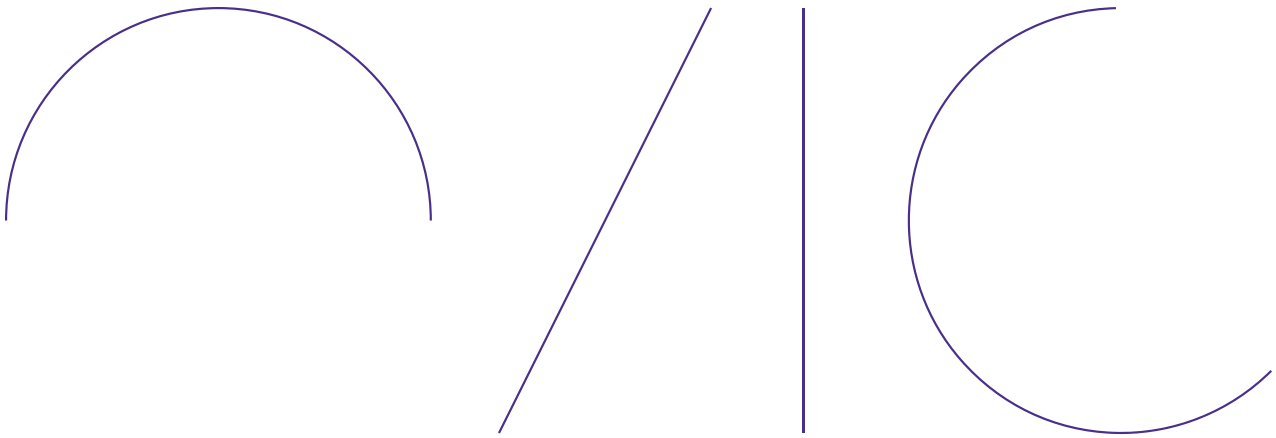
Office of the Victorian Information Commissioner

Outsourcing in the Victorian public sector

A guide to outsourcing arrangements



Document details

Document details	Outsourcing in the Victorian public sector
Publication date	2025/03/04
Review date	2026/03/04
Security classification	OFFICIAL
Document status	Published
Authority	Office of the Victorian Information Commissioner
Author	Policy team

Version	Author	Date	Additions/changes
1.0	Policy team	2025/03/04	N/A

Disclaimer

The information in this document is general in nature and does not constitute legal advice.

Copyright

Table of Contents

Introduction

This resource discusses the information privacy and information security considerations 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.

The resource provides a starting point for organisations to consider information privacy and information security when outsourcing a program or a service. It is not exhaustive. Organisations should seek their own legal and policy advice to ensure an outsourcing arrangement complies with the PDP Act and any other legislation by which they are bound, such as the *Freedom of Information Act 1982* (Vic) (**FOI Act**) and the *Public Records Act 1973* (Vic) (**Public Records Act**).

This resource is limited to an overview of the steps that organisations should take to ensure their outsourcing arrangements contain strong information privacy and information security protections. It is not a complete guide on the entire outsourcing and procurement process organisations are required to follow. For guidance on the other elements of the procurement process, organisations should visit the Buying for Victoria website, or speak to their organisation's procurement officer.[1]

Scope of resource

The guidance in this resource applies to outsourcing arrangements that involve the collection, use, disclosure or management of personal information[2] and public sector information (referred to as public sector data[3] in the PDP Act).

An outsourcing arrangement refers to a contractual agreement, in which an organisation engages a third party to deliver a program or service on its behalf, or procures technology from a third party to deliver a program or service.

Examples of outsourcing arrangements include engaging a third party to:

- provide communication and customer service functions, such as call centres or emergency hotlines
- conduct community consultation and other stakeholder engagement activities
- recruitment services

[1] See https://www.buyingfor.vic.gov.au/.

[2] Personal information is defined in section 3 of the PDP Act. It means information or an opinion that is recorded in any form and whether true or not, about an individual whose identity is apparent or can reasonably be ascertained, from the information or opinion. Further guidance on personal information is available in the Key Concepts chapter of OVIC's Guidelines to the Information Privacy Principles: https://ovic.vic.gov.au/book/key-concepts/.

[3] Public sector data is defined in section 3 of the PDP Act. It means any information (including personal information) obtained, received or held by an agency or body to which Part 4 of the PDP Act applies, whether or not the agency or body obtained, received, or holds that information in connection with the functions of that agency or body.

- provide Information Technology services, such as developing and maintaining websites, portals, platforms and webforms
- migrate the organisation's data
- provide Software-as-a-Service (SaaS) services
- deliver a program or service that involves the use of artificial intelligence
- perform administrative work, such as providing transcription services
- print and distribute physical correspondence
- provide security and surveillance services
- provide asset maintenance services, such as utilities maintenance or establishment of new utility services.

The word 'information' is used throughout this resource to refer to both personal information and public sector information, except where it is necessary to distinguish between the two.

This resource considers health information only in the context of information security obligations in Part 4 of the PDP Act. This resource does not consider information privacy obligations in relation to health information. Organisations should refer to the *Health Records Act 2001* (Vic) or consult the Health Complaints Commissioner if the outsourcing arrangement involves health information.

