March 2021

Commercial Insights

Do your staff members understand their obligations regarding the handling and storage of personal information?

A recent decision of the Australian Information and Privacy Commissioner, Commissioner Falk, highlights the importance of staff training on the collection and storage of personal information and the need to manage customers' personal information in an open and transparent way.

In 2017, Flight Centre held a 'design jam' to create technological solutions for travel agents. Participants were given a dataset containing 106 million rows of data. The dataset had been cleansed so that data fields known to contain personal information were de-identified, leaving what was thought to be only the customer's year of birth, postcode, gender and booking information. Flight Centre representatives had reviewed a 1000-row sample of the dataset to ensure that it did not contain any personal information.

During the event it was discovered that the dataset did in fact contain a free text field that was not cleansed. In some cases this free text field was populated with personal information including credit card information, passport numbers, birthdates, usernames and passwords to vendor portals. The personal information of 6,918 individual customers was contained in the dataset.

In November 2020, the Office of the Australian Information Commissioner determined that Flight Centre had breached 6,918 customers' privacy at the 2017 'design jam'. Specifically, Commissioner Falk found that Flight Centre had breached three Australian Privacy Principles by:

- failing to take reasonable steps to implement practices to ensure compliance with the Australian Privacy Principles
- disclosing individuals' personal information without consent, and
- failing to take reasonable steps to protect individuals' personal information.

Mitigating steps taken by Flight Centre included:

1. notifying the individuals affected of the breach. However, Flight Centre was unable to contact 1,012 of the 6,918 individuals affected due to having insufficient contact details
2. arranging replacement passports for affected individuals
3. arranging credit monitoring and identity theft services for affected individuals
4. ensuring that the dataset was destroyed by all design jam participants, and
5. implementing weekly IT scans and improvements to IT systems, to ensure personnel were not able to save personal information in free text fields, engaged third party threat intelligence specialists to confirm no data was leaked, and updated its privacy and data handling policies and staff training.

March 2021

This case confirms the importance of collecting only the personal information that is necessary, and having clear and concise policies on the handling and storage of personal information, which staff understand and are adequately trained on.

While the decision acknowledges that human error may occur, organisations that are required to comply with the Privacy Act, need to have adequate policies and procedures in place to minimise the impact of human error and, where possible, prevent privacy infringement in the first place.

This article was written by Special Counsel, Hayley Bowman. If you have any questions about your compliance obligations for the handling and storage of personal information, please contact Hayley Bowman.

Hayley Bowman

Special Counsel

+61 3 9810 6723

hbowman@meridianlawyers.com.au