Protective data security in the Victorian public sector

No. 4, September 2017

Alice Petrie
Research & Inquiries Officer
Parliamentary Library & Information Service
Acknowledgments
The author would like to thank Debra Reeves, Marianne Aroozoo, Caley Otter, Igor Dosen, Bella Lesman, Jon Breukel, and Carolyn Macvean for their help in the preparation of this paper.
Contents

Abbreviations ................................................................................................................................. iv
Executive summary .......................................................................................................................... 1
Introduction ...................................................................................................................................... 2
1. Background .................................................................................................................................. 2
  2. Victorian Protective Data Security Framework ....................................................................... 5
     Victorian Protective Data Security Standards (VPDSS) .......................................................... 6
     Assurance model ....................................................................................................................... 8
     Security planning ..................................................................................................................... 8
     Organisational compliance ..................................................................................................... 8
     Risk-based assurance .............................................................................................................. 8
     Assurance reporting ................................................................................................................ 8
     Supplementary security guides and supporting resources ....................................................... 8
     Responses to the VPDSF ......................................................................................................... 9
     Victoria’s legislation and agency roles .................................................................................... 10
     Legislation .................................................................................................................................. 10
     Agency roles ............................................................................................................................ 11
3. International and domestic approaches to data security ......................................................... 13
   International .............................................................................................................................. 13
   International standards and guidelines .................................................................................. 13
   International law ...................................................................................................................... 14
   International collaboration ....................................................................................................... 14
   Federal ......................................................................................................................................... 15
   Legislation .................................................................................................................................... 15
   Policies and guidance .............................................................................................................. 15
   Agency roles ............................................................................................................................. 16
   Jurisdictional comparison—states and territories .................................................................. 18
References .......................................................................................................................................... 19
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACSC</td>
<td>Australian Cyber Security Centre (Federal)</td>
</tr>
<tr>
<td>AGD</td>
<td>Attorney-General’s Department (Federal)</td>
</tr>
<tr>
<td>APP</td>
<td>Australian Privacy Principle</td>
</tr>
<tr>
<td>APEC</td>
<td>Asia-Pacific Economic Cooperation</td>
</tr>
<tr>
<td>CSS</td>
<td>Cyber Security Strategy (Federal)</td>
</tr>
<tr>
<td>DPC</td>
<td>Department of Premier and Cabinet (Victoria)</td>
</tr>
<tr>
<td>FOI Amendment Act</td>
<td>Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017 (Vic)</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and communications technology</td>
</tr>
<tr>
<td>IPP</td>
<td>Information Privacy Principle</td>
</tr>
<tr>
<td>ISM</td>
<td>Information Security Manual (Federal)</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>OAIC</td>
<td>Office of the Australian Information Commissioner (Federal)</td>
</tr>
<tr>
<td>OCPDP</td>
<td>Office of the Commissioner for Privacy and Data Protection (Victoria)</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OECD Guidelines</td>
<td>Organisation for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data</td>
</tr>
<tr>
<td>OVIC</td>
<td>Office of the Victorian Information Commissioner</td>
</tr>
<tr>
<td>PDP Act</td>
<td>Privacy and Data Protection Act 2014 (Vic)</td>
</tr>
<tr>
<td>Privacy Act</td>
<td>Privacy Act 1988 (Cth)</td>
</tr>
<tr>
<td>PSPF</td>
<td>Protective Security Policy Framework (Federal)</td>
</tr>
<tr>
<td>VPDSF</td>
<td>Victorian Protective Data Security Framework</td>
</tr>
<tr>
<td>VPDSS</td>
<td>Victorian Protective Data Security Standards</td>
</tr>
<tr>
<td>WoVG</td>
<td>Whole of Victorian Government</td>
</tr>
</tbody>
</table>
Executive summary

Cyber crime is a rapidly evolving global threat to information and data security, and is estimated to cost the Australian economy around $1 billion each year.\(^1\) According to the federal government’s Cyber Security Strategy, threat actors target Australian government networks on an almost daily basis,\(^2\) compromising system security, service delivery and information access.

As the cyber threat environment evolves and becomes more sophisticated, it is critical to monitor and develop information security systems and capabilities to protect the privacy of individuals and their personal information, particularly in regard to sensitive data held by government agencies.\(^3\) Such agencies rely on this data to provide frontline operations and services, and it is therefore central to their effective operation that data integrity is maintained.

The Victorian Protective Data Security Framework (VPDSF) was released on 28 June 2016, taking effect from 1 July 2016.\(^4\) The VPDSF sets out its objectives as being to assist Victorian public service departments and agencies to ‘identify information and determine ownership, assess the value of information, identify and manage protective data security risks, apply security measures, create a positive security culture and mature their protective data security capability’.\(^5\)

The VPDSF defines protective data security as ‘the practice of implementing security measures to protect Victorian government information’.\(^6\) It aims to maintain the privacy of individuals without creating unnecessary barriers to the use and distribution of personal information within and between government agencies. While all Australian jurisdictions have some form of information security policy in place that governs public sector use of data, Victoria is the first state or territory to introduce an assurance model to complement its mandatory security standards.

The assurance model sets out certain compliance and assurance activities that public service organisations are required to undertake in order to assess their ongoing protective data security development in line with the VPDSF.

Each government organisation is required to develop, implement and maintain a Security Risk Profile Assessment and a Protective Data Security Plan.\(^7\) Organisations must then submit these plans to the Office of the Victorian Information Commissioner (OVIC) within two years after the issue of the Victorian Protective Data Security Standards (VPDSS), and review the documents every subsequent two years, or whenever there is a significant change to their operating or security environment.\(^8\)

In addition, organisations must report annually to the OVIC on their implementation of, and compliance with, the VPDSF, and also perform a maturity assessment in line with standard 12 of the VPDSS.