Obligations in the PDP Act

This section sets out the information privacy and information security obligations organisations must consider when outsourcing.

Information privacy obligations

> Personal information involved in an outsourcing arrangement must be handled by an organisation in accordance with the Information Privacy Principles.

Organisations subject to Part 3 of the PDP Act must comply with the 10 Information Privacy Principles (**IPPs**) set out in Schedule 1 of the Act.[4] The IPPs set the minimum standard for handling personal

[4] Section 13 of the PDP Act lists organisations that are subject to Part 3. See also section 20, which establishes the obligation for organisations to comply with the IPPs.

information throughout the information lifecycle, from when it is collected to when it is no longer needed.[5]

When an organisation enters into a contract with a third party, it is the organisation's responsibility to ensure any personal information involved in the arrangement is handled in accordance with the IPPs. The default position under the PDP Act is that the organisation is liable for any breach of the IPPs that occurs under the arrangement, even if the breach is caused by the third party.[6]

Varying liability for privacy obligations

The default position can be varied where section 17 of the PDP Act applies. The contract or agreement can require the third party to be bound by the IPPs in the same way, and to the same extent, as the outsourcing organisation for the purposes of the contract.

Both the organisation and the third party will be responsible for any acts done or practices engaged in by the third party that contravene the IPPs, unless the organisation can show that:

- the contract had a provision in force, at the relevant time, that bound the third party to the IPPs in the same way and to the same extent as the organisation,[7] and
- the relevant IPP is capable of being enforced against the third party in accordance with the procedures in the PDP Act.[8]

If the organisation can demonstrate this, it will not be responsible for the acts or practices of the third party. The third party will be solely responsible for its acts or practices, for the purposes of the IPPs.

Organisations should satisfy themselves that their particular outsourcing arrangement will operate under a 'State contract' as defined in the PDP Act,[9] and therefore meet the requirements for the third party to be liable for its acts or practices. Organisations may wish to seek legal advice on this matter.

If a third party, bound by the IPPs, chooses to subcontract some of its functions under the contract, it would be prudent for the third party to pass on privacy obligations to the subcontractor, to ensure the subcontractor is also required to comply with the IPPs.[10] Outsourcing organisations should include a provision in the State contract requiring the third party to bind any subcontractors to the IPPs.

The third party and any subcontractors they use may be subject to the Australian Privacy Principles in the *Privacy Act 1988* (Cth) (**Privacy Act**) as part of their normal commercial operations. However, when

[5] Detailed guidance on each of the IPPs is available in the Guidelines to the IPPs: https://ovic.vic.gov.au/privacy/resources-for-organisations/guidelines-to-the-information-privacy-principles/.

[6] Section 17, PDP Act.

[7] Even though a third party states it complies with equivalent privacy law, the third party will not be bound by the IPPs unless the contract specifies it.

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

[9] Section 3, PDP Act.

[10] Sections 4(3) and 13(1)(j), PDP Act.

handling personal information for the purposes of a State contract with a Victorian public sector organisation, the third party may be exempt from complying with the APPs,[11] and therefore not bound by any overarching privacy framework. Therefore, organisations should ensure third parties are bound to the IPPs, and require third parties to bind any subcontractor to the IPPs.

Remember that even where a third party assumes liability for privacy obligations, an organisation remains liable for its own actions in relation to the contract, such as its decision to engage the third party in the first place. Organisations must therefore take an active role in managing and monitoring their arrangements with third parties.

Information security obligations

> Public sector information involved in an outsourcing arrangement must be handled in accordance with the Victorian Protective Data Security Standards.

The Victorian Protective Data Security Framework (**VPDSF**), established under Part 4 of the PDP Act, monitors and assures the security of public sector information and information systems, across the Victorian public sector.[12] It provides a risk-based model to track and measure the extent to which organisations implement the Victorian Protective Data Security Standards (**VPDSS**) and comply with requirements under Part 4 of the PDP Act. [13]

The head of an organisation subject to Part 4 of the PDP Act[14] must ensure that a contracted third party does not do an act, or engage in a practice, that contravenes a protective data security standard.[15]

The VPDSS set out the mandatory requirements to protect public sector information across all security domains including governance, information, personnel, information communications technology (**ICT**) and physical security.

Standard 8 requires organisations to ensure any third party they engage collects, uses, discloses, holds, manages or transfers public sector information securely.[16]

---

[11] Section 7B(5), Privacy Act.

[12] Detailed information on the VPDSF is available on OVIC's website: https://ovic.vic.gov.au/information-security/framework-vpdsf/.

[13] Detailed information on the VPDSS is available on OVIC's website: https://ovic.vic.gov.au/information-security/standards/.

[14] Section 84 of the PDP Act sets out the organisations that are subject to Part 4.

[15] Section 88(2), PDP Act.

[16] In 2022, OVIC conducted an audit to assess four organisations' adherence to Standard 8 of the VPDSS and to identify areas of potential improvement. OVIC examined whether the four organisations had appropriate practices and procedures in place to ensure that third parties they shared public sector information with were protecting it appropriately, including when they collected, held, used, disclosed or transferred information. The audit report is available on the OVIC website: https://ovic.vic.gov.au/regulatory-action/audit-report-standard-8-of-the-victorian-protective-data-security-standards/.

