Guidelines for outsourcing in the Victorian public sector

Checklist

Issued May 2017

Commissioner for Privacy and Data Protection

VICTORIA State Government

This page is intentionally left blank.

Guidelines for outsourcing in the Victorian public sector

Checklist

Issued May 2017

Published by the Commissioner for Privacy and Data Protection
PO Box 24014
Melbourne Victoria 3001

First published May 2017

Also published on:
http://www.cpdp.vic.gov.au

ISBN 978-0-9946370-9-3

DOCUMENT DETAILS	
Security Classification	Public domain
Version	V.01
Issue Date	May 2017
Document Status	Final
Authority/Approval	Office of the Commissioner for Privacy and Data Protection (CPDP)

This page is intentionally left blank.

How to use this document

This checklist and the accompanying guide aim to assist Victorian public sector bodies and their contracted service providers (CSPs) to effectively manage the privacy and security of official information (public sector data and personal information) in outsourcing arrangements.

This checklist provides a high level overview of the matters that ought to be considered at each stage of an outsourcing arrangement, by walking through a series of questions to help public sector bodies determine whether they are meeting their privacy and data security obligations under the *Privacy and Data Protection Act 2014* (PDPA). The accompanying guide explores each question in more detail and explains the relevant requirements under the PDPA. If you select a response that is shaded orange in the checklist, you are encouraged to refer to the accompanying guide for further guidance. The question numbers in this checklist correspond with the headings in the guide for ease of reference.

The documents are structured around three key phases of an outsourcing arrangement:

- *Planning the outsourcing arrangement*, covered by Steps 1-4
- *Implementing the outsourcing arrangement*, covered by Step 5
- *Concluding the outsourcing arrangement*, covered by Step 6.

Although the checklist and guide are primarily directed at Victorian public sector bodies, they provide a useful road map for CSPs to understand, and prepare to respond to, the privacy and data security requirements of their public sector clients.

The privacy requirements relate to *personal information* as defined under the PDPA; *health information* is expressly excluded from the remit of the checklist and guide. Outsourcing arrangements involving health information should be determined in accordance with the *Health Records Act 2001*.

The checklist and guide are intended to provide a starting point for the consideration of privacy and data security risks in an outsourcing arrangement. The matters canvassed here are of a general nature and **not exhaustive**. The documents may overlook risks and issues that arise in specific contexts, and organisations are encouraged to seek their own legal advice to ensure they are meeting their obligations.

These documents are guidelines only. They do not supersede information handling provisions in other legislation, and are not intended to create new policy for the Victorian public sector. Instead they describe the privacy and data security obligations that already exist under the PDPA, and aim to simplify the process for public sector bodies in navigating the regulatory landscape.

The checklist and guide assume a certain level of prior privacy and data security knowledge. Where possible, the guide refers to other materials that will provide further detail and explanation of key concepts.

Step One — Planning the outsourcing arrangement

1.1 Consider privacy and data security in the design of the outsourcing arrangement

a)	Does the outsourcing arrangement diminish privacy protections or data security for official information afforded by the outsourcing party?	Yes	No
If yes –			
	Are there any alternative arrangements that could achieve the same objectives with a lesser impact to privacy and data security?	Yes	No
	Do the expected benefits outweigh the increased risk to the privacy or security of official information?	Yes	No

1.2 Identify and assess the value of all information that may be affected by the outsourcing arrangement

a)	Will the CSP ***collect, generate or have direct access*** to official information that is:		
	Publicly available?	Yes	No
	UNCLASSIFIED but non-public, requires a Dissemination Limiting Marker (DLM) or has a Business Impact Level (BIL) of 1?	Yes	No
	PROTECTED or above, or has a BIL of 2 or above?	Yes	No
	Personal information?	Yes	No
b)	Might the CSP have ***indirect access*** to official information that is:		
	Publicly available?	Yes	No

	UNCLASSIFIED but non-public, requires a DLM, or has a BIL of 1?	Yes	No
	PROTECTED or above, or has a BIL of 2 or above?	Yes	No
	Personal information?	Yes	No
c)	Might the contracted services affect the ***confidentiality, integrity, or availability*** of official information (whether or not the CSP has access to it) that is:		
	Publicly available?	Yes	No
	UNCLASSIFIED but non-public, requires a DLM, or has a BIL of 1?	Yes	No
	PROTECTED or above, or has a BIL of 2 or above?	Yes	No
	Personal information?	Yes	No

1.3 Be aware of any relevant secrecy or information handling obligations

a)	Does the proposed outsourcing arrangement comply with secrecy and information handling provisions in other legislation, including enabling legislation?	Yes	No
b)	Does the outsourcing arrangement involve new or different uses or disclosures of personal information that the outsourcing party already holds?	Yes	No
If yes –			
	Are these consistent with the relevant collection notices?	Yes	No
	Are these consistent with existing privacy policies?	Yes	No

Step Two — Choosing the right CSP

2.1 Consider whether the CSP is sufficiently resourced to provide adequate privacy and data security protections

a)	Will the CSP require significant upgrades or changes to any of the following in order to comply with the VPDSF and the IPPs?		
	Security governance	Yes	No
	Personnel screening	Yes	No
	Physical security	Yes	No
	ICT security	Yes	No
	Policies and procedures for handling personal information	Yes	No
b)	If yes to any of the above –		
	Does the CSP have access to sufficient expertise and/or resources to enable them to make any necessary changes?	Yes	No

2.2 Consider the privacy and data security culture and track record of the CSP

a)	Is the CSP able to demonstrate an ongoing commitment and willingness to maintain high standards of privacy and data security?	Yes	No
b)	Does the CSP have a history of privacy incidents and/or data breaches?	Yes	No
If yes –			
	Are they able to demonstrate that they responded quickly and effectively, and that the root causes of the incidents have been remediated?	Yes	No

2.3 Consider whether the CSP will engage a subcontractor (or subcontractors)

a)	Will the CSP engage a subcontractor to perform functions or activities under the State contract?	Yes	No
If yes –			
	Have appropriate steps been taken to manage any privacy and data security risks that may arise from the subcontracting relationship?	Yes	No

2.4 Consider whether the CSP is an interstate or overseas organisation, and whether information will be transmitted or stored outside Victoria

a)	Is the CSP based interstate or overseas?	Yes	No
If yes –			
	Have the risks to data confidentiality, integrity or availability that may arise from another jurisdiction's legislative requirements been considered?	Yes	No
	Will the PDPA be enforceable against the CSP (and can section 17 of the PDPA be relied upon to allocate responsibility for IPP compliance to the CSP)?	Yes	No
b)	Will information be stored or transmitted outside of Victoria?	Yes	No
If yes –			
	Have any additional risks that may be associated with holding information offshore (including as a result of foreign legislative requirements) been considered?	Yes	No
	Has the application of IPP 9, which limits transborder flows of personal information, been taken into account?	Yes	No

Step Three — VPDSF