Privacy and Data Protection Bill 2014

Overview
11, 12 June 2014
Introduced & 2nd read in Legislative Assembly

5 Aug 2014
Debate listed to resume in Legislative Assembly

9 Dec 2014 (or earlier)
Commences – if passed and assented to
Overview: key elements

Purposes

Part 2: Application

Part 3: Information Privacy

Part 4: Protective Data Security

Part 5: Law Enforcement Data Security

Part 6: Commissioner for Privacy and Data Protection
Bill Purposes

To:

1. provide for **responsible collection and handling of personal information** in the Victorian public sector

2. provide **remedies for interferences** with the information privacy of an individual

3. establish a **protective data security regime** for the Victorian public sector

4. establish a **regime for monitoring and assuring** public sector data security

5. establish the **Commissioner for Privacy and Data Protection**

6. repeal the **Information Privacy Act 2000** and the **Commissioner for Law Enforcement Data Security Act 2005** and make consequential amendments
Part 2: Application

Part 2 ‘information’ means:

- personal information
- public sector data
- law enforcement data
- crime statistics data

General exemptions apply to:

- Courts & Tribunals (re judicial or quasi-judicial functions)
- Parliamentary Committees (re Parliamentary Committee functions)
- Publicly-available information
Part 3: Information Privacy

- **Same application** as in Section 9, *Information Privacy Act 2000*

- **Taken to be re-enacted:**
  - Information Privacy Principles (Schedule 1)
  - codes of practice provisions
  - information privacy complaints provisions

- **Three new mechanisms:**
  - public interest determinations
  - information usage arrangements
  - certificates
Information Privacy Mechanisms

Clause 20(3): compliance with Information Privacy Principles not required for act or practice permitted under:

**Mechanism 1**  public interest determination (PID)
  temporary public interest determination (TPID)

**Mechanism 2**  information usage arrangement (IUA)

These provide options for the Commissioner and relevant Ministers to:

- authorise practices that depart from IPPs for public purposes, where public interest test met; or
- permit handling of personal information as authorised or required by law (ie under an information handling provision); but
- cannot be made re Principle 4, Data Protection or Principle 6, Access and Correction.
Commissioner may certify act or practice is consistent with:

- Information Privacy Principle
- Approved code of practice
- Information handling provision

While certificate is current, an organisation acting in good faith in reliance on it does not breach the relevant IPP, code or Provision.
Part 4: Protective Data Security

Applies to

- public sector agencies
- special bodies (Section 6, Public Administration Act 2004)
- declared bodies (Governor in Council)

Does not apply to

- councils
- universities
- bodies/governing bodies where another jurisdiction can appoint member
- certain health service providers under
  - Health Services Act 1988
  - Ambulance Services Act 1986
Part 4 (cont.)

➢ Covers:
  ● public sector data
  ● public sector data systems

➢ Commissioner to:
  ● develop protective data security Framework
  ● issue protective data security Standards (general or customised)
  ● receive protective data security Plans from agencies & bodies
  ● perform related functions under Part 6, e.g. monitoring and assurance

➢ Public sector body Head to:
  ● ensure body/agency & Contracted Service Provider don’t contravene Standard
  ● undertake security risk profile assessment (within 2 years of Standard)
  ● prepare protective data security Plan (within 2 years of Standard)
  ● review Plan if significant change in operating environment OR every 2 years
Part 5: Law Enforcement Data Security

- Expands existing regime under *Commissioner for Law Enforcement Data Security Act 2005*

- Applies to:
  - Victoria Police
  - Chief Statistician
  - Employees or consultants engaged under section 6, Crime Statistics Bill 2014 (sent to Legislative Council)

- Existing 2007 Standards apply until new Standards issued

- For New Standards — Commissioner must consult:
  - Chief Commissioner of Police
  - Chief Statistician
Part 6: Commissioner

- Establishes Commissioner for Privacy and Data Protection
- Has separate specified functions re privacy and data protection (clause 103)
- Powers include:
  - general powers - all things necessary or convenient re functions
  - access to data, data systems and crime statistics (may copy and take extracts)
  - reports to the Minister, and publications
  - disclosures during audits to specified persons and bodies
  - disclosure to the IBAC
Privacy & Data Protection Bill – What it means for you