Varying liability for information security obligations

Unlike information privacy obligations in Part 3 of the PDP Act, an organisation cannot pass on liability for its information security obligations to a third party by contract. An organisation remains liable for any incidents caused by the third party's failure to comply with information security obligations.[17] This means organisations need to be satisfied about the security practices of the third party, and to check that they do in fact have the required security through the lifespan of the contract (and potentially beyond, in the case of retention and disposal policies).

Planning the outsourcing arrangement

This section looks at the steps organisations should take when planning their outsourcing arrangement, prior to engaging a third party.

Key steps in planning an outsourcing arrangement:

1. Identify information that will be involved in the arrangement and determine its value.
2. Determine whether information involved in the arrangement is subject to secrecy or confidentiality provisions, or other information handling provisions.
3. Conduct due diligence on the third party and identify risks involved in the arrangement.
4. Determine the information privacy and information security measures required to mitigate the risks identified.

Identify information involved in the arrangement and determine its value

Organisations should first identify all the information that will be involved in the outsourcing arrangement. Organisations should ensure the amount of information involved is reasonable and proportionate to the function or service being outsourced, so that only the minimum amount of information necessary is involved in the arrangement.

Where a significant amount of public sector information (including personal information) will be handled, there may be a higher risk of harm that could be caused by mishandling of the information. Organisations should consider whether it is appropriate to outsource a function or service that will

[17] Section 88(2), PDP Act.

involve handling significant amounts of personal information. If an organisation chooses to do so, appropriate measures will need to be in place to protect the information, in line with its value.

Determining the value of the information will enable organisations to implement appropriate measures to protect the information throughout the life of the arrangement.

For organisations subject to Part 4 of the PDP Act, the measures adopted to protect information should be consistent with the security value of the information. Organisations can follow the three-step process below to identify the security value of information:

- Identify all public sector information that may be affected by the arrangement. This includes information to which the third party will have direct and indirect access, and may generate on behalf of the organisation.

- Assess the potential impact to government operations, organisations or individuals, if the public sector information is compromised using the VPDSF Business Impact Level table.[18]

- Determine the overall security value of the information based on the assessment of the impact of a compromise to the information. Establishing the overall security value of the information will also enable organisations to determine:

    - which protective marking(s), if any, should be applied to the information

    - whether additional security measures are required, beyond those established by the protective marking(s), to further protect the information.

Irrespective of the financial value of the outsourcing arrangement, or the length of time for which the arrangement will be in place, the value of the information should determine the information privacy and information security measures that are put in place to protect the information.

Detailed guidance on assessing the security value of public sector information is available on OVIC's website.[19]

Confidentiality, secrecy provisions and additional information handling obligations

An organisation's enabling legislation may contain confidentiality or secrecy provisions that restrict the ways in which information can be used or disclosed, or prohibit the organisation from using specific information. Similarly, information handling provisions contained in the enabling legislation may limit the

[18] The Business Impact Level table is available on OVIC's website: https://ovic.vic.gov.au/information-security/victorian-protective-data-security-framework-business-impact-level-table-v2-1/.

[19] Guidance on assessing the security value of public sector information is available at: https://ovic.vic.gov.au/information-security/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/.

ways in which an organisation can collect, use or disclose information under an outsourcing arrangement.

Organisations should determine whether the information that will be involved in the outsourcing arrangement is subject to any confidentiality, secrecy or information handling provisions, and structure the arrangement accordingly.

Conduct due diligence and identify information privacy and information security risks

Organisations should conduct robust due diligence on a third party *before* entering into an outsourcing arrangement, to determine whether it will be capable of complying with information privacy and information security obligations and handling information appropriately.

Due diligence involves taking steps before entering into an outsourcing arrangement to identify, assess and mitigate the information privacy and information security risks associated with engaging third parties.

It is not enough for organisations to impose contractual obligations on a third party or assume that due diligence has been conducted where the third party is from a government supplier panel or register of pre-qualified suppliers. Organisations need to assure themselves that the third party can comply with the organisation's relevant requirements.

At a minimum, when conducting due diligence organisations should:

1. **Identify any information privacy and information security risks associated with the outsourcing arrangement.** Before engaging a third party, organisations should undertake a Privacy Impact Assessment (**PIA**)[20] and a Security Risk Assessment (**SRA**).[21]

   Among other things, a PIA and SRA will help organisations to:

   - assess the outsourcing arrangement against the IPPs and information security obligations
   - identify any information privacy and information security risks associated with the outsourcing arrangement
   - implement measures to mitigate the impact of identified risks
   - establish the third party's capacity to handle information consistently with information privacy and information security obligations
   - decide whether to proceed with engaging the third party in question, dependent on the residual risks.

[20] Detailed guidance on conducting a PIA is available on OVIC's website: https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-impact-assessment/.

[21] Note that organisations subject to Part 4 of the PDP Act are required to ensure a third party securely collects, uses, discloses, holds, manages or transfers public sector information in line with Standard 8 of the VPDSS.