---

1 Department of the Prime Minister and Cabinet (2016) Australia’s Cyber Security Strategy, Canberra, DPMC, p. 15.
2 ibid., p. 36.
3 In this research paper, the terms public service or public sector ‘agencies’, ‘departments’, ‘bodies’ and ‘organisations’ will be used interchangeably to represent government bodies.
4 Commissioner for Privacy and Data Protection (2016) Victorian Protective Data Security Framework, Melbourne, OCPDP.
5 ibid., p. 12.
6 ibid., p. 11.
7 Privacy and Data Protection Act 2014 (Vic) (PDP Act), s 89(1).
8 ibid., s 89(4).
Introduction

The Victorian Government’s information security protections have undergone scrutiny in previous years from a number of state and federal government bodies and have received criticism for being considerably weak in relation to the existing threat environment. This was reinforced by the federal Cyber Security Operations Centre reporting in its Cyber Intrusion Activity Report, Australian State and Territory Governments: January–June 2013 that ‘The networks of the Victorian and West Australian state governments accounted for the highest proportion of cyber security incidents responded to ... between January and June 2013’. In response to this scrutiny, the Privacy and Data Protection Act 2014 (Vic) (PDP Act) was adopted and Victoria’s protective data security framework was subsequently developed.

This paper provides an overview of the VPDSF and the role it plays in protecting personal information held by government agencies.

Section 1 outlines the development of a protective data security framework in Victoria. Section 2 examines the structure of the VPDSF, its elements and responses to its introduction. Section 3 outlines the international and domestic context of issues surrounding protective data security, and how these have influenced, and contributed to, the development of Victoria’s own framework, and also offers a jurisdictional comparison of data security and privacy regimes within Australia at state and federal levels.

1. Background

In 2009, the Victorian Auditor-General undertook an investigation of the Victorian public sector’s information security framework. This examined the ways in which personal information was collected and stored by government agencies, the effectiveness of risk management and governance practices within individual agencies, and the sufficiency of central policy direction to ensure whole-of-government information security. The report, Maintaining the Integrity and Confidentiality of Personal Information, found that ‘central direction and effective coordination of the broad scope of information security risks remains weak’, and that in the absence of coordinated guidance and oversight, ‘the importance of protecting personal information has not been properly understood by the sector’.

A number of recommendations were contained in the report, including that the Victorian Government:

- expedite the release of a comprehensive, integrated suite of standards and guidance that address all aspects of information security including protective security, and which are based on risk and relevant to local conditions;
- mandate that all public sector agencies adopt the whole-of-government information security policies and standards;
- establish clear oversight to monitor implementation of information security policies and standards and compliance with the reporting requirements; and
- establish a process to identify and communicate emerging information security risks to the sector.

---

11 ibid., p. x.
Subsequent to this report, the Victorian Government developed its Information Security Management Policy (ISMP), which set out that specified departments and agencies must implement a revised set of policies, standards and guidelines relating to data privacy and information security. The revised framework centred on two documents created by the Australian Government: the Protective Security Policy Framework (PSPF), and the Information Security Manual (ISM). As part of the ISMP, specified agencies were each required to implement an Information Security Management Framework demonstrating that agency’s progress in complying with the Victorian adaptation of the PSPF and ISM as set out in SEC STD 01: Information Security Management Framework Standard.

The Victorian Auditor-General undertook another related audit in 2013 titled WoVG Information Security Management Framework, which examined the implementation of the Victorian Government’s ISMP and related standards within the specified public sector agencies, as well as the ongoing effectiveness of the regime. The report found that while the content of the ISMP was adequate, the mandatory implementation of the framework applied only to ‘inner’ and not ‘outer’ departments and agencies, meaning that over 500 ‘outer’ agencies were not required to adhere to any common security policy or standard. In addition, it found that ‘Agencies have not effectively implemented Victorian Government information security policy and standards. Agencies are potentially exposed to cyber attacks, primarily because of inadequate ICT [information and communications technology] security controls and immature operational processes.’ Further, the report concluded that there had been ‘inadequate central oversight of the ability of public sector systems to resist cyber attack and the follow up of the status of emerging or known cyber threats’. For example, Victorian public bodies experiencing significant cyber security threats were reporting these incidents directly to the federal Australian Signals Directorate, but not to any state-level agencies.

At the same time as the release of the report, the government announced the development of a new strategy targeting cyber security within its public sector framework. The Privacy and Data Protection Bill 2014 was introduced into the Legislative Assembly on 11 June 2014 by the Attorney-General, the Hon Robert Clark MP. The Bill passed both houses on 19 August 2014, and received Royal Assent on 2 September 2014. The Office for the Commissioner for Privacy and Data Protection (OCPDP) was subsequently established to administer the PDP Act and to develop a whole-of-government data security framework.

The VPDSF was released on 28 June 2016, taking effect from 1 July 2016. The VPDSF sets out its objectives as being to assist Victorian public service departments and agencies to ‘identify information

---

13 Attorney-General’s Department (2014) Protective Security Policy Framework, Canberra, AGD. For further discussion of this document see Section 3 of this paper.
14 Australian Signals Directorate (2016) Information Security Manual, Canberra, ASD. For further discussion of this document see Section 3 of this paper.
16 Victorian Auditor-General’s Office (2013) op. cit.
17 ibid., p. x.
18 ibid.
19 ibid., p. vii.
20 ibid., p. x.
22 Privacy and Data Protection Bill 2014 (Vic).
and determine ownership, assess the value of information, identify and manage protective data security risks, apply security measures, create a positive security culture and mature their protective data security capability’.24

On 1 September 2017 the OCPDP was amalgamated with the Office of the Freedom of Information Commissioner to create a combined OVIC, as per the Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017 (Vic) (FOI Amendment Act).25 OVIC has responsibility for the functions previously assigned to the OCPDP (for further information on these changes, see Section 3).

