Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES

Outsourcing in the Victorian public sector – Short guide

This resource is intended to provide a simplified overview of the matters Victorian public sector organisations (**organisations**) subject to the *Privacy and Data Protection Act 2014* (**PDP Act**) should take into account when entering into outsourcing arrangements. Detailed guidance on these considerations is available in the Outsourcing in the Victorian public sector resource.

Obligations in the PDP Act

Information privacy obligations

Organisations subject to Part 3 of the PDP Act should ensure any personal information involved in an outsourcing arrangement is handled in accordance with the 10 Information Privacy Principles (**IPPs**) in Schedule 1 of the Act.[1]

Organisations *can* pass on the obligation for complying with the IPPs to the third party – by ensuring the third party is bound to the IPPs under a State contract. The IPPs can then be enforced against the third party.[2] Where this occurs, the third party will likely be responsible for any breach of the IPPs.

Information security obligations

The head of an organisation subject to Part 4 of the PDP Act must ensure public sector information involved in an outsourcing arrangement is handled in accordance with the Victorian Protective Data Security Standards (**VPDSS**).[3]

Organisations *cannot* pass on the obligation to comply with information security requirements to a third party. Organisations remain liable for any incidents caused by the third party's failure to handle

[1] Section 13 of the PDP Act lists organisations that are subject to Part 3.

[2] Section 17(4), PDP Act.

[3] Section 88(2), PDP Act. See also section 84 of the PDP Act, which sets out the organisations that are subject to Part 4.

information in line with the VPDSS. This means organisations need to be satisfied about the security practices of the third party.

Planning the outsourcing arrangement

The key steps involved in planning the outsourcing arrangement include:

1. Identifying information that will be involved in the arrangement and determining its value.
2. Determining whether any secrecy, confidentiality or other information handling provisions restrict or prohibit information from being used and disclosed in an outsourcing arrangement.
3. Conducting due diligence on the third party and identify risks involved in the arrangement.
4. Determining the information privacy and information security measures required to mitigate the risks identified from the due diligence activities.

Key terms of the outsourcing contract

The contract should include the following elements:

1. A clause that sufficiently binds the third party to the IPPs in the same way, and to the same extent, as the organisation.[4] Organisations should require third parties to bind any subcontractors to the IPPs.
2. Clearly defined roles and responsibilities of each party to the contract.
3. Information privacy and information security obligations, set out in clear and unambiguous terms.
4. Detailed process for handling information privacy and information security incidents, and information privacy complaints.
5. A clause stipulating that the organisation has a right to access information held by the third party for purposes of the contract, to ensure the organisation can fulfil its obligations under the *Freedom of Information Act 1982* (Vic).
6. Compliance and oversight mechanisms to ensure the organisation actively monitors the third party's compliance with information privacy and information security obligations.
7. Details on how information should be handled once the contract comes to an end.

[4] See section 17 of the PDP Act.

During the outsourcing arrangement

Privacy policies and notices of collection

The organisation's privacy policies and notices of collection should accurately reflect how information will be handled under the outsourcing arrangement. In addition, organisations should ensure the third party has a privacy policy that explains how information will be handled under the arrangement, and, where applicable, has appropriate notices of collection.

Training and awareness

Organisations should ensure the third party has a comprehensive information privacy and information security training program for its employees that is delivered regularly.

Ongoing monitoring and assurance

Organisations should have processes in place to monitor the third party's compliance with information privacy and information security obligations throughout the life of the arrangement. The terms of the contract are not self-enforcing and require assurance that they are being adhered to.

Ending the outsourcing arrangement

Recordkeeping obligations

Organisations should ensure information involved in the outsourcing arrangement is handled in line with obligations under the *Public Records Act 1973* (Vic).

Destruction or transfer of information held by the third party

Organisations should have policies and procedures in place to ensure information is handled appropriately once the outsourcing arrangement ends. Organisations should not solely rely on the third party handling information as required by contractual obligations.

Final audit or report from the third party

Organisations should conduct a final audit of the third party to ensure all information involved in the outsourcing arrangement is accounted for and has been handled in line with the required obligations.