The PIA and SRA should be reviewed regularly throughout the duration of the arrangement to ensure the risks are re-assessed and managed appropriately, or any new risks are identified and managed.

Organisations should be mindful of the Victorian Government Risk Management Framework, which requires certain organisations to identify, assess and manage all risks to which they are exposed, including risks associated with handling public sector information.[22]

2. **Ensure the third party has a clear understanding of the information privacy and information security requirements it must comply with when handling information under the arrangement**. Consider whether the third party already has an understanding of the PDP Act, or is already subject to another privacy law. Not all third parties will be familiar with the requirements of the PDP Act. For example, a third party that does not ordinarily provide services to government may not have had to comply with any State or Commonwealth privacy laws. Additionally, a third party subject to the Commonwealth Privacy Act may be exempt from complying with obligations under that Act when handling personal information for purposes of an outsourcing arrangement with a state government organisation, in line with section 7B(5) of the Commonwealth Privacy Act.[23] Therefore, it is crucial for organisations to make sure the third party has a comprehensive understanding of its information handling obligations.

3. **Ensure the third party has the resources to comply with the information privacy and information security requirements in the arrangement**. For example, a third party may need to improve its security governance practices, upgrade its ICT security or install a new records management system to capture, share or store information securely before the arrangement begins, which is likely to incur costs. There may also be ongoing financial costs for the third party for the duration of the arrangement.

   Depending on the nature of the information that will be involved in the outsourcing arrangement, organisations may seek specific advice from the third party on the measures it has in place to handle information appropriately. For example, organisations may ask the third party to complete a self-assessment against the Australian Signals Directorate *Essential Eight*.[24]

4. **Review the third party's information privacy and information security history and its privacy and security culture**. A third party should have a clear track record of good information privacy and information security practices and be able to articulate the steps they take to ensure information privacy and information security. It should also be able to demonstrate its commitment and willingness to comply with information privacy and information security obligations relevant to the outsourcing arrangement.

---

[22] The Victorian Government Risk Management Framework is available at: https://www.vmia.vic.gov.au/tools-and-insights/victorian-government-risk-management-framework.

[23] Section 7B(5), Privacy Act.

[24] The Essential Eight are strategies developed by the Australia Signals Directorate to help organisations protect themselves against cyber threats. Detailed information on the Essential Eight is available at: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight.

If a third party has previously experienced an information privacy or information security incident, organisations should assess how it handled the incident, what measures it implemented to minimise the risk of the incident reoccurring, and ensure it has a robust incident response plan in place. Before engaging a third party, organisations should take its response to prior incidents into account.

5. **Confirm whether the third party will engage one or more subcontractors to perform any of the functions or activities under the arrangement.** If a third party intends to engage a subcontractor, the relationship between the subcontractor and the third party should be subject to the same information privacy and information security requirements as the relationship between the organisation and the third party. Outsourcing organisations should include a term in their contract with the third party that requires the third party to bind the subcontractor to the IPPs in the same way and to the same extent as the organisation. In addition, organisations should ensure subcontractors understand and are required to comply with the IPPs and information security obligations in the PDP Act.

   Organisations should know what work the subcontractor will undertake, what information the subcontractor will handle, and the potential information privacy and information security risks associated with the arrangement. Organisations should ensure appropriate measures are implemented to manage any information privacy and information security risks that may arise in the arrangement between the third party and the subcontractor.

6. **Confirm whether any information involved in the arrangement will be held, stored or transferred outside Victoria**. Holding, storing or transferring information outside Victoria increases information privacy and information security risks. For example, there may be an increased risk of the information being used for purposes other than originally intended, or an increased risk in the information being held for longer than necessary, which may result in an information privacy or information security incident.

   If organisations choose to engage a third party based outside Victoria, or if information involved in the outsourcing arrangement will be held, stored or transferred outside Victoria, organisations must ensure the information remains subject to adequate information privacy protections as required by IPP 9.[25]

   Additionally, like Australia, many foreign jurisdictions have legislative powers that allow access to information for purposes of law enforcement or national interest. Therefore, even where information is held locally, foreign-owned companies doing business in Victoria may be subject to foreign legislative requirements that may compromise the privacy or security of the information.

[25] Detailed guidance on IPP 9 is available in the Guidelines to the IPPs: https://ovic.vic.gov.au/book/ipp-9-transborder-data-flows/.

Determine required information privacy and information security measures

Organisations must ensure any information that may be involved in or affected by an outsourcing arrangement is handled consistently with information privacy and information security obligations. Organisations should take a risk-based approach to protecting information. This means, the measures implemented to protect information should be proportionate to any risks to the privacy and security of the information identified during a risk assessment.

Information privacy measures

The PIA conducted while undertaking due diligence on a third party will help organisations determine the measures that should be implemented to minimise any identified information privacy risks. For instance, if the PIA reveals that the third party may collect more personal information than is needed for the outsourcing arrangement, organisations can take steps to minimise the amount of personal information that will be involved in the arrangement.