In addition to these developments, the Victorian Government has created and supported a number of initiatives over recent years to see Victoria transition into a ‘cyber security state’.26 In 2016, for example, the Victorian Government established a cyber security cluster in Melbourne at the Goods Shed, Docklands. This centre hosts the Data61 Cyber Security and Innovation Hub, the digital research arm of the Commonwealth Scientific and Industrial Research Organisation (CSIRO) alongside a new Oceania Cyber Security Centre. The Victorian Government has also signed agreements to establish within the hub a number of cyber security experts and organisations, including the University of Oxford’s Global Cyber Security Capacity Centre.27 The government’s aim for this research hub is to keep Victoria ‘at the forefront of Australia’s cyber security expertise and capabilities’,28 with these groups collaborating to undertake new research, reduce cyber security risks with assistance from private sector organisations, and perform audits at a national level of system capabilities and risks.29

The rapid growth of cyber security experts establishing at the Goods Shed has resulted in its recognition as the largest cyber security cluster in Australia.30

Further, the Victorian Government has recently announced its Cyber Victoria program, which seeks to ensure that Victoria is home to the ‘most skilled cyber workforce in the Asia Pacific region’, and to provide resources to improve the cyber capacity of existing and emerging companies.31 The Victorian Government’s emphasis on its own public sector’s data security is set within this context.

24 ibid., p. 12.


30 Invest Victoria (2017) Victoria to become Australia’s first cyber ready state, media release, 29 May.

2. Victorian Protective Data Security Framework

The overarching purpose of the VPDSF is to ‘establish, monitor and assure security of information within the Victorian Government’. The framework also aims to encourage a cultural shift in the way protective data security is considered on a day-to-day basis, aiming to fortify it as a necessary element of any operating environment.

The VPDSF consists primarily of the Victorian Protective Data Security Standards (VPDSS), the assurance model, and a number of supplementary security guides and supporting resources. Figure 1 provides an overview of the structure of the VPDSF, with the assurance model overlaying the framework.

**Figure 1. VPDSF structural overview**

A number of guiding principles set out the concepts supporting the general themes contained within the VPDSF. These relate to the establishment of:

- strong governance arrangements to ensure protective data security requirements are reflected in organisational planning;
- risk management;
- an understanding of information value;
- a positive security culture with clear personal accountability and a mature understanding of managing risk, responsibility and reputation;
- a continuous improvement lifecycle model to facilitate opportunities to improve organisational practices; and
- the ability of sound protective data security practices to assist an organisation to achieve its objectives.

---

33 ibid., p. 9.
34 ibid., p. 25.
The guiding principles correlate to the VPDSS, which are implemented under plans set out within the assurance model. The former OCPDP (now OVIC), in addition, issued a number of supplementary security guides and supporting resources to assist organisations in fulfilling their obligations. These various elements are interrelated to establish an all-encompassing protective data security regime.

Where personal information held by a Victorian public sector agency has national interest, the requirements under the federal PSPF supersede those of the VPDSF.

**Victorian Protective Data Security Standards (VPDSS)**

The VPDSS comprise 18 standards, each of which are supported by four protocols, which together provide ‘a set of criteria for the consistent application of risk-managed security practices across Victorian government information’. The VPDSF sets out that these standards should be planned, implemented, monitored on an ongoing basis, and improved as necessary by Victorian public sector agencies. They are grouped into areas of security governance (12 standards) and the four security domains: information security (three standards), personnel security (one standard), ICT security (one standard) and physical security (one standard). Organisations are required to adhere to the VPDSS in line with the compliance requirements set out in section 88 of the PDP Act.

Organisations are also required to comply with the 10 Information Privacy Principles (IPPs) set out in Schedule 1 of the PDP Act, which govern the collection and use of personal information by public service bodies. The IPPs and the VPDSS are closely related. Under IPP 4.1, government agencies are required to ‘... take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure’. The VPDSF sets out that organisations should use the VPDSS as the primary reference point in terms of ensuring compliance with this IPP.

The VPDSS are consistent with the standards set out in the federal PSPF, but also contain a number of variances, which reflect the distinct operating requirements of Victoria’s public service. Many of the standards similarly refer to the implementation of International Organization for Standardization (ISO) standards, and measures contained within the Australian Signals Directorate’s ISM, in recommending adequate controls (these documents are discussed in the international and federal sections of Section 3 below).

Table 1 sets out the standards and the required output for implementation.

**Table 1. Victorian Protective Data Security Standards**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Security Management Framework <em>(Security governance)</em></td>
<td>An organisation must establish, implement and maintain a security management framework proportionate to their size, resources and risk posture.</td>
</tr>
</tbody>
</table>

---

35 ibid., p. 31.
36 PDP Act, sch 1 s 4(1).
<table>
<thead>
<tr>
<th></th>
<th>Security Policies and Procedures <em>(Security governance)</em></th>
<th>An organisation must establish, implement and maintain security policies and procedures proportionate to their size, resources and risk posture.</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Information Access <em>(Security governance)</em></td>
<td>An organisation must establish, implement and maintain an access management regime for access to public sector data.</td>
</tr>
<tr>
<td>5</td>
<td>Security Obligations <em>(Security governance)</em></td>
<td>An organisation must define, document, communicate and regularly review the security obligations of all persons with access to public sector data.</td>
</tr>
<tr>
<td>6</td>
<td>Security Training and Awareness <em>(Security governance)</em></td>
<td>An organisation must ensure all persons with access to public sector data undertake security training and awareness.</td>
</tr>
<tr>
<td>7</td>
<td>Security Incident Management <em>(Security governance)</em></td>
<td>An organisation must establish, implement and maintain a security incident management regime proportionate to their size, resources and risk posture.</td>
</tr>
<tr>
<td>8</td>
<td>Business Continuity Management <em>(Security governance)</em></td>
<td>An organisation must establish, implement and maintain a business continuity management program that addresses the security of public sector data.</td>
</tr>
<tr>
<td>9</td>
<td>Contracted Service Providers <em>(Security governance)</em></td>
<td>An organisation must ensure that contracted service providers with access to public sector data, do not do an act or engage in a practice that contravenes the VPDSS.</td>
</tr>
<tr>
<td>10</td>
<td>Government Services <em>(Security governance)</em></td>
<td>An organisation that receives a government service from another organisation must ensure that the service complies with the VPDSS in respect to public sector data that is collected, held, used, managed, disclosed or transferred.</td>
</tr>
<tr>
<td>11</td>
<td>Security Plans <em>(Security governance)</em></td>
<td>An organisation must establish, implement and maintain a protective data security plan to manage their security risks.</td>
</tr>
<tr>
<td>12</td>
<td>Compliance <em>(Security governance)</em></td>
<td>An organisation must perform an annual assessment of their implementation of the VPDSS and report their level of compliance to the Victorian Information Commissioner.</td>
</tr>
<tr>
<td>13</td>
<td>Information Value <em>(Information security)</em></td>
<td>An organisation must conduct an information assessment considering the potential compromise to the confidentiality, integrity and availability of public sector data.</td>
</tr>
<tr>
<td>14</td>
<td>Information Management <em>(Information security)</em></td>
<td>An organisation must establish, implement and maintain information security controls in their information management framework.</td>
</tr>
<tr>
<td>15</td>
<td>Information Sharing <em>(Information security)</em></td>
<td>An organisation must ensure that security controls are applied when sharing public sector data.</td>
</tr>
<tr>
<td>16</td>
<td>Personnel Lifecycle <em>(Personnel security)</em></td>
<td>An organisation must establish, implement and maintain personnel security controls in their personnel management regime.</td>
</tr>
<tr>
<td>17</td>
<td>Information Communications Technology (ICT) Lifecycle <em>(ICT security)</em></td>
<td>An organisation must establish, implement and maintain Information Communications Technology (ICT) security controls in their ICT management regime.</td>
</tr>
<tr>
<td>18</td>
<td>Physical Lifecycle <em>(Physical security)</em></td>
<td>An organisation must establish, implement and maintain physical security controls in their physical management regime.</td>
</tr>
</tbody>
</table>