David Watts, Acting Privacy Commissioner
Tuesday, 22 July 2014
Privacy and Data Protection Bill 2014

- Key privacy changes are the inclusion of three flexibility mechanisms that permit departures from the IPPs where there is a substantial countervailing public interest:
  - Public Interest Determinations (permanent and temporary)
  - Information Usage Arrangements
  - Certification

- Key security changes:
  - PDPC to develop Victorian Protective Data Security Framework (VPDSF)
  - PDPC to issue Protective Data Security Standards
  - Statutory requirement to consult
Regulatory Model

5 standard criteria for ‘good’ regulation

– legal authority
– accountability
– due process
– expertise (expert judgement over competing values or options)
– efficient outcomes
Enforcement Approaches

• Options range from formal enforcement through to informal techniques, including education, advice, persuasion, negotiation.

• Persuasive compliance model probably best adapted to achieve PDPB objectives.
Public Interest Determinations

- Based on Commonwealth model
- Commissioner may permit departures from IPPs (except IPP 4 – security and IPP 6 – access) where the departure substantially outweighs the public interest in complying with IPPs
- Can be amended, revoked or time-limited
- PID exceeding 1 year must report
Temporary PID

- Commissioner can make a temporary PID for no more than 12 months in urgent circumstances
- Same test
- Applicable, for example, in emergency circumstances where information needs to be shared as part of an emergency response
Substantiality test

• More than equal, less than overwhelming
• Guidance can be derived from existing exceptions to IPP2
• Preliminary – substantiality test a qualitative one
• Can the outcome be achieved in a less privacy invasive way?
• Can compensating measures be implemented? Eg, ratchet down and ratchet up?
Public interest

- A normative concept – how things *should be* based on assumptions about that which is socially valued
- Regard to other rights and interests a component of normative analysis
- Promotion of the objects of the PDPB
- Danger in defining public interest too broadly – this supported by substantiability test
- ‘Balancing’ discourse can be unhelpful – implies winners and losers
- What ‘ought’ to be changes over time
Information Usage Arrangements

- Based on NZ equivalent provisions
- An IUA is an arrangement for handling personal information for one or more public purposes
  AND
- Modifies application of an IPP (but not 4 or 6)
IUA #2

• Must specify parties to the IUA, the type of PI to be handled, describe how arrangement would facilitate one or more public purposes

• Two basic types:
  – modify/non compliance with an IPP; and
  – arrangement for purposes of information handling provision

• If modifies or provides for noncompliance with an IPP, must identify the IPP and how it would be modified or not complied with
IUA #3

- If arrangement for purpose of an information handling provision, must identify provision, describe its effect
- Describe personal information to be covered
- State manner in which PI could be used, including disclosure to another person or body and in what circumstances
IUA #4

- IUA must have a lead agency
- Commissioner to consider whether the public interest in an arrangement modifying or not complying with an IPP substantially outweighs interest in complying
- Similar test for information handling provision
IUA #5

• Commissioner must issue a report
• If public interest test satisfied, Commissioner must issue a certificate
• Both must be sent to relevant Ministers
• Ministers must approve
• IUA then published on Commissioner’s web site
Certification

- Designed to address risk appetite or differences in opinion about privacy acts or practices
- Comparable to an advisory opinion
- Commissioner may issue certificate
- Acting in good faith on the certificate means no contravention of IPP
- Can be reviewed by VCAT
Access to Flexibility mechanisms

• Remember existing provisions allow departures from IPP 2 (Use and Disclosure) in some circumstances
• Applications will need to be properly documented and explained
• Need for consultation
• Be prepared to be scrutinised and to be clear about public interest
• Guidance on process and procedure to be developed
Privacy by Design

– OVPC policy from 1 July 2014
– Internationally accepted benchmark
– A methodology to build privacy into the architecture of ICT and business process
– Addresses the myth that respect for privacy and the deployment of new ICT is mutually exclusive – a zero sum game
– Addresses myth that Privacy impedes innovation and consigns us to a technological ghetto
Privacy by Design #2

Seven Foundational Principles:
–Proactive, not reactive; Preventative not Remedial
–Privacy as the Default Setting
–Privacy Embedded into Design
–Full Functionality – Positive-sum, not Zero-sum
–End-to-end Security – Full Lifecycle Protection
–Visibility and Transparency – Keep it Open
–Respect for User Privacy – Keep it User-Centric
Privacy by Design #3 - So what is the link between PbD and the PDPB?