Information security measures

Similarly, the SRA will help identify the measures that should be implemented to minimise any identified information security risks. The measures an organisation implements will be informed by its information security obligations in the PDP Act.

IPP 4.1 requires organisations to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure. IPP 4.1 is focused on the risk of harm to an individual if the security of their personal information is compromised. Therefore, organisations should implement measures that are proportionate to the potential information privacy risks to individuals and the potential harm they may experience.[26]

Organisations subject to Part 4 of the PDP Act are required to implement measures to protect the confidentiality, integrity and availability of all public sector information (including personal information) across five security domains: governance, information, personnel, ICT and physical security. Complying with the VPDSS enables an organisation to implement appropriate measures.[27]

While Part 4 of the PDP Act is focused on the risk to information security broadly, some of the measures organisations may implement to manage information security risks may be relevant to helping organisations protect the personal information they hold. Organisations that are not subject to Part 4 of the PDP Act are still encouraged to consider the VPDSS in meeting their obligations under IPP 4.1.

[26] Detailed guidance on complying with IPP 4 is available in the data security chapter of the Guidelines to the IPPs: https://ovic.vic.gov.au/book/ipp-4-data-security/.

[27] For detailed guidance on measures an organisation can take to ensure a third party handles public sector information in line with information security obligations, see the Standard 8 – Third Party Arrangements chapter of OVIC's VPDSS Implementation Guidance V2.3: https://ovic.vic.gov.au/wp-content/uploads/2024/02/VPDSS-V2.0-Implementation-Guidance-V2.3-web-version.pdf.

For example, protective markings are security labels assigned to public sector information (which includes personal information). Applying protective markings to information signifies the minimum security obligations that apply to the information and indicates how the information should be handled throughout the information lifecycle.[28]

Organisations should require third parties to respect protective markings that have been applied to information that will be involved in the outsourcing arrangement, and to apply protective markings to any new information that may be created by the third party under the arrangement where appropriate.

Example

Staff at an organisation consider that the information management system presently in use is not fit for purpose. The executive officers are aware that other organisations use SharePoint.

The organisation wants to engage a supplier of information management services to:

- build a customised SharePoint system
- migrate all of the data from the present system to SharePoint
- decommission the present system.

The supplier will outsource all of the content migration tasks to its own contractor, based in Alaska. The supplier's standard contract terms state that 'both parties must comply with the *Privacy Act 1988* and the Australian Privacy Principles' (**APPs**).

Before engaging the supplier, the organisation should consider the following:

- The type and volume of information that will be involved in the data migration, and its security value. Is it limited to a particular type of information or function of the organisation, or is it all the organisation's information?
- The systems that will be involved in the project, including its security value, the roles and responsibilities relating to the system and where it's located. For example, what are the implications of the subcontractor storing the organisation's data in Alaska?
- Undertaking a PIA and SRA for the data migration project. A PIA and SRA should also be completed for the new SharePoint system, ensuring that it is customised in a way that will meet the organisation's information privacy and information security requirements.
- Ensuring the controls and mitigation strategies identified in the PIA and SRA are reflected in the contract with the supplier, along with other expectations the organisation has for specific information privacy controls and information security controls under the five security domains. Examples include:

[28] Detailed guidance on protective markings is available in OVIC's Practitioner Guide: Protective Markings resource: https://ovic.vic.gov.au/information-security/practitioner-guide-protective-markings/.

- Governance: clearly defined roles and responsibilities, right to audit, change management processes, dispute resolution, incident management and legislative requirements
- Information: anyone with access to the information and systems honour the controls that accompany the protective marking, and any new material generated by the supplier is assessed and managed in accordance with the organisation's instructions
- Personnel: minimum eligibility and suitability screening checks of the supplier's personnel and subcontractors, and security considerations embedded into personnel onboarding and offboarding processes
- ICT: appropriate access controls are in place, patches are applied regularly, firewalls are monitored and anti-malware software is installed and monitored
- Physical: facilities, equipment and services are appropriately secured.

The initial risks associated with the project, and subsequent controls, should be monitored throughout the organisation's engagement with the supplier. This will provide a form of ongoing assurance regarding the protection of the information and systems.

The organisation should request the supplier amend its standard contract to bind the supplier to the PDP Act and the IPPs, not the Privacy Act and the APPs. The organisation should also require the supplier to bind the subcontractor to the PDP Act and the IPPs in their agreement.

Example

Tim is a privacy officer at an organisation. One of the organisation's functions is to investigate noise complaints, such as noise from loud machinery, industrial noise and loud music. Tim recently became aware of a private company that provides surveillance technologies specifically for noise surveillance. The company can install a recording device at any location and provide an analytical report from its Audio Surveillance specialists.

Tim thinks that the company's technology could be useful for his organisation's functions. Tim and the executive officers of the organisation meet with the company's sales representatives, who provide the organisation with its standard contract. The contract requires that both parties 'comply with applicable privacy laws' but does not mention the PDP Act or the IPPs.