Source: Information sourced from Victorian Protective Data Security Framework, pp. 32-49
Assurance model

The assurance model sets out certain compliance and assurance activities that public service organisations are required to undertake in order to assess their ongoing protective data security development in line with the VPDSF. The OVIC plays a core role within the assurance model in working with organisations to ensure continuing capability development and best practice security resilience and effectiveness. In this way, organisations are able to provide assurance to the OVIC, which then reports to the Victorian Government on the broader security of information held within its public sector.

Security planning
Each government organisation is required to develop, implement and maintain a Security Risk Profile Assessment (assessing the organisation’s data security risks) and a Protective Data Security Plan (including action items to address identified data security risks). Organisations are required to submit these documents to the OVIC within two years after the issue of the above VPDSS. Every organisation to whom the protective data security provisions under Part 4 of the PDP Act applies will then be required to review these documents every subsequent two years, or whenever there is a significant change to their operating or security environment. Organisations may also seek customised protective data security standards where certain operating conditions or requirements necessitate a departure from the standard VPDSS.

Development of a Security Risk Profile Assessment and Protective Data Security Plan is also set out as a requirement in standards 2 and 11 of the VPDSS. These documents will assist the OVIC in conducting its security monitoring and assurance activities.

Organisational compliance
Organisations must report annually to the OVIC on their implementation of, and compliance with, the VPDSF, and also perform a maturity assessment in line with standard 12 of the VPDSS.

Risk-based assurance
The OVIC will implement its obligations under the assurance model by assessing each organisation’s implementation of the VPDSF, and the broader development of Victoria’s overall protective data security. Organisations must assist the OVIC by providing requested information or documents where necessary, as well as access to data systems to ensure a full assessment.

Assurance reporting
The OVIC has a number of reporting obligations, including reporting annually to the Special Minister of State on the ongoing maturity of the Victorian public sector with the protective data security model.

Supplementary security guides and supporting resources
The former OCPDP produced a number of additional materials to assist public sector organisations to comply with their obligations under the PDP Act and VPDSF, which are now publicly available under the ‘data security resources’ section of the OVIC webpage. This includes the VPDSF Information

---

38 PDP Act, s 89(1).
39 ibid., s 89(4).
40 ibid., s 86.
Security Management Collection, which provides guidance on the implementation of the VPDSS and how to identify and manage information assets and value.

Responses to the VPDSF

The VPDSF has received a generally favourable response. In particular, it has been described as ‘showing determined cyber security leadership from central government while offering a progressive information assurance framework that can be used as a benchmark for all other states’. In relation to the previous Victorian Auditor-General’s reports, which revealed weak security practices within a number of Victorian Government agencies, the inclusion of an assurance model now ensures that government bodies will have to demonstrate their compliance with, and implementation of, information security policies for the first time. The various elements of the assurance model, including requirements for annual reporting, encourage a cultural shift to consider data security as an integral part of each agency’s business model. Looking forward, Victorian Auditor-General’s Office announced in its Annual Plan 2017–18 that it will commence a review into the effectiveness of the VPDSF and the VPDSS, and their ability to improve public sector cyber resilience, in 2018–19.

The VPDSF has further been described as being ‘light on prescriptive or practical demands on how agencies should actually build security into their systems and operations’. Instead, it lists a number of external policies and standards to be employed. For example, many of the VPDSS implement elements of the internationally accepted ISO suite of standards, the use of which will allow for a ‘much more flexible approach to implementation’ as information security professionals will already be familiar with these standards. Noting the breadth of organisations to which the framework applies, the VPDSF also provides caveats that internal procedures should be proportionate to each agency’s specific situation, affording space for flexible implementation as required.

On a broader level, the various privacy and information security regimes across Australia remain complex to navigate, creating difficulties for the private sector in terms of having to comply with diverse obligations when engaging in business or contractual arrangements across multiple jurisdictions. Neither South Australia nor Western Australia, for example, have enacted specific privacy legislation (see the jurisdictional comparison in Section 4). Stronger collaboration and coordination across federal and state governments could assist the growth of data security capability within Australia as new cyber threats emerge.