• Those who seek exemption from the law bear the onus of making their case
• Implicit in making a case for access to any of the flexibility mechanisms is that the questions posed by the seven foundational principles have been answered
• More generally, observing PbD will deliver better information outcomes and improved service delivery – not at the expense of privacy but because the right framework has been implemented from the outset
Key security functions of the new office include, but are not limited to…

- Develop the Victorian Protective Data Security Standards (VPDSS)

- Provide supporting assistance to public sector organisations to implement associated controls. This assistance will come in the form of -
  - supporting templates
  - Guidelines
  - tools, and
  - other material…

- Monitor and review the implementation of the VPDSS

- Continue to monitor and review the implementation of the existing CLEDS Standards for agencies handling and holding law enforcement data

- Analyse security incidents & threats trends across the Victorian Public sector
Aims & Objectives of VPDSS

- Ensure the VPDS Standards are:
  - Flexible
  - Robust
  - Durable
  - Adaptable
  - Widely accessible

- Reflect contemporary security standards both locally and Internationally – confidentiality, integrity, availability

- Support Victorian State government service delivery functions

- Facilitate appropriate information sharing – the right information to the right people, at the right time
- Promote the concept of Security by Design, and foster a culture where security is seen as a business enabler, rather than an impediment

- Underpin cultural change within Victorian public sector organisations

- Tailor the Standards to meet the needs of Victorian Government public sector organisations, whilst aligning with the Commonwealth PSPF policies

- Promote a risk based approach to support the practical implementation of protective security measures, in order to protect official information assets and services in a proportionate manner that supports (and does not inhibit) government business.
What has informed the development of these Standards?

VPDSS draws on principal elements from Australian and international security standards, policies, schemes, frameworks and benchmarks including, but not limited to:

- Whole of Victorian Government security Standards
- Commissioner for Law Enforcement Data Security (CLEDS) Standards
- Commonwealth Government PSPF
- OECD
- ISO 27000 family of Standards
- UK Security Policy
- Australian Standards
- NIST
Tiered Approach -

In order to support the aims and objectives of the VPDSF, the structure of the Standards and supporting material has been tiered into four main sections.

- **Tier 1 - Standards**
- **Tier 2 - Objectives**
- **Tier 3 - Controls**
  - Each control will be accompanied by an applicability statement which identifies which ‘Organisational Class’ is expected to comply with the particular control
- **Tier 4 - Tool Kit**
  - The Tool Kit will include templates, guides, proformas, working examples, etc.
Separate Information & ICT Standards

- Ensures that each element (i.e. confidentiality, integrity, availability) of information is given equal consideration, regardless of media or format.

- Provides a consistent valuation & classification criteria across all Vic Gov. official information & helps develop a level of maturity around their material without jumping into the other functional domains of ICT, Physical or Personnel Security.

- Provides a central focus on Information Lifecycle principles and the protective measures need to support the security of information at every stage.

- Provides a platform to support secure Information Sharing.

- Ensure all users (not just ICT SME’s) understand the important messages associated with Information Security aren’t lost and are accessible.

- Allow for focused ICT statements that purely concentrate on the technology and ICT systems, rather than the material / information that is being housed within it these tools.

- Ensure ICT Security controls are embedded in all stages of the system development (i.e. Security by Design), rather than a piecemeal approach to system security.
### Development of the VPDSS

#### Key Stages

<table>
<thead>
<tr>
<th>Year</th>
<th>Month</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>August</td>
<td>Commenced review of existing policies and frameworks</td>
</tr>
<tr>
<td></td>
<td>September</td>
<td>Developed draft Victorian Protective Data Security Standards &amp; Objectives</td>
</tr>
<tr>
<td></td>
<td>November</td>
<td>Conceptual introduction of VPDSS with Commonwealth Attorney Generals team</td>
</tr>
<tr>
<td>2014</td>
<td>January - February</td>
<td>Initial consultation with select stakeholders</td>
</tr>
<tr>
<td></td>
<td>March</td>
<td>Initial VPDSS presentation provided to Commonwealth Attorney General's</td>
</tr>
<tr>
<td></td>
<td>March - April</td>
<td>Consultations commence with key Victorian Government agencies</td>
</tr>
<tr>
<td></td>
<td>May - July</td>
<td>Awaiting passage of legislation</td>
</tr>
</tbody>
</table>

*We are here…*
Staged implementation approach preferred.