Before engaging the company, Tim should consider the following:

- what personal information the organisation will disclose to the compnay to carry out its work, and how that information will be handled (IPP 2)
- what personal information will be collected by the surveillance technology, including any personal information that may be inadvertently collected, ensuring the collection is fair and not unreasonably intrusive on individuals (IPP 1)
- whether personal information will be shared for secondary purposes by the company (IPP 2)
- how an individual can request access to that information (IPP 6)
- whether any personal information will be stored or transferred outside Victoria (IPP 9)

- the information security controls the company will have in place to protect the information (IPP 4, VPDSS).

Before engaging the company, Tim should also conduct a PIA and SRA to identify any outstanding information privacy and information security risks of engaging the company, and appropriate mitigation strategies. Tim also needs to ensure the residual risks are monitored and reviewed throughout the project, and that further mitigation strategies are put in place as required.

Tim should also request that the company update the contract to include specific reference to the PDP Act and the IPPs, and ensure that the company has the capacity to comply with the IPPs and the PDP Act.

The outsourcing contract

This section discusses the key terms of the contract with the third party. While the terms of the contract with the third party will depend on a range of matters, the contract should include the following elements:

1. Section 17 PDP Act: Where the outsourcing arrangement involves the handling of personal information, organisations should include a clause in the State contract that would have the effect of binding the third party to the IPPs for the purposes of the State contract, in the same way and to the same extent as the organisation.[29]

   The wording of this clause is crucial. It will not be sufficient for the contract to state broadly that the third party will comply with 'relevant privacy law(s)'. Organisations should ensure their contracts are specific about which laws or privacy principles apply, and include any specific protections the organisation expects the third party to implement. Further, organisations should consider ensuring the wording of the clause replicates the wording of section 17(2) of the PDP Act, as appropriate, to ensure the third party is clearly bound to the IPPs.

   In addition, the contract should include a clause requiring the third party to bind any subcontractor to the IPPs. Binding the third party, and any subcontractor, to the IPPs ensures they will be required to handle personal information in a way that adequately protects information privacy.

2. Roles and responsibilities: the contract should clearly specify the roles and responsibilities of each party relating to the functions or activities that are outsourced, including those who will be the key point(s) of contact for information privacy and information security obligations. Where applicable,

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

depending on the type of information involved in the outsourcing arrangement, the contract should also specify the individual(s) who are authorised to access the information.[30]

3. Information privacy and information security obligations: the contract should set out the relevant information privacy and information security obligations the third party must comply with in clear and unambiguous terms. For example, the contract could require a third party to only use personal information for the purposes of carrying out services under the contract. Further, key terms should be well-defined. For example, the third party should have a thorough understanding of what constitutes 'information' for the purposes of the outsourcing arrangement so that the correct information is handled in line with relevant obligations.[31]

   Additionally, an organisation should have a clear understanding of how a third party will handle information under the arrangement and have sufficient oversight over the third party's information handling practices, to ensure it complies with information privacy and information security obligations for the duration of the contract, and handles information appropriately at the end of the contract.

4. Incident management and complaints handling: the outsourcing arrangement should set out the process that will be followed in the event of an information privacy or information security incident, where information subject to the arrangement is, or may have been, compromised. The roles and responsibilities of each party to the arrangement should be clear, including who is responsible for notifying individuals impacted by the incident and reporting the incident to OVIC in line with the Information Security Incident Notification Scheme,[32] where applicable.[33]

   Similarly, the arrangement should set out how enquiries and complaints about the handling of information under the arrangement will be dealt with. Among other things, the arrangement should specify which party is responsible for responding to complaints or enquires, the timeframes for responding, and other bodies to whom the matter may be referred, where applicable.

---

[30] One of the findings in OVIC's investigation into the misuse of Department of Health (**DH**) information by third party employees was that the services agreement between DH and the third party lacked clarity around which party was responsible for managing pre-employment screening requirements, ultimately leading to a breach of IPP 4.1. The investigation report is available here: https://ovic.vic.gov.au/regulatory-action/misuse-of-department-of-health-information-by-third-party-employees-during-pandemic-response/.

[31] OVIC's investigation into the Datatime Services Pty Ltd (**Datatime**) data breach found that one of the reasons Datatime may not have complied with IPP 4.2 was a lack of clarity about what information should be destroyed or de-identified due to a confusion about the terms 'records' and 'data'. OVIC's investigation report is available here: https://ovic.vic.gov.au/regulatory-action/investigation-into-datatime-services-pty-ltd-data-breach/.

[32] Organisations subject to Part 4 of the PDP Act should notify OVIC of incidents that compromise the confidentiality, integrity or availability of public sector information, that have been assessed as having a 'limited' business impact on government operations, organisations or individuals. Detailed guidance on the Information Security Incident Notification Scheme is available on OVIC's website: https://ovic.vic.gov.au/information-security/ovic-information-security-incident-notification-scheme/.

[33] OVIC also has guidance on managing the privacy impacts of a data breach here: https://ovic.vic.gov.au/privacy/resources-for-organisations/managing-the-privacy-impacts-of-a-data-breach/, and guidance on minimising the privacy impacts of an incident, published jointly with the Public Record Office Victoria: https://ovic.vic.gov.au/privacy/resources-for-organisations/joint-public-statement-with-prov-minimising-the-privacy-impacts-of-an-incident/.