---

42 Commissioner for Privacy and Data Protection (2017) VPDSF Information Security Management Collection, Melbourne, OCPDP.
46 P. Cowan (2016) op. cit.
47 T. Campbell (2016) op. cit.
48 P. Cowan (2016) op. cit.
49 For a discussion of the harmonisation of these varying policies, see V. Draudins (2017) ‘Harmonising Australia’s privacy regime’, The Mandarin, 1 August.
50 For example, through the ongoing establishment of Joint Cyber Security Centres. See G. Brandis, Attorney-General, and D. Tehan, Minister Assisting the Prime Minister on Cyber Security (2017) Turnbull Government launches first Joint Cyber Security Centre, media release, 24 February.
Victoria’s legislation and agency roles

Legislation

**Privacy and Data Protection Act 2014 (Vic)**

The PDP Act came into effect on 17 September 2014, and repealed and replaced the *Information Privacy Act 2000* (Vic) (Information Privacy Act) and the *Commissioner for Law Enforcement Data Security Act 2005* (Vic). In doing so, the PDP Act merged the two separate roles of Privacy Commissioner and Commissioner for Law Enforcement Data Security into one Commissioner for Privacy and Data Protection, to administer the new data protection regime. These roles were again amended by the FOI Amendment Act (see ‘other legislation’ below).

While many of the provisions relating to privacy in the PDP Act are similar to those previously contained in the Information Privacy Act, the PDP Act also contains a number of new measures and mechanisms to provide for a more comprehensive whole-of-government framework specifically targeted at protecting data held by Victorian public sector agencies.

**Purpose**

The PDP Act creates a framework for the responsible collection and handling of personal information within the Victorian public sector; provides remedies for interferences with such information; and provides for the establishment of a protective data security regime for the Victorian public sector.

According to the former OCPDP, the PDP Act is ‘the first piece of legislation in Australia to combine privacy and data protection regimes into a single regulatory framework’.

**Application**

In regard to the information privacy aspects of the PDP Act, Victorian public sector bodies must adhere to the 10 IPPs set out in Schedule 1, which govern the collection and use of personal information by government agencies, and which are based on the Organisation for Economic Co-operation and Development’s (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines). Organisations must not commit an act, or engage in a practice, that contravenes an IPP in respect of personal information collected, held, managed, used, disclosed or transferred by it, unless otherwise permitted to do so. Alongside permitted departure from some IPPs for law enforcement purposes, bodies are also able to depart from IPPs in conjunction with certain mechanisms where it is determined to be in the public interest.

The protective data security provisions under Part 4 of the PDP Act apply to Victorian public service organisations and agencies, but do not apply to local councils, universities, public hospitals or health services, or ambulance services. The provisions are also binding on service providers performing a contract with a Victorian public service body.

---

51 PDP Act as originally passed, pt 6.
53 See Section 3 for more information on this document.
54 PDP Act, s 20(1).
55 These mechanisms are set out in the PDP Act as public interest determinations, temporary public interest determinations, and information usage arrangements. See PDP Act, divs 5-6.
56 PDP Act, s 84. It is not explained in this Act nor in its explanatory materials why these bodies are exempt from compliance with the VPDSF.
Part 4 also sets out that the Victorian Information Commissioner (previously the Commissioner for Privacy and Data Protection) is required to develop a protective data security framework for monitoring and assuring the security of public sector data. In addition, it establishes that the Victorian Information Commissioner may issue protective data security standards for the security, confidentiality and integrity of public sector data.\(^{57}\)

**Other legislation**

*Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017*

The FOI Amendment Act received Royal Assent on 16 May 2017. This Act provided for the amalgamation of the OCPDP with the Office of the Freedom of Information Commissioner to create the OVIC. Attorney-General Martin Pakula MP stated during the second reading speech on the Bill that this merger would bring Victoria’s privacy and information regimes into line with the systems established in New South Wales, Queensland and the Commonwealth.\(^{58}\) Despite these changes, the privacy and data protection obligations of public sector agencies as set out within the PDP Act remain the same.

OVIC assumed the functions of the above two offices from 1 September 2017.

*Health Records Act 2001 (Vic)*

Health information is excluded from the provisions of the PDP Act. Instead, the *Health Records Act 2001 (Vic)* (the HRA) sets out how data pertaining to health is collected and handled by public agencies in Victoria.\(^{59}\) The Health Services Commissioner administers the HRA, and it includes a number of Health Privacy Principles which are similar in nature to the IPPs.

*Charter of Human Rights and Responsibilities Act 2006 (Vic)*

Section 13 of the *Charter of Human Rights and Responsibilities Act 2006 (Vic)* (the Charter) confers a right to privacy, which provides that an individual’s personal information cannot be unlawfully or arbitrarily interfered with.\(^{60}\)

The Victorian Government, public authorities and local councils must consider the rights contained in the Charter, including the right to privacy, when drafting new laws, and set out the compatibility of the draft legislation with those rights in a statement of compatibility presented to the Victorian Parliament.

The Parliament’s Scrutiny of Acts and Regulations Committee is required to scrutinise all Bills and Statutory Rules for their compatibility with human rights as set out in the Charter, and report to the Parliament on their findings. This committee’s functions are set out in section 17 of the *Parliamentary Committees Act 2003 (Vic)*, and include a requirement to report to the Parliament on whether any bill ‘unduly requires or authorises acts or practices that may have an adverse effect on personal privacy within the meaning of the Privacy and Data Protection Act 2014’.\(^{61}\)

**Agency roles**

*Office of the Victorian Information Commissioner*

The OCPDP was established in September 2014, and Part 6 of the PDP Act as passed set out one of its functions as the administration of that Act. Within that office, the Commissioner for Privacy and Data Protection is required to develop a protective data security framework for monitoring and assuring the security of public sector data. In addition, it establishes that the Victorian Information Commissioner may issue protective data security standards for the security, confidentiality and integrity of public sector data and access to public sector data.\(^{57}\)

\(^{57}\) ibid., pt 4.


\(^{59}\) Health Records Act 2001 (Vic).

\(^{60}\) Charter of Human Rights and Responsibilities Act 2006 (Vic).

