Office of the Victorian Information Commissioner

Victorian Privacy Network meeting – 6 March 2025: Responses to questions from Q&A

OVIC's Outsourcing Guidance – Adriana Nugent, Office of the Victorian Information Commissioner

1. **Has the guidance followed the principles of statutory interpretation from cases like Project Blue Sky, and 2nd reading speeches that state the Information Privacy Act which is the predecessor to the PDP Act is intended to be "much stronger than the commonwealth act"? I believe that this was in the Hon Jenny Mikakos' 2nd reading speech in late 2000. Also related acts, like the Electronic Transactions Act (also mentioned in J. Mikakos 2nd reading speech).**

   The *Outsourcing in the Victorian public sector guidance* (**Outsourcing guidance**) is an updated version of a resource published by the former Commissioner for Privacy and Data Protection. The content in the outsourcing guidance is informed by privacy and information security obligations in the *Privacy and Data Protection Act 2014* (**PDP Act**), relevant case law and OVIC's view on outsourcing best practice.

2. **Does OVIC offer 'model contract terms' to section 17 and can you elaborate on what happens if such terms are not included? Also, does OVIC offer additional guidance on expectations? There is some detailed guidance in the PSPF, or does OVIC work with VGPB to promote good practices in WoVG contract templates? With Government panels - the due diligence should take into account whether the panel includes any due diligence, or it is simply a panel of organisations that have registered their interest in providing services, with no due diligence.**

   Section 17

   OVIC has not developed model contract terms that organisations can include in their outsourcing contracts. OVIC suggests that each agency should consult with their own internal legal team on the most appropriate terms for their engagement.

   OVIC recommends a clause like section 17(2) in the outsourcing contract which would enable an organisation to bind the third party to the Information Privacy Principles (**IPPs**). This ensures the third party is required to comply with the IPPs when handling personal information involved in the outsourcing arrangement. In addition, it ensures the third party is liable for any acts or practices it engages in that breach the IPPs.

   If a third party intends to engage a subcontractor to undertake any of the functions or activities in the outsourcing contract, OVIC recommends the organisation also requires the third party to bind the sub-contractors to the IPPs.

Additional guidance on expectations

If a third party intends to engage a subcontractor to undertake any of the functions or activities in the outsourcing contract, OVIC recommends the organisation also require the third party to bind any sub-contractors to the IPPs.

In addition to the guidance on outsourcing, OVIC has a range of privacy and information security resources that provide further guidance on matters that may be relevant to outsourcing arrangements. Many of these resources have been referenced in the outsourcing guidance such as the Guidelines to the Information Privacy Principles and the Victorian Protective Data Security Standards Implementation Guidance Version 2.3. There are also Australian/New Zealand Standards on information security in supplier relationships that provide helpful information. For example, the *AS/NZS ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls*. This resource is referenced in the outsourcing guidance and is accessible through the Victorian Government Library Service.

OVIC is not currently working with the Victorian Government Purchasing Board (**VGPB**) to promote good practice in whole of Victorian Government contract templates. However, OVIC has informed VGPB of the updated outsourcing guidance.

Government panels and due diligence

As mentioned in the outsourcing resource, organisations should not assume due diligence has been conducted on a third party that has been selected from a government supplier panel or from a register of pre-qualified suppliers. If an organisation intends to choose a third party from a government supplier panel, then as part of its due diligence activities the organisation should take into account whether the panel has conducted due diligence on the third party.

Organisations should satisfy themselves that a third party from a government supplier panel can comply with the relevant privacy and information security requirements that will be included in the outsourcing contract.

3. **Would OVIC consider another Vic Gov agency as a third party?**

This depends on the circumstances and whether the government agencies involved are separate legal entities. OVIC suggests that an agency seeks legal advice on this issue before entering into an engagement.

4. **Should planning the outsourcing arrangement also include ongoing reporting - this would be consistent with higher levels of maturity (e.g. Core) of VPDSS.**

The resource provides an overview of privacy and information security matters organisations should consider at each stage of the outsourcing process (noting the resource does not cover the entire outsourcing and procurement process organisations are required to follow). While the resource covers reporting when discussing the terms of the contract (page 18) and the life of the outsourcing arrangement (page 20), it is open to organisations to also consider reporting when planning the arrangement.