For example…

Legislation comes into effect

Grandfathering period commences - Aim to build resilience within Public Sector Organisations

Agencies will be expected to report against Governance Standards

Agencies will be expected to report against Information Security Standards

Agencies will be expected to report against Personnel Security Standards

Agencies will be expected to report against Physical Security Standards

Agencies will be expected to report against ICT Security Standards

The Grandfathering period will depend on what Standards have come into effect…
Organisational Classes – Levels of risk

## Organisational Class Criteria for VPDSF

<table>
<thead>
<tr>
<th>Class</th>
<th>Standards</th>
<th>Controls</th>
<th>Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Mandatory</td>
<td>Applicability statement Class A</td>
<td>Independent auditing</td>
</tr>
<tr>
<td>B</td>
<td>Mandatory</td>
<td>Applicability statement Class B</td>
<td>Public assurance/self-assessment OR Exception reporting &amp; change in circumstances of any of the following criteria</td>
</tr>
</tbody>
</table>

### Class A

- **Protective Marking**
  - PROTECTED
  - Sensitive: Cabinet

- Critical Assets (including critical and essential services, critical information, infrastructure and critical physical infrastructure)
  - **Critical High Impact** (Refer to Business Impact Levels)

- Foreign ownership (country)
  - **<50%**

- Size (in terms of turnover)
  - **>1001**

### Class B

- **Material breaking a DECM**
  - For Official Use Only (FOUO)
  - Sensitive
  - Sensitive: Personal
  - Sensitive: Legal

- **UNCLASSIFIED** - unaccompanied by a DECM

- **PUBLIC DOMAIN**

### Class C

- **Contracted Service Providers and External Bodies**

  - Standards: Mandatory
  - Controls: Applicability statement Class C
  - Reporting: yet to be determined

**For Official Use Only**
Organisational Classes – Levels of risk

Some questions

• What about portfolio agencies? Should they be permitted to adhere to Departmental security framework?
• There are around 2000 organisations to which the VPDSF will apply. The Commissioner has an obligation to consult about the VPDSS – how do you consult with this number of organisations?
Thank you
Need more information?

Deidre Missingham  
8684 0483  
deidre.missingham@vgso.vic.gov.au

VGSO blog  
‘Privacy Bill Goes Public’ (13 June 2014)  
vgso.vic.gov.au/vgso-blog

---

**Privacy & Data Protection workshops**

**Privacy Module**  
1.5 Substantive Law CPD points

This session runs for 1.5 hours and covers:
- Information Privacy – what’s different, what stays the same?  
- New options for sharing: public interest determinations (PID); temporary public interest determination (TPID); and approved information usage arrangements (IUA).  
- Understanding certification

Cost: $200 excluding GST

**Data Protection Module**  
1 Substantive Law CPD point

This session runs for 1 hour and covers:
- Context and background  
- Role of the PDP Commissioner  
- Responsibilities of public sector body Heads

Cost $150 excluding GST
# Privacy & Data Protection workshops

<table>
<thead>
<tr>
<th>SESSION DATES</th>
<th>MORNING SESSION</th>
<th>BREAK</th>
<th>AFTERNOON SESSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friday 8 August</td>
<td>Privacy module 10.30am – 12pm</td>
<td>Lunch 30 mins</td>
<td>Data Protection module 12.30pm—1.30pm</td>
</tr>
<tr>
<td>Monday 11 August</td>
<td>Data Protection module 11am—12pm</td>
<td>Lunch 30 mins</td>
<td>Privacy module 12.30pm—2pm</td>
</tr>
<tr>
<td>Friday 15 August</td>
<td>Privacy module 10.30am – 12pm</td>
<td>Lunch 30 mins</td>
<td>Data Protection module 12.30pm—1.30pm</td>
</tr>
<tr>
<td>Tuesday 19 August</td>
<td>Data Protection module 11am—12pm</td>
<td>Lunch 30 mins</td>
<td>Privacy module 12.30pm—2pm</td>
</tr>
</tbody>
</table>