\(^{61}\) Parliamentary Committees Act 2003 (Vic), s 17(a)(iv).
Protection’s functions included to issue protective data security standards and law enforcement data security standards; develop the Victorian protective data security framework and to promote the uptake of the standards by the public sector; and conduct monitoring and assurance activities, including audits, to ascertain compliance with data security standards.

From 1 September 2017, the OVIC commenced operations.62 The OVIC is headed by the Information Commissioner, and supported by the Privacy and Data Protection Deputy Commissioner and Public Access Deputy Commissioner. The role previously performed by the Commissioner for Privacy and Data Protection, in relation to the regulation of activity concerning information privacy, protective data security and law enforcement data security, was conferred upon the Information Commissioner.63

**Department of Premier and Cabinet**

The Department of Premier and Cabinet (DPC) is the central coordination agency for issues relating to cyber security and information technology, and is responsible for coordinating critical hazard responses, including in relation to cyber attacks. DPC also supports the administrative functions of the OVIC.

As part of the Victorian Government’s **Information Technology Strategy for the Victorian Government, 2016 to 2020**, DPC committed to creating a state strategy for cyber security.64 This strategy was developed by the Cyber Security Strategy Group, composed of experts from both the federal and Victorian governments as well as major enterprises. The **Victorian Cyber Security Strategy** was launched by the Special Minister of State on 25 August 2017.65 Within this framework, the Victorian Government has committed to a number of actions relating to public engagement, planning, partnering, service maturity and capability, with the purpose of developing and implementing cyber security capabilities across government.66 These actions include:

- appointment of a Chief Information Security Officer for the Victorian Government within DPC who will be responsible for implementing the **Victorian Cyber Security Strategy**;
- standardised reporting and communication requirements across all departments and agencies;
- development and operation of a communication and engagement program for cyber security awareness within the Victorian Government;
- establishment of formal channels and mechanisms to engage with Australian Government cyber security services and strategic planning; and
- development of emergency governance structures, such as with Emergency Management Victoria.67

The initiatives contained in this strategy are intended to support the principles and approach of the VPDSF.68

---

63 PDP Act, s 8A.
66 ibid., p. 2.
67 ibid., pp. 23-25.
68 ibid., p. 6.
3. International and domestic approaches to data security

This section will broadly examine the structure and development of information security and data privacy frameworks—including the main policy guidance and standards issued at international and federal levels, and a jurisdictional comparison of the comparable data privacy regimes of the states and territories—and how these have influenced Victoria’s own framework.

International

International standards and guidelines

*Organisation for Economic Co-operation and Development*

The OECD developed its OECD Guidelines in 1980, which constituted the first collaborative international privacy framework.69 These guidelines were developed by an Expert Group consisting of representatives of the OECD member countries, chaired by then-Chairman of the Australian Law Reform Commission, the Hon. Justice Michael Kirby. They set out a number of basic principles which could be incorporated into existing or draft legislation, with the aim of enabling the free flow of information across borders while protecting fundamental rights and liberties, such as privacy. The OECD recommended the cooperation and collaboration of member states in their implementation of the guidelines and the creation of specific procedures of consultation for their application.

Specifically, the OECD Guidelines set out eight basic principles (to be considered as minimum standards) as agreed by the Expert Group, which relate to data collection, use, disclosure, quality, security, transparency and accountability.70 These were updated in 2013 to respond to a rapidly changing digital environment, including in relation to the volume of personal data being collected, used and stored, the extent of threats to privacy, and the number and variety of actors capable of either putting privacy at risk or protecting privacy.71 While the basic principles remained the same, new concepts were introduced which included national privacy strategies (with co-ordination at the highest level of government) and data security breach notification (covering both notice to an authority and notice to an individual affected by a security breach).72

The Australian Privacy Principles (APPs) set out in the *Privacy Act 1988* (Cth) (Privacy Act),73 and the IPPs contained in the PDP Act, are largely based on the OECD Guidelines.

*International Organization for Standardization*

The ISO is an international non-governmental organisation that brings together the national standards organisations of 163 countries. The ISO develops collaborative international standards aimed at ensuring the quality, safety and efficiency of services and systems across a variety of industries and technologies, assisting the facilitation of international trade.

---


70 ibid.


72 ibid., p. 4.

73 *Privacy Act 1988* (Cth) (Privacy Act).
The ISO 27000 series of standards ‘provide best practice recommendations on risks and controls within the context of an overall information security management system’. These are widely accepted as the global standards for information security policy, and they inform the development of security frameworks within both the public and private sectors, including the VPDSF.

**International law**

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides for certain protections relating to privacy (including information privacy), and prohibits any unlawful or arbitrary interference with this right. The United Nations Human Rights Committee, the treaty monitoring body for the ICCPR, has set out that ‘The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.’ Australia, as a party to this covenant, therefore has an obligation under international law to ensure that individuals’ right to privacy is protected, and only limited in certain circumstances.

In addition, the Human Rights Committee has stated that ‘every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files.’ This confers an obligation on State Parties to the ICCPR to ensure that relevant domestic privacy laws enable individuals to ascertain from public bodies the private information held about them by those bodies.

While the ICCPR does not operate as a direct source of law in Australia (meaning that it has not been wholly incorporated into domestic law), Australia has voluntarily committed to adhere to the rights set out in the covenant, and is required to report periodically to the Human Rights Committee on its progress in implementing those rights. Certain provisions of the various treaties and conventions to which Australia is a party, however, reflected in domestic legislation, including in relation to domestic privacy law.

**International collaboration**

Australia collaborates internationally on issues relating to data privacy and cyber security through membership of international organisations and working groups, defence and security exercises, and information sharing. Australia is, for example, a member of the Asia-Pacific Economic Cooperation (APEC) Data Privacy Sub Group that developed the *APEC Privacy Framework* in 2004, and the federal Office of the Australian Information Commissioner (OAIC) is a participant of the *APEC Cross-border Privacy Enforcement Arrangement*, which promotes regional cooperation on information privacy legislation and its enforcement. The APEC privacy framework also contains nine core privacy principles representing a minimum standard for its members (and was developed in accordance with the OECD Guidelines discussed above). Australia has also, for example, cooperated with Canada, New Zealand, and other countries.

