reasonableness of security arrangements made is objectively determined, having regard to what a reasonable person would consider appropriate in the circumstances. In the context of section 24, this means that an organisation is not required to provide an absolute guarantee for the protection of personal data in its possession, but that it must make such security arrangements as a reasonable person would consider appropriate, given the nature of the personal data involved and the particular circumstances of that organisation.

18. In assessing the reasonableness of security arrangements, the Commission will also take into consideration the factors set out in the Advisory Guidelines on Key Concepts in the PDPA:

    (a) the nature of the personal data;

    (b) the form in which the personal data has been collected (e.g. physical or electronic); and

    (c) the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.

Tigerair

19. As an organisation under the PDPA, Tigerair has the primary responsibility of ensuring that there are reasonable security arrangements in place to protect the personal data in its possession or under its control. Tigerair remains ultimately responsible even though it had engaged a data intermediary to provide ground handling services and process personal data on its behalf.

20. Under the Ground Handling Services Contract, Tigerair required SATS to establish and maintain local procedures to comply with the PDPA in its provision of services to Tigerair.

21. SATS was also required to carry out all services in accordance with Tigerair's ground services manual ("**Ground Services Manual**"). The Ground Services Manual specifically provided that ground handlers were to adhere to the requirements of the PDPA, including the obligations to use personal data only for the purposes for which consent had been obtained, protect personal data in its custody, and prevent disclosure to unauthorised persons.

22. In the present context, the ground handling services fell under the responsibility of SATS and APS, both of whom had the responsibility of ensuring that in the provision of these services, personal data was

adequately protected. In this regard, having imposed a contractual obligation on SATS to establish and maintain local procedures to comply with the PDPA, the Commission finds it reasonable for Tigerair to have expected SATS to carry out its obligations in accordance with the contract and the relevant sections of the Ground Services Manual.

23. Further, given that SATS was contractually accountable for APS' provision of services, it was reasonable for Tigerair to have expected SATS to ensure that APS would implement reasonable security arrangements to protect the personal data that it processed on behalf of Tigerair. This is especially since Tigerair did not have oversight over the actions of APS' employees.

24. Accordingly, the Commission finds that Tigerair had complied with its Protection Obligation under section 24 of the PDPA.

SATS

25. SATS had, in its Service Agreement with APS for the sub-contracting of ground handling services for Tigerair, expressly required APS to comply with and ensure that the ground handling services were provided and performed in a manner which did not infringe any applicable laws, regulations and directions, including the PDPA.

26. In addition, SATS implemented the SATS Group Code of Conduct ("**Group Code of Conduct**"), which required all employees who may handle, receive, collect, use, disclose or transfer any personal data to comply with the PDPA and the Personal Data Protection Policy ("**Group Data Protection Policy**").

27. The Group Data Protection Policy sets out guidelines on the physical measures that should be undertaken to protect personal data. Specifically, the guidelines recommended that there should be proper and secure disposal of documents containing personal data, such as requiring such documents to be shredded. APS was required to comply with both the Group Code of Conduct and the Group Data Protection Policy as it was a member of the SATS Group.

28. SATS also sent periodic updates and reminders to the SATS Group management and staff (including those from APS) to remind them about their data protection obligations under the Group Code of Conduct and the Group Data Protection Policy. Pertinently, SATS conducted annual "Control Self-Assessment" exercises as part of its enterprise risk management and required the General Manager of APS to confirm APS' compliance with the Group Data Protection Policy.

29. In view of the above, the Commission finds that SATS made reasonable security arrangements and fulfilled its Protection Obligation under section 24 of the PDPA.

APS

30. APS represented that it had put in place security arrangements and the Data Breach Incident was an isolated incident that occurred as a result of a lapse by an APS employee. Pursuant to section 53(1) of the PDPA, any act done or conduct engaged in by an employee in the course of his employment shall be treated as done or engaged in by his employer as well as by him, regardless of whether it was done or engaged in with the employer's knowledge or approval. Accordingly, APS remains responsible for its employee's conduct.

31. Although the Commission finds that APS did have some security arrangements in place, the Commission is not satisfied that APS fulfilled its Protection Obligation under section 24 of the PDPA.

