Independent Review – Findings and Recommendations

Context

In late 2016, the Department of Education and Training (the Department) commenced a formal review of the Education and Training Reform Regulations 2007 (the Regulations). A proposed draft of the Education and Training Reform Regulations 2017 was released for public consultation, along with a regulatory impact statement (RIS), on 21 December 2016 for a period of 69 days.

The consultation period closed on 28 February 2017. Over 540 submissions were received, with more than 530 of these relating to home schooling. On Friday 7 April 2017, the Department published the submissions on its website. On Saturday 8 April 2017 was made aware that it had inadvertently published personal information of people when uploading the submissions and removed all submissions from its website.

An independent review of the incident was subsequently commissioned by the Department at the request of the Secretary. This independent review has been undertaken by a director of Worklogic Pty Ltd ("the Reviewer").

The purpose of the independent review is to independently identify what errors occurred and make recommendations to eliminate or reduce the risk of breaches occurring in the future.

Findings

The central finding of the review is that while there was no single point of failure, and there was a significant amount of work put into the regulations review, departmental staff lacked awareness of privacy risk and did not manage that risk effectively.

Factors contributing to privacy incident

The factors contributing to the breach of privacy for some submitters included:

1. the way in which consents were obtained
2. the level of awareness and training on privacy principles
3. the project management approach
4. the method of collation and coding of submissions
5. regard to the sensitivity of the information
6. Awareness of the implications of publication of metadata
7. The need for improved oversight and guidance on managing public consultation processes.

Actions taken by the Department once privacy incident identified

The Reviewer understands that the Department responded to the identified privacy breach immediately, by taking the submissions down, notifying people promptly and responding to media inquiries in a timely manner, apologising and engaging with people to address their concerns, assessing the impact and using the assessment to inform further actions, such as a phone line for people to enquire or express their concerns.

It therefore appears to the Reviewer that the relevant Departmental staff took all available measures to manage the incident as promptly, professionally and constructively as was possible in the circumstances.

The process to manage re-publication of the submissions with individuals' direct consent sought was still underway as this report was prepared.

Recommendations to reduce future risk

The Reviewer has identified the following recommendations to reduce the future risk of a similar incident occurring in the future, which fall within the following three categories:

1. General education about privacy requirements

- The Department increases staff awareness of privacy principles and requirements, what constitutes personal and sensitive information, and in particular, how to respond in the event of a privacy incident, through increased internal messaging, information through "Privacy Week" events and ensuring that training on the Department's Code of Conduct includes privacy.
- The Department includes privacy risk as a component of all relevant risk registers/assessments.
- The Department includes more targeted training on privacy. In particular, the Privacy Officer creates content on training modules on privacy as part of all induction training, bespoke management training, staff training (particularly for website content authors) and refresher training modules. (NB: the Reviewer understands that proactive, organisational-wide training has already commenced).

2. General education about relevant IT/Communications issues

- Delivery of a Department-wide awareness campaign, in relation to the following issues:
  - Document management – i.e. accessibility and metadata issues
  - Records management;
  - Responsibilities of website content authors (including authorisation required); and
  - Promotion of use of the 'Engage Victoria' website in relation to matters of public consultation.

3. Improved public consultation process

a) Development of Submission Guidelines

The Department provides clearer written guidance in relation to the publishing of information provided by stakeholders/members of the public. This could be achieved by:

- The Department forming a working group with representatives from the legal, communications, policy and privacy areas to develop Submission Guidelines to be used in relation to the public consultation process (N.B. one participant noted that such a document used to be available on the Privacy Commission website).

- The resulting Submission Guidelines consider and address:
    - Whether a project charter detailing risk and mitigation strategies, and/or privacy impact assessment is required;
    - Technical control of private, identifying information;
    - Where explicit (vs. implicit) consent to publish is required;
    - Consideration of the relative merits of a discretionary vetting/redaction process, to remove sensitive material, in consultation with the individual author of the submission;
    - Acknowledgment of an overall discretion that the Department may exercise in relation to publishing certain material in any event;
    - Quality assurance process requirements (including file management, review and checking of work, authorisation levels), and
    - Incident management.

b) Improved processing of submissions

The Department improves the technological system for processing submissions from stakeholders and the public required, which reduces the risk of human error.

This could be achieved through consideration of the following:

- Public consultation could be managed, in many cases, via the Engage Victoria website in preference to using email or online survey communication options.

- Alternatively, where a more 'low tech' option for managing submissions is considered appropriate in the circumstances, the Department improves communication and process around the quality control of information released.

  This should include:

    - A clear, upfront submission coversheet or 'tick-a-box' option clearly indicating whether or not the author expressly consents to: (i) having the submission published, and (ii) being identified, such that it is not necessary to ascertain these preferences from within the body of the submission;

- Review of relevant document management issues (e.g. the format, location and naming of each category of submission in terms of privacy setting/consent given by the author), and
- Review of what is appropriate information to publish in any event, noting policy, legal and any other considerations relevant.

c) More rigorous project planning and management

- The Department promotes improved cross-divisional project planning and project management in relation to matters of public consultation, and all projects involve completing a suitably comprehensive risk register prior to any regulation review or public consultation process. From a privacy perspective, this could include (as noted above) general education about privacy requirements, improvement of knowledge of privacy principles and requirements, and what constitutes personal and sensitive information, and, in particular, how to respond in the event of a privacy incident.
- The Department provides refresher training at managerial level to ensure that there is responsibility, at the commencement of any project, for the proactive establishment of and adherence to appropriate timelines, resourcing, cross-divisional consultation, quality assurance, supervision and attainment of necessary authorisation to publish submissions.