---


77 ibid., p. 3.


the United Kingdom and the United States as part of the International Computer Network Defence Coordination Working Group, which promotes information sharing on international cyber security issues.\(^{81}\)

**Federal**

**Legislation**

*Privacy Act 1988 (Cth)*

The Privacy Act came into operation on 1 January 1989, and gave effect to Australia’s commitment to implement into domestic law the OECD Guidelines, as well as its obligations in relation to the right to privacy as contained in article 17 of the ICCPR.

The Privacy Act regulates how information is stored, used and protected by federal public sector agencies, and some large Australian companies. It contains 13 APPs which are based on the principles established in the OECD Guidelines.\(^{82}\) Federal government bodies are required to adhere to these APPs when interacting with personal information.

**Policies and guidance**

*Protective Security Policy Framework (PSPF)*

The Attorney-General’s Department (AGD) manages the PSPF, which is the overarching Australian Government policy regarding data privacy and security.\(^{83}\) The individual information security procedures of each federal agency are required to adhere to this framework, which contains 36 mandatory requirements to assist those bodies to manage security risks, provide assurance to the government and public, and assist the growth of a protective data security culture.\(^{84}\)

The PSPF also includes a mandatory audit, review and reporting process, with each department or agency preparing a self-assessment report that is submitted to the relevant portfolio minister. The PSPF is currently under review, in response to recommendations from the *Independent Review of Whole-of-Government Internal Regulation*.

*Information Security Manual (ISM)*

The ISM is the standard governing the security of Australian Government ICT systems and supplements the PSPF.\(^{85}\) The ISM supports the strategic priorities set out in the federal government’s *Cyber Security Strategy (CSS)* by ‘providing detailed information about the cyber security threat, as well as assisting agencies in determining appropriate controls to protect their information and systems’.\(^{86}\) The Australian Signals Directorate issues the ISM.

The ISM also provides further detail regarding required implementation of the *Strategies to Mitigate Cyber Security Incidents*,\(^{87}\) also known as the ‘Top 4’ Strategies (updated in 2017 to replace the former

---


\(^{82}\) Privacy Act, sch 1.

\(^{83}\) Attorney-General’s Department (2014) op. cit.


\(^{87}\) Australian Signals Directorate (2017) *Strategies to Mitigate Cyber Security Incidents*, Canberra, ASD.
Strategies to Mitigate Targeted Cyber Intrusions). The Australian Signals Directorate has estimated that implementation of the Top 4 Strategies will mitigate ‘at least 85% of the adversary techniques used in targeted cyber intrusions’ that it has observed.

Cyber Security Strategy (CSS)

The Department of Prime Minister and Cabinet published its most recent CSS in 2016. The CSS introduces five main priorities for Australia’s cyber security development leading up to 2020, including emphasis on a national cyber partnership and strong cyber defences. Further, it establishes an operational model for joint cyber security centres in key capital cities to promote information sharing between federal and state governments and the private sector. The first such centre opened in Brisbane in February 2017, with centres planned to open in Sydney, Melbourne and Perth by the end of 2017. The first annual update to this report was released in April 2017.

Agency roles

A number of federal departments and agencies have roles relating to the implementation of data privacy and information security policies, guidelines and strategies. The leading agencies are briefly outlined below.

Office of the Australian Information Commissioner (OAIC)

The OAIC is a federal independent statutory agency administered by the AGD, which was established in 2010 by the Australian Information Commissioner Act 2010 (Cth) (AIC Act). The OAIC houses the Australian Information Commissioner, who is required under the AIC Act to report to the Attorney-General on ‘the collection, use, disclosure, management, administration or storage of, or accessibility to, information held by the Government’, and the systems used to provide for these activities. One of the OAIC’s primary functions is in relation to privacy law and policy, conferred upon it by the Privacy Act and other laws. The OAIC administers the APPs discussed above, and provides advice and guidance to agencies and organisations on the application and requirements of the Privacy Act.

The OAIC announced in May 2017, together with the Department of Prime Minister and Cabinet, the joint development of a new Privacy Code to ‘enhance the capability of Commonwealth agencies to deliver data innovation that integrates personal data protection’. The new Privacy Code is expected to be implemented in 2018.

---

88 Department of the Prime Minister and Cabinet (2017) ASD releases Essential Eight Maturity Model, media release, Canberra, DPMC, 7 July.
89 Australian Signals Directorate (2017) op. cit.
90 Department of the Prime Minister and Cabinet (2016) op. cit.
91 ibid., p. 5.
92 ibid., p. 59.
93 G. Brandis, Attorney-General, and D. Tehan, Minister Assisting the Prime Minister on Cyber Security (2017) op. cit.
95 ibid.
96 Australian Information Commissioner Act 2010 (Cth), pt 2 div 3(7).
97 Department of the Prime Minister and Cabinet and Office of the Australian Information Commissioner (2017) Developing an APS-wide Privacy Code, media release, Canberra, DPMC & OAIC.
**Australian Cyber Security Centre (ACSC)**

The Australian Cyber Security Centre (ACSC) (previously the Cyber Security Operations Centre) is the Australian Government’s lead agency for operational responses to cyber attacks, as well as the central hub for collaboration between the public and private sector on issues relating to cyber security. In addition, it reports on the nature and extent of emerging and existing threats. The ACSC coordinates cyber security capabilities from across the Australian Government, including the Australian Signals Directorate, AGD, Australian Security Intelligence Organisation, Australian Federal Police and the Australian Criminal Intelligence Commission. On 18 July 2017, it was announced that the ACSC would establish 24/7 capability to respond to ‘serious cyber incidents’.

**Department of Prime Minister and Cabinet**

The Department of Prime Minister and Cabinet is the lead federal government department for developing cyber security policy, and implements the CSS. It also hosts a Public Data Branch, which has a number of functions relating to data capability, privacy and accessibility.