32. As mentioned at paragraph 27 above, APS is part of the SATS Group, all APS employees are required to comply with the Group Code of Conduct and the Group Data Protection Policy. The Group Code of Conduct was annexed to APS employees' letters of employment and all new APS employees received a briefing on the requirement to comply with the PDPA during their employee induction programme.

33. However, APS relied solely on the administrative safeguards implemented by SATS, which applied to the organisations within the SATS Group. There was no evidence that APS provided additional information or implemented additional safeguards in order to contextualise the group level policies to its ground operations. In line with the Commission's observation *In the Matter of National University of Singapore* that general guidelines did not necessarily translate into the kind of practices that were actually needed on the ground to protect personal data[1], it is likewise important here for organisations to ensure that an organisation's policies and training have to be contextualised to its operational setting. In this case, there was no evidence that APS had any procedure or policy of its own apart from the SATS Group Data Protection Policy.

34. Crucially, given that the personal data found in the Flight Manifest provided further access to personal information of an even more sensitive nature found on the "Manage My Bookings" portal, the impact to the passengers from the improper disposal was higher. Given the potential adverse consequences of unauthorised access to that personal data (from the initial and secondary exposure), APS should have afforded a high level of protection to such personal data, with greater attention given to the proper disposal of documents containing such personal data. The specific scenarios (like the present) where there are risks of data leaks through inappropriate handling or disposal of Flight Manifests that are likely to arise in ground operations (eg staff handling Flight Manifests at the gates) ought to have been part of the effort to

[1] [2017] SGPDPC 5, at [32].

translate and contextualise the group level policies for APS's specific circumstances.

35. Additionally, as the Commission observed *In the Matter of National University of Singapore*[2], security policies and procedures are essential but they are only effective when properly and consistently implemented and followed by employees. Ongoing training on the organisation's data protection obligations and the organisation's data protection policies and procedures is key to fostering and maintaining a high organisational awareness of data protection concerns and to ensure that the data protection obligations under the PDPA are consistently understood and acted upon by employees. This was also observed by the Commission *In the Matter of National University of Singapore*[3]. Yet, as set out in paragraph 32 above, the only training that APS employees appeared to have received was a general data protection briefing during the employee induction programme for new employees.

36. APS should have provided customised training and regular refresher training for APS employees who routinely handled passengers' personal data. APS processes the personal data of a large number of individuals, including passenger identification information such as the Flight Manifest, on a regular basis in the course of its duties.

37. Given the Commission's findings on the lack of administrative and physical safeguards in place, the Commission finds that APS did not make reasonable security arrangements to protect the personal data it processed on behalf of Tigerair.

D. THE COMMISSION'S DIRECTIONS

38. For the reasons set out above, the Commission has determined that APS did not comply with its Protection Obligation under section 24 of the PDPA. In exercise of the power conferred upon the Commission pursuant to section 29(1) of the PDPA, the Commission directs APS to:

    (a) conduct a review of its procedure for proper disposal of personal data in its possession and/or control;

    (b) introduce data protection policies that are contextualised and pertinent to the services provided by APS and functions performed by its staff; and

    (c) include a programme for initial and refresher training on its implementation by the APS staff in the course of its operations.

39. In assessing the breach and remedial directions to be imposed (including not imposing a financial penalty on APS in this case), the Commission

[2] [2017] SGPDPC 5, at [25].
[3] [2017] SGPDPC 5, at [20] – [28].

considered various factors relating to the case, including the mitigating factors set out below:

(a) the gate hold room where the Flight Manifest was disposed was accessible only by passengers and airport staff;

(b) the bin where the Flight Manifest was disposed could reasonably be expected to be emptied regularly as part of routine maintenance;

(c) the Flight Manifest held data that served as login credentials to individual passengers' personal data on the "Manage My Bookings" portal. However, the information on the page was only accessible for a limited time until the last traveling date on the passenger's itinerary;

(d) there were no complaints of any actual unauthorised access to the manage my bookings page of any passenger.

40. The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA. Organisations should take the necessary action to ensure that they comply with their obligations under the PDPA. The Commission will not hesitate to take the appropriate enforcement action against the organisations accordingly.

YEONG ZEE KIN
DEPUTY COMMISSIONER
PERSONAL DATA PROTECTION COMMISSION