PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2012-B7506

In the matter of an investigation under section 50(1) of the

Personal Data Protection Act 2012

And

Aman Group S.a.r.l and/or

Amanresort International Pte Ltd

SUMMARY OF THE DECISION

1. On 5 December 2020, the Personal Data Protection Commission (the "**Commission**") received a notification from SingCERT of a personal data breach involving Aman Group S.a.r.l ("**Aman Group**") and/or Amanresort International Pte Ltd ("**Aman SG**"). 9 systems in London and 2 systems in Singapore were compromised and files containing personal data exfiltrated (the "**Incident**").

2. As a result of the Incident, personal data of approximately 2,500 individuals which included their name, date of birth, address, email address, phone number and profession were affected.

3. The Aman Group engaged an external cybersecurity company, Ankura Consulting, to investigate the Incident. Its investigations found that the threat actor(s) had gained unauthorised access into 11 systems, which included 9 servers based in London and 2 servers based in Singapore.

4. While the investigations did not uncover any evidence of what the initial method and point of entry were, the most likely scenario is that the threat actor had initially entered via the London based systems. This is because the suspicious activities were first detected in the London systems. Thereafter, the threat actor subsequently gained access to the 2 Singapore based servers by creating administrator account credentials. There was no evidence that the firewalls in the Singapore based servers were breached.

5. Investigations could not conclusively exclude the possibility that data may have been exfiltrated from one of the Singapore based servers. However, analysis conducted by the Aman Group on four extracts obtained from the threat actor(s) failed to establish any conclusive links between the extracts and the current database in the affected Singapore based server.

6. Investigations further revealed that any exfiltrated data would have been encrypted and was in a proprietary format. Aman Group's assessment was that

the encryption and the proprietary format made it unlikely that the threat actor(s) would be able access and recreate the data in plaintext. Their assessment is that even if there had been exfiltration, there was no evidence that the exfiltrated data was in fact compromised. This is because the extracts obtained from the threat actor(s) do not resemble the current database in the affected Singapore based server.

7. Following the Incident, the Aman Group took prompt and extensive remedial actions to mitigate the effects of the Incident and enhance the robustness of its security measures.

8. Further, based on the facts as disclosed, Aman SG is a regional office. It did not hold the data protection role and was not in possession or control of the personal data in the 2 Singapore based servers. As such, Aman SG could not be held accountable for the Incident and cannot be said to be in breach of the Protection obligation under section 24 of the PDPA.

9. In view of the above, the Deputy Commissioner for Personal Data Protection is satisfied of the view that the Aman Group had met its Protection obligation under section 24 of the Personal Data Protection Act ("PDPA") and that no enforcement action needs to be taken in relation to the Incident.

The following provision(s) of the Personal Data Protection Act 2012 had been 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 –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.