**Attorney-General’s Department (AGD)**

The AGD coordinates a number of initiatives relating to protective security policy and cyber security through its Cyber Crime and Security Branch. This includes the National Computer Emergency Response Team, who are the first point of contact within government for non-government bodies experiencing cyber threats, and who coordinate with the ACSC to share data on cyber incidents. The AGD also manages the Trusted Information Sharing Network for Critical Infrastructure Resilience, which provides a secure environment for the sharing of information across sectors to address critical security issues. In addition, the AGD will coordinate the new joint cyber security centres.

---

98 Department of the Prime Minister and Cabinet (2017) *Press Conference with the Prime Minister, the Hon. Malcolm Turnbull MP, Attorney-General, Senator the Hon. George Brandis QC, Minister for Immigration and Border Protection, the Hon. Peter Dutton MP and Minister for Justice, the Hon. Michael Keenan MP*, Canberra, 18 July.

<table>
<thead>
<tr>
<th></th>
<th>VIC</th>
<th>WA</th>
<th>SA</th>
<th>TAS</th>
<th>QLD</th>
<th>NSW</th>
<th>NT</th>
<th>ACT</th>
<th>Commonwealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevance</td>
<td>Privacy and Data Protection Act 2014 (Vic)</td>
<td>None. The Information Privacy Bill 2007 (containing a</td>
<td>None. SA has a non-legislative administrative scheme</td>
<td>Personal Information and Protection Act 2004 (Tas)</td>
<td>Information Privacy 2009 (QLD)</td>
<td>Privacy and Personal Information Protection Act 1998 (NSW).</td>
<td>Information Act 2002 (NT)</td>
<td>Information Privacy Act 2014 (ACT) (Replaced the previously used Privacy Act 1988 (Cth))</td>
<td>Privacy Act 1988 (Cth)</td>
</tr>
<tr>
<td>Relevant</td>
<td>legislation featuring use of personal data by public</td>
<td>agencies</td>
<td></td>
<td></td>
<td></td>
<td>NSW was the first state to enact public sector privacy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>agencies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>laws</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>principles contained in legislation</td>
<td>Information Privacy Principles (IPPs), Privacy and</td>
<td>None. Some principles are broadly enshrined within the</td>
<td>Personal information protection principles (PIPPs),</td>
<td>Information Protection Principles (IPPs), Information</td>
<td>Information Protection Principles (IPPs), Privacy and</td>
<td>Information Protection Principles (IPPs),</td>
<td>Information Protection Principles (IPPs),</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>principles</td>
<td></td>
<td>Contains 11 principles</td>
<td></td>
<td>div 1</td>
<td></td>
<td>Contains 10 principles which are similar to the Victorian IPPs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existence of</td>
<td>Victorian Information Commissioner, and Privacy and</td>
<td>WA Information Commissioner, dealing only with freedom</td>
<td>None. The IPPs are overseen by a Privacy Committee</td>
<td>QLD Privacy Commissioner</td>
<td>NSW Privacy Commissioner</td>
<td>NT Information Commissioner</td>
<td>Australian Information Commissioner</td>
<td>Australian Information Commissioner (under arrangement between the ACT government and the federal government)</td>
<td></td>
</tr>
<tr>
<td>a relevant</td>
<td>Data Protection Deputy Commissioner (previously the</td>
<td>of information issues</td>
<td>None. The Tasmanian Ombudsman is responsible for</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commissioner</td>
<td>Commissioner for Privacy and Data Protection)</td>
<td></td>
<td>complaints-handling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right to</td>
<td>Charter of Human Rights and Responsibilities Act 2006</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Human Rights Act 2004 (ACT) s 12</td>
<td>No</td>
</tr>
<tr>
<td>privacy</td>
<td>(VIC) s 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>legislated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
References


Department of Premier and Cabinet (2017) *Cyber Security Strategy*, Melbourne, DPC.


Department of the Prime Minister and Cabinet (2017) *ASD releases Essential Eight Maturity Model*, media release, Canberra, DPMC, 7 July.


Department of Premier and Cabinet (2017) *Cyber Security Strategy*, Melbourne, DPC.


Department of the Prime Minister and Cabinet (2017) *Press Conference with the Prime Minister, the Hon. Malcolm Turnbull MP, Attorney-General, Senator the Hon. George Brandis QC, Minister for Immigration and Border Protection, the Hon. Peter Dutton MP and Minister for Justice, the Hon. Michael Keenan MP*, Canberra, 18 July.
Department of the Prime Minister and Cabinet (2017) *Australia's Cyber Security Strategy: 2017 Update*, Canberra, DPMC.

Department of the Prime Minister and Cabinet (2016) *Australia’s Cyber Security Strategy*, Canberra, DPMC.

Department of the Prime Minister and Cabinet (2017) *Press Conference with the Prime Minister, the Hon. Malcolm Turnbull MP, Attorney-General, Senator the Hon. George Brandis QC, Minister for Immigration and Border Protection, the Hon. Peter Dutton MP and Minister for Justice, the Hon. Michael Keenan MP*, Canberra, 18 July.

Department of the Prime Minister and Cabinet and Office of the Australian Information Commissioner (2017) *Developing an APS-wide Privacy Code*, media release, Canberra, DPMC & OAIC.


UN Human Rights Committee (1988) *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April, Geneva, HRC.


Research & Inquiries Service

Research papers are produced by the Library’s Research & Inquiries service. They provide in-depth coverage and detailed analysis of topics of interest to Members of Parliament. Research publications are prepared for Parliament in response to Members, and in anticipation of their requirements, in areas of interest to the Victorian legislature.

Information in this paper was current as at the time of printing. It should not be considered as a complete guide to the particular subject or legislation covered. While it is intended that all information provided is accurate, it does not represent professional legal opinion. Any views expressed are those of the author(s).

Some hyperlinks may only be accessible on the Parliament of Victoria’s intranet. All links are current and available as at the time of publication.

Enquiries:
Jon Breukel
Coordinator, Research & Inquiries
Victorian Parliamentary Library & Information Service
Parliament House
Spring Street, Melbourne
Telephone (03) 9651 8633
www.parliament.vic.gov.au