

## PERSONAL DATA PROTECTION COMMISSION

Case No. DP-1804-B1931

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

And

Royal Caribbean Cruises (Asia) Pte. Ltd.

### **SUMMARY OF THE DECISION**

1. On 5 April 2018, the Personal Data Protection Commission (“**Commission**”) commenced investigation against Royal Caribbean Cruises (Asia) Pte Ltd (the “**Organisation**”) after receiving a complaint from a member of the public (the “**Complaint**”). The complainant stated that she had received the personal data of unrelated individuals in an email payment reminder sent by the Organisation.
2. Investigations revealed that, from 8 February 2018 to 4 April 2018, the personal data of 526 individuals were inadvertently disclosed to other unrelated members of the public via unintended email payment reminders (the “**Data Breach Incident**”). The personal data disclosed included booking IDs, ship codes, sailing dates, names, net amounts due, amounts paid, balance due and the balance due date (the “**Affected Personal Data**”).
3. The Organisation is part of the Royal Caribbean Group, and is the wholly owned subsidiary and data intermediary of the USA-based Royal Caribbean Cruises Ltd

(Liberia) (“**RCL**”). It is responsible for the following business functions on behalf of RCL:

- (a) Conducting sales and marketing activities on behalf of the cruise ship operators of the Royal Caribbean Group, including RCL;
- (b) Taking cruise bookings from Singapore-based customers of RCL;
- (c) Administering a loyalty membership programme on behalf of RCL; and
- (d) Collecting payments from Singapore-based customers of RCL who made their bookings via walk-in, roadshows and online bookings at the Royal Caribbean Group’s Singapore website.

4. RCL’s branch office in the Philippines (“**RCL Philippines**”) provides IT support to entities within the Royal Caribbean Group, and does not have a separate legal identity from RCL. On 1 January 2017, the Organisation entered into an operative intercompany agreement with RCL Philippines for the provision of IT support and customer services support. Such services included providing technical support for the business software applications and services used by the Organisation.

5. As part of its business functions, the Organisation would send its Singapore customers email payment reminders prior to the commencement of their cruises. On 8 February 2020, the Organisation automated this business function through a business software enterprise operated by RCL Philippines (the “**Hyperion System**”), which would generate pre-programmed emails to individual customers to remind them of outstanding bill amounts (the “**Direct Payment Reminder**”). Concurrently, a collated list of the customers (together with other personal data) who received the Direct Payment Reminder would be generated and sent via email

to the Organisation (“**Collated Payment Reminder**”). Both the Direct Payment Reminder and Collated Payment Reminder were automatically generated on a scheduled frequency and sent to the customers and Organisation by the Hyperion System without any manual intervention from the Organisation (the “**Automated Payment Reminder System**”).

6. The Automated Payment Reminder System had been successfully implemented in other countries, and RCL Philippines put in place the following process to handle requests from Royal Caribbean Group entities related to the Hyperion System:
  - (a) RCL Philippines would receive a request from respective Royal Caribbean entity for a new process to be implemented in the Hyperion System;
  - (b) RCL Philippines would review the scope of the request and configure the Hyperion System;
  - (c) RCL Philippines would then run a test cycle and a test email would be generated to RCL Philippines to test for whether the content was in line with the request by the requesting Royal Caribbean entity;
  - (d) Thereafter, RCL Philippines would send a sample of the output email to the relevant Royal Caribbean entity to review; and
  - (e) The relevant Royal Caribbean entity would sign off on the implementation and RCL Philippines would then implement the new process to go live.
  
7. Investigations revealed that the Data Breach Incident occurred because RCL Philippines made an error in the coding of the email parameters in the Structured Query Language (“**SQL**”) script when configuring the Hyperion System as described in paragraph 6(b), leading to the Collated Payment Reminders being

sent to the first customers in the mailing lists instead of the Organisation. Consequently, the personal data of the Singapore customers contained in the Collated Payment Reminders were disclosed to certain unrelated customers.

8. Both the Organisation and RCL Philippines were not aware of this error until they were informed of the Complaint to the Commission referenced in paragraph 1. As the Automated Payment Reminder System was new and unfamiliar to the Organisation at the material time, the Organisation and its employees were also not aware that it was supposed to be receiving the Collated Payment Reminders.
9. The Data Breach Incident happened after the Organisation provided lists of Singapore customers with outstanding payments due to RCL Philippines for processing with the Hyperion System. The Commission is of the view that the coding error that occurred during the configuration of the Hyperion System was wholly within RCL Philippines' operations and that the Data Breach Incident did not arise from any business functions that the Organisation was conducting as a data intermediary on behalf of RCL.
10. In the above circumstances, the Deputy Commissioner for Personal Data Protection finds that the Organisation was not in breach of the Protection Obligation under section 24 of the PDPA.

11. We note that the Organisation had taken the following remedial actions:

- (a) Conducted additional trainings for its employees to be mindful of the importance of data protection in its business processes;
- (b) Reviewed its supervisory framework for new employees so that similar incidents would not happen again; and
- (c) Reviewed its communication with RCL Philippines for implementation of any new processes.

The following is the provision of the Personal Data Protection Act 2012 cited in the above summary:

**Protection of personal data**

**24.** An organisation shall 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.