COMPLIANCE NOTICE

Under section 78 of the *Privacy and Data Protection Act 2014 (Vic)*

Office of the Victorian Information Commissioner

To: **Department of Transport** (integrating the Public Transport Development Authority)
1 Spring Street,
Melbourne, Victoria 3000
(the **Organisation**)

I, Rachel Dixon, under sections 8B(1)(a) and 8C(2)(e) of the *Privacy and Data Protection Act 2014 (Vic)* (**PDP Act**), serve this compliance notice under Division 9 of Part 3 of the PDP Act.

1. Background

1.1 In or around July 2018, the Organisation created and disclosed a dataset to a third party. The dataset contained information extracted from the myki electronic ticketing system operated by the Organisation.

1.2 While the dataset was claimed to be deidentified, I am satisfied that information about individuals could be reasonably ascertained. Consequently, I consider that the dataset contained personal information.

1.3 Accordingly, in disclosing the dataset to the third party, I am satisfied that the Organisation contravened:

1.3.1 Information Privacy Principle 2.1 by disclosing personal information for a purpose other than that for which it was collected; and

1.3.2 Information Privacy Principle 4.1 by not taking reasonable steps to protect the personal information it held from misuse and loss and from unauthorised access, modification or disclosure.

1.4 I am also satisfied that the contravention was serious having regard to:

1.4.1 the type and amount of information that was released;

1.4.2 the likelihood and extent of harm to individuals that could arise; and

1.4.3 the circumstances surrounding the release.

2. Action and Period Specified

2.1 In accordance with section 78(2) of the PDP Act, this compliance notice requires the Organisation to take this specified action within the specified period for the purpose of ensuring compliance with Information Privacy Principles 2.1 and 4.1.

***Specified Action 1 – Data release policies and procedures*:** The Organisation must develop and document policies and procedures for data release decisions, and provide OVIC with a copy of these policies and procedures by 1 March 2020. The policies and procedures must:

- clearly explain how data release decisions should be made including identifying:
  - the considerations that must be taken into account;
  - who is authorised to make decisions; and
  - how those decisions should be documented (including through privacy impact assessments);

- consider information data security controls relevant to downstream disclosures of data, scope creep, and data re-identification risks; and
- comply with the PDP Act and Information Privacy Principles.

***Specified Action 2 – Data governance program*:** The Organisation must implement a data governance program by October 2020. The data governance program must include data governance policies and procedures that are consistent with the PDP Act and Information Privacy Principles.

***Specified Action 3 - Training*:** The Organisation must deliver training about the above data release and data governance policies and procedures to all relevant staff and data owners in the Organisation. The training must enable relevant staff and data owners to identify risks in the Organisation's operations, match those risks to policies and procedures (including those developed as part of Specified Section 1 and Specified Action 2), and give effect to those policies and procedures.

- Delivery of training on data release policies and procedures must commence no later than 1 April 2020.
- Delivery of training on data governance policies and procedures must commence no later than 1 November 2020.
- The Organisation must provide OVIC with training course materials and a schedule for training when training commences.

Specified Action 4 - Reporting: The Organisation will provide OVIC with a report of its progress and compliance with Specified Action 1, Specified Action 2 and Specified Action 3, on 2 March 2020, 1 September 2020 and a final report on 1 March 2021.

3. Enforcement of this compliance notice

3.1 The Organisation must comply with this compliance notice.

3.2 If the Organisation does not comply with this compliance notice, the penalty is:

3.2.1 600 penalty units, in the case of an individual; and

3.2.2 3000 penalty units, in the case of a body corporate.

3.3 If the Organisation considers that it is not reasonably possible to take the action specified in this compliance notice within the period specified, the Organisation may apply to my office before the period of time specified in the compliance notice expires to extend the period of time specified in this compliance notice.

4. Application for review

4.1 An individual or organisation whose interests are affected by my decision to serve this compliance notice may apply to the Victorian Civil and Administrative Tribunal for review of my decision.

Rachel Dixon
Privacy and Data Protection Deputy Commissioner
05 August 2019