5. Access to information: information involved in an outsourcing arrangement should remain accessible and available to organisations to ensure they can fulfil their obligations under the FOI Act. The FOI Act is the primary mechanism for access to and correction of documents held by organisations. In an outsourcing arrangement, an organisation should ensure it remains in possession or control of information created and held by a third party so that the information can be accessed under the FOI Act. The contract between an organisation and a third party should stipulate that the organisation has a right to access information held by the third party for the purposes of the contract, to ensure proper accountability and transparency of outsourced government functions and services.

   IPP 6 gives individuals the right to access their personal information held by an organisation, subject to some exceptions, and make corrections to it.[34] If an individual's personal information is involved in an outsourcing arrangement, organisations should ensure they can comply with the requirement to provide access to the information. IPP 6 will apply to information held by the third party where the third party has been contractually bound to the IPPs. Note that IPP 6 will only apply where the FOI Act does not.[35]

6. Compliance and oversight mechanisms: organisations should actively monitor a third party's compliance with the IPPs and information security obligations, and any contractual obligations relating to information handling. The outsourcing arrangement should either require the third party to be involved in the organisation's protective data security plan,[36] or otherwise include robust compliance and oversight mechanisms. The mechanisms will depend on the nature and duration of the arrangement but could include:

   - periodic reviews of the outsourcing arrangement, to assess whether it remains fit-for-purpose
   - regular reviews of the third party's information handling practices, including monitoring of compliance with any recordkeeping obligations
   - regular reviews of PIAs and SRAs undertaken in relation to the outsourcing arrangement, to ensure risks are monitored appropriately
   - a requirement for the third party to annually attest to compliance with the information privacy and information security obligations in the arrangement

[34] Section 4(1) of the PDP Act states that organisations hold personal information if the information is contained in a document that is in the possession or under the control of the organisation, whether alone or jointly with other persons or bodies, irrespective of where the document is situated, whether in or outside Victoria.

[35] Further guidance on when IPP 6 applies is available in the IPP Guidelines: https://ovic.vic.gov.au/book/ipp-6-access-and-correction/.

[36] Section 89(3), PDP Act. The protective data security plan of an organisation subject to Part 4 of the PDP Act must address a third party's compliance with the VPDSS applicable to the organisation, where the third party collects, holds, uses, manages, discloses or transfers public sector data for the organisation.

- a requirement for the third party to inform the organisation of any changes in its information privacy or information security practices that impact the way in which information is handled under the arrangement.

The contract should stipulate the consequences for the third party if it fails to comply with the required information privacy and information security obligations. Organisations should make it clear to the third party what action it will take for non-compliance with the contract.

7. Information handling at the end of a contract: the contract should specify how the third party should handle information once the contract ends. For example, the contract could require the third party to return all information involved in the outsourcing arrangement to the organisation within a specified timeframe at the end of the contract, or dispose of the information in line with relevant obligations. The contract should also contain provisions that enable the organisation to be satisfied that documents have been properly dealt with, for example, clauses that:

    - require the third party to attest that it has complied with the specified information handling requirements at the conclusion of the contract
    - permit the organisation to audit the third party's systems to ensure relevant information has been removed.

Similarly, where the organisation provided assets to the third party to facilitate the outsourcing arrangement, such as workstations and IT equipment, the contract should detail how these will be returned to the organisation.

The contract between the third party and any subcontractors should also contain provisions relevant to the subcontractor's handling of information at the conclusion of the contract.

During the outsourcing arrangement

This section discusses matters that are relevant during the life of the outsourcing arrangement.

Privacy policies and notices of collection

Organisations should ensure their privacy policies[37] and any relevant notices of collection[38] accurately reflect the way in which personal information will be handled under the outsourcing arrangement. For

[37] Detailed guidance on privacy policies is available on OVIC's website: https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-policies/, and in the Guidelines to the IPPs in relation to IPP 5: https://ovic.vic.gov.au/book/ipp-5-openness/#IPP_5.1:_Written_policy_on_management_of_personal_information_.

[38] Detailed guidance on notices of collection is available in the IPP Guidelines in relation to IPP 1: https://ovic.vic.gov.au/book/ipp-1-collection/.

example, whether personal information collected will be disclosed to third parties, and the circumstances in which it will be disclosed.

In addition, organisations should ensure a third party has a comprehensive privacy policy that reflects how personal information will be handled under the arrangement and, where applicable, creates or updates any relevant notices of collection. Where personal information is involved, it should be clear to individuals from privacy policies and notices of collection exactly which organisation is handling their information.

Training and awareness

Organisations should ensure the third party (and its subcontractors if applicable) has a comprehensive information privacy and information security training and awareness program for its employees. Information is more likely to be handled in accordance with relevant information privacy and information security obligations where employees know and understand their role in handling information appropriately. Training should be provided to employees at the start of their employment and regularly in the course of their employment.

An organisation may wish to ensure the training a third party provides to its employees is consistent with that which the organisation provides to its own employees.

