PERSONAL DATA PROTECTION COMMISSION

Case No. DP-1911-B5268

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

And

Interauct! Pte Ltd

SUMMARY OF THE DECISION

1. Interauct! Pte Ltd (the "**Organisation**") operated an online mobile number auction (the "**Auction**") for a telecommunications provider (the "**Telco**"). This arrangement started in the year 2000 and ended in 2018.

2. In November 2019, the Commission was informed that the Telco's cybersecurity team had located an internet sub-domain containing files with the personal data of individuals who had participated in the Auction (the "**Files**"). The Files contained the following types of personal data:

    a. Name;

    b. ID (such as passport or NRIC number);

    c. Mobile number;

    d. Address;

    e. Date of birth; and

    f. Email address.

3. The Commission's investigations revealed the following:

a. The Organisation had engaged a vendor to provide web hosting services for the Auction. In 2012 and 2016, the vendor conducted server migration exercises. On both occasions, the Organisation created backups of the Files prior to server migration exercises and uploaded them on the vendor's servers. The Organisation did not delete the Files after the server migration were completed;

b. In April 2019, the vendor misconfigured its servers. As a result, the Files became accessible on the internet sub-domain. However, to access this sub-domain requires an individual to key in either one of two URLs exactly. Both URLs were complex and lengthy. It was therefore difficult for an individual to determine the URLs exactly to enter the sub-domain. Indeed, an examination of server logs found that only the Telco had accessed the sub-domain;

c. The Files contained a mix of individuals' personal data, as well as dummy data used for testing purposes. An analysis of the Files showed that there were approximately 8,750 individuals' personal data contained in them. The Telco compared the data with its customer records, and via a reconciliation process, was able to identify 3,380 individuals as its customers. In this regard, the Telco informed that it would have been very difficult for a third party, without access to the Telco's customer records, to carry out such a reconciliation exercise. This means that even if an individual had

accessed the Files, it would have been difficult to him to identify the individuals from the personal data in the Files;

d. The Organisation deleted the Files within three hours of the Telco notifying the Organisation of their discovery of the internet sub-domain. The Organisation had also ensured that the vendor fixed the misconfiguration of the servers, which was done within six hours of the discovery of the internet sub-domain.

4. The Deputy Commissioner for Personal Data Protection (the "**Deputy Commissioner**") finds that the Organisation had put in place, via the vendor, reasonable security arrangements to protect the personal data. In particular, the security arrangements in place would have prevented direct access by unauthorised third-parties to the Files hosted on the server. This had greatly reduced the potential adverse impact of the incident.

5. However, the Organisation admitted that there was no reason to retain the Files after the migration exercises were completed. If the Files had been duly deleted, the personal data in the Files would not have been compromised in the first place. The Deputy Commissioner therefore finds the Organisation in breach of the Retention Limitation Obligation under section 25 of the Personal Data Protection Act 2012.

6. After considering the facts and circumstances of the incident, including the fact that the personal data in the Files was ultimately not exposed, the Deputy Commissioner has

decided to issue a warning to the Organisation for the breach of the Retention Limitation Obligation. No other direction is required as the breach has been remedied.