Local Government obligations under Part 4 of the *Privacy and Data Protection Act (2014)*

Introduction

The Victorian Government has committed to the effective management of information security risks within the Victorian public sector. This commitment will benefit the Victorian community by ensuring that government organisations adhere to a transparent set of security principles and are held accountable for protecting public sector information collected, held, used, managed, disclosed or transferred by it or its contractors.

The secure management of information is critical to Government service delivery, public trust and confidence.

What is the Victorian Protective Data Security Framework and the Victorian Protective Data Security Standards?

As required by Part 4 of the Privacy and Data Protection Act, 2014 (**PDP Act**), our office has published the Victorian Protective Data Security Framework (**Framework**) and issued the Victorian Protective Data Security Standards (**Standards**) to assist Victorian public-sector organisations meet their obligations for the protection of public sector information.

Aren't all Council functions exempt under Part 4 of the PDP Act?

Whilst Part 4, section 84 (2)(a) of the PDP Act explicitly excludes Councils, it is common for them to act as, or perform the functions of, a public entity. Common examples of a public entity include Committees of Management for Crown Land Reserves, Cemetery Trusts or a body that is government controlled[1].

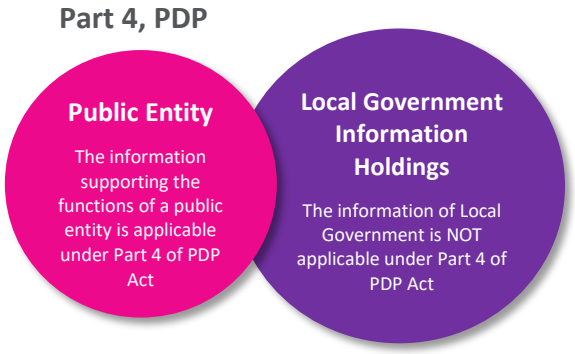
Obligations under Part 4

As outlined under the PDP Act a public entity must abide by the requirements outlined under Part 4 of the PDP Act. In doing so, Local Government have the following options.

[1] Refer to 'Does the VPDSF apply to your organisation' document on the OVIC website.

Option 1

Able to separate information holdings of the different entities:



Option 2

Unable to separate information holdings of the different entities:

Option 1 explained

Ideally, Local Government would be in a position to separate the information holdings relating to the public entity from its broader information holdings.

In doing so security measures outlined in the Standards can be limited to the public entity information holdings, and don't need to be applied to Local Government's broader information holdings.

While the requirements under the Part 4 of the PDP Act are only applicable to the functions of the public entity, more often than not, the information relating to the public entity is stored on, or processed using Local Government systems, personnel or facilities.

Option 2 explained

If Local Government is unable to separate the information relevant to the public entity from general Local Government information holdings, then the security measures outlined under the Standards need to be applied to all of Local Government's information holdings.

Accompanying reporting on the application of these security measures must also be supplied to OVIC as part of the requirements under the Framework and the Standards.

What are the benefits of implementing the Standards?

- ☑ Awareness of your organisation's information assets and their security value

  Understanding the breadth and security value of your organisation's information assets can help you identify information security risks, prioritise work and better manage resources.

- ☑ Supports Information Privacy Principle (IPP) 4.1

- ☑ Meeting your information security obligations as outlined in:

  - Health Privacy Principle (HPP) 4
  - Information Sharing Agreements and Memorandum of Understanding (MOU) and contracts
  - Third party arrangements (including government service providers and industry partners)
  - Other legal, regulatory and administrative requirements

What are my obligations under the Part 4 of the PDP Act 2014?

- ☑ Undertake a Security Risk Profile Assessment, and

- ☑ Develop a Protective Data Security Plan (PDSP)[2], and produce associated deliverables

What reporting do I need to provide to OVIC?

- ☑ You must provide a copy of your PDSP to OVIC every two years, or sooner in the event of significant change[3]

- ☑ A signed attestation must be provided by your public sector body Head annually, reaffirming your organisation's commitment to undertaking the works outlined in your PDSP

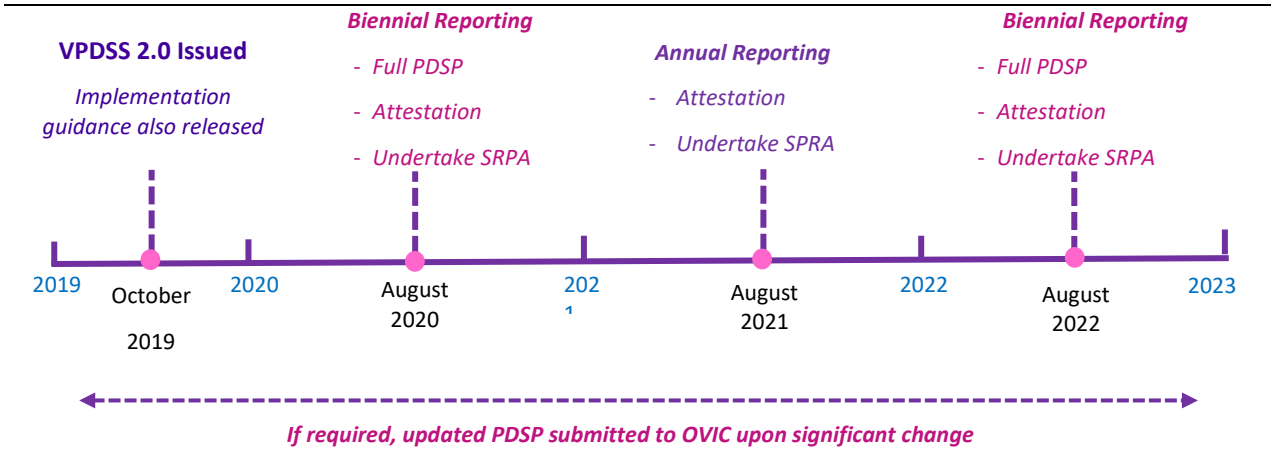
- ☑ Notify OVIC of any security incidents where there is a compromise of confidentialty, integrity or avialbility of information[4]

[2] Refer to PDP Act 2014, s89.

[3] Organisations that find themselves subject to a 'significant change', may seek to negotiate with OVIC on reporting timelines.

[4] For more information on the Incident Notification Scheme, please refer to the VPDSF Resources section of the OVIC website.

Visual representation of Reporting Timeframes and Deliverables



Who is ultimately accountable?

Under legislation, the public sector body Head of an agency or body is accountable under Part 4 of the PDP Act. For Local Government, this may be the **CEO** or **head of a Council.**

Where can I find out more?

ovic.vic.gov.au/data-protection

security@ovic.vic.gov.au