Ongoing monitoring and assurance

Organisations should implement measures to ensure a third party upholds information privacy and information security obligations for the duration of the arrangement. The terms of a contract are not self-enforcing and require a level of assurance that they are being adhered to. Such measures could include:

- conducting regular site visits, surveys, reports, attestations or audits on how the third party (and where applicable, its subcontractors) is handling information and complying with obligations
- regularly reviewing the outsourcing arrangement, including reassessing information privacy and information security risks and associated mitigation strategies, and updating them as needed
- working closely with the third party to respond to information privacy and information security incidents when they occur
- reviewing any significant changes to the outsourcing arrangement that may impact information privacy or information security
- having a clear process in place for ensuring information is handled appropriately once the arrangement comes to an end.

Ending the outsourcing arrangement

When the outsourcing arrangement comes to an end, either by way of completion of the contract or termination by one of the parties, an organisation should ensure all information involved in the arrangement is handled in line with information privacy, information security and recordkeeping obligations.[39] Retaining information for longer than necessary not only increases the risk to the security of the information but also increases the risk of function creep, where the information is used for purposes beyond those specified in the outsourcing arrangement.

Recordkeeping obligations

Most organisations subject to the PDP Act will also be bound by the Public Records Act. Organisations must comply with recordkeeping standards[40] that apply to information[41] that is collected, used, disclosed, created or otherwise involved in the outsourcing arrangement, such as retention and disposal authorities (**RDAs**). RDAs set the minimum required retention periods, authorise the disposal of public records and identify records that have permanent value.[42]

Organisations that are required to comply with the IPPs must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose. It should be noted that a valid purpose for retaining personal information is to comply with relevant recordkeeping requirements in the Public Records Act.[43]

Destruction or transfer of information held by the third party

Organisations should not rely solely on the third party to return the information or dispose of it according to the terms of the outsourcing arrangement.

In addition to any contractual clauses specifying how the third party is required to handle information at the end of the arrangement, organisations should have comprehensive policy and procedure documentation that applies when a contract ends. The documentation should cover key matters such as

[39] For example, IPP 4.2 in the PDP Act requires an organisation to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

[40] The recordkeeping standards developed by the Public Record Office Victoria (**PROV**) are a set of mandatory principles and requirements regarding the creation, access, storage, management and disposal of public records. Further information on the standards is available on PROV's website: https://prov.vic.gov.au/recordkeeping-government/getting-started.

[41] Under the Public Records Act, information and data are considered records and should be handled in line with relevant recordkeeping obligations.

[42] Detailed information on RDAs is available on PROV's website: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas.

[43] Detailed guidance on IPP 4.2 is available in the data security Chapter of the IPP Guidelines on OVIC's website: https://ovic.vic.gov.au/book/ipp-4-data-security/#IPP_4.2_Disposal_of_Data.

what will happen to the information once the arrangement ends and the role(s) responsible for ensuring the information is handled in line with information privacy, information security and recordkeeping obligations.

Organisations should require third parties to attest to their compliance with obligations that apply at the conclusion of the contract.

Final audit or report from the third party

Organisations should consider undertaking a final audit of the third party or require the third party to submit a final report, to make sure all information involved in the outsourcing arrangement is accounted for and has been handled in line with the relevant obligations. Failing to conduct a final audit or account for all the relevant information can pose a significant risk to the privacy and security of the information.

Example

In 2024 OVIC completed an investigation into Datatime Pty Ltd, a third party engaged by multiple Victorian Government organisations to provide data entry and document scanning services. Datatime suffered a data breach in the form of a ransomware attack. This resulted in a malicious actor gaining access to the personal information of thousands of Victorians.

OVIC's investigation focused on IPP 4, specifically, the security measures that Datatime had in place to protect the personal information it held, and its data retention and disposal practices. Datatime was voluntarily wound up before OVIC could complete its investigation, however it appeared that Datatime's cybersecurity controls were lacking in the following areas:

- insufficient application control measures and restriction of administrative privileges
- absence of multi-factor authentication across all user accounts for logging into its networks directly and via Virtual Private Network
- complex passphrase rules for Datatime accounts
- ineffective firewall configuration to control incoming and outgoing network traffic
- endpoint detection and prevention software on Datatime computers
- incident detection and response by way of insufficient capture and monitoring of relevant logs.

OVIC also found the following concerns in relation to data retention and disposal:

- data from as early as the year 2003 was found to have been retained by Datatime
- Datatime did not understand its obligations to comply with IPP 4.2 and its intersection with the Public Records Act
- the terms of Datatime's contracts with Victorian Government organisations were not well defined and Datatime was unclear about what information it should destroy and when.

Organisations should actively monitor a third party's (and their own) compliance with the IPPs and any contractual obligations relating to information handling. Depending on the privacy risks involved, this may include attestations, surveys, reports, site visits or audits. Contract provisions are not self-enforcing, and require some level of assurance that they are, in fact, being adhered to.

Outsourcing organisations should conduct appropriate due diligence in relation to a prospective third party's information security posture, to ensure it will be capable of appropriately handling public sector information, including personal information. Where a third party is engaged over a long period of time, the outsourcing organisation should regularly review the third party's practices. Due diligence does not end once the contract is signed.

www.ovic.vic.gov.au