PERSONAL DATA PROTECTION COMMISSION

Case No. DP-1812-B3091

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

And

L'Oreal Singapore Pte. Ltd.

SUMMARY OF THE DECISION

1. L'Oreal Singapore Pte Ltd (the "**Organisation**") operated a website which had a login portal that enabled its customers to view their profile information, redeem vouchers and make enquiries about customer points ("**Customer Login Page**"). The customers' profile information included their name, email address, postal address, mobile number and date of birth (the "**Personal Data**"). The development and maintenance of the website was carried out by a vendor engaged by the Organisation.

2. To improve the loading speed of the website, the Organisation instructed its vendor to make some changes to the website in November 2018. However, the Organisation failed to scope the User Acceptance Tests ("**UATs**") to include the normal functioning of the website, in particular the login and caching functions of the Customer Login Page, after the code changes were introduced. As a result, when a customer ("**Customer A**") logged into the Customer Login Page, his or her Personal Data would be cached. Customer A's Personal Data would then be disclosed to customers who subsequently logged in to the

Customer Login Page until the cache was refreshed. Similarly, the Personal Data of the second customer ("**Customer B**"), who logged in after the cache refresh, would be cached, leading to disclosure of Customer B's Personal Data to the third customer who logs in next, and all subsequent customers until the next cache refresh. When the Organisation came to know of this, the Organisation disabled the Customer Login Page. The Organisation also engaged a consultant to assist in its investigations into the matter and to provide recommendations to prevent similar incidents in the future.

3. The Personal Data Protection Commission ("**Commission**") found that Personal Data of 7 individuals had been exposed to the risk of unauthorised disclosure as a result of the Organisation's failure to ensure appropriate testing of its website or make other security arrangements to protect the Personal Data. The Commission notes the Organisation's representations that it had completed all necessary and appropriate UATs based upon the reasonably foreseeable impact of the requested changes to its website. However, as mentioned at [2] above, the scope of the UATs was inadequate because it did not simulate the normal operating environment of the website. In particular, the UATs only provided for a limited test case of a single user logging into the website, and failed to include the foreseeable scenario of multiple users logging in sequentially.

4. Having considered the representations and taking into account all the relevant circumstances, the Deputy Commissioner for Personal Data Protection found the Organisation in breach of section 24 of the Personal Data Protection Act 2012 and decided to give a warning to the Organisation.