5. What if the third party and/or subcontractor already abides to the *Privacy Act 1988 (*Cth), would you still have to bind the third party to IPPs even though IPPs are less stringent and only applicable to government bodies?

   In some circumstances, as set out in section 7B(5) of the *Privacy Act 1988* (Cth) (**Privacy Act**), a third party bound by the Australian Privacy Principles (**APPs**) may be exempt from complying with the APPs where it is involved in an outsourcing arrangement with a State government organisation.

   As the third party will not be required to comply with the APPs, it will not be obligated to handle personal information in a way that protects privacy. Specific measures must be taken to ensure the third party handles information appropriately.

   This is why it is important for Victorian public sector organisations to adequately bind a third party to the IPPs. Binding a third party to the IPPs ensures the third party is held accountable for any acts or practices it engages in that breach the IPPs.

6. Is there a recommended course of action if an organisation discovers after engaging a third party that the third part isn't complying with privacy obligations? Especially when it may be the organisation's responsibility because the contract may not have been rigorous enough.

   It is open to an organisation to determine what steps it will take to deal with a third party that is not complying with privacy obligations. In determining the appropriate course of action, OVIC suggests that an agency seeks legal advice on the particular contract issues before taking any action concerning privacy compliance.

7. What is the best way to get executive buy-in to get better contract management support?

   Organisations subject to the PDP Act are required to collect, use, disclose and protect personal information and public sector information they hold. Crucially, under Part 4 of the PDP Act, a public sector body head is obligated to ensure a contracted service provider does not do an act or engage in a practice that is contrary to a Victorian Protective Data Security Standard. Highlighting that this is a legislated requirement that is the responsibility of the head of a public sector body can ensure outsourcing arrangements and contract management are done well.

   In addition to ensuring compliance with legislative obligations, managing outsourcing contracts appropriately offers other benefits. These include:

   - minimises any privacy and information security risks to the information involved in the outsourcing arrangement
   - can help avoid future contractual issues that may have adverse financial, legal and/or reputational impacts on the organisation
   - demonstrates to stakeholders and the public that the organisation values privacy and information security

- helps build public trust in an organisation's information handling practices and enhances the organisation's social licence to use personal information and public sector information in other projects and initiatives.

Executives that understand the value of robust contract management are likely to provide the necessary resources and support to ensure outsourcing contracts are managed properly.

Executives can be engaged on outsourcing matters in a number of ways, such as:

- having standing items on meeting agendas relating to contract management
- providing regular presentations or briefings to executives on managing current outsourcing arrangements
- including information management in outsourcing arrangements in risk registers.

Promoting transparency of AI usage within the public sector– Emma Stephens, Office of the Victorian Information Commissioner

1. **Is Notice sufficient? Notice is from the Commonwealth Act - while it may be sufficient for the PDP Act, it is not consistent with the text of the PDP Act.**

Providing 'notice of collection' is a shorthand way to refer to an organisation's obligation under IPP 1.3 in Schedule 1 of the *Privacy and Data Protection Act 2014* (Vic). The obligation under IPP 1.3 reads:

"At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of –

(a) the identity of the organisation and how to contact it; and
(b) the fact that the individual is able to gain access to the information; and
(c) the purposes for which the information is collected; and
(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and
(e) any law that requires the particular information to be collected; and
(f) the main consequences (if any) for the individual if all or part of the information is not provided."

2. **Could the guidance on AI risk assessments that are available on PROV website be used as a starting point for the transparency assessment? Is this in line with OVIC transparency standards?**

OVIC recognises that proper recordkeeping under the *Public Records Act 1973* (Vic) is essential to fulfilling an organisation's transparency obligations under the *Freedom of Information Act 1982* (Vic) and *Privacy and Data Protection Act 2014* (Vic). OVIC will consider resources produced by the Public Record Office Victoria (PROV) in developing OVIC's transparency guidance, including PROV's new Create, Capture & Control Standard, AI Technologies and Recordkeeping Policy and other AI resources.

The Department of Government Services is also piloting an AI Assurance Framework for the Victorian Public Sector that includes consideration of transparency. The Pilot Framework is available on the Victorian Public Sector Commission's Innovation Network. OVIC will consider this framework in developing OVIC's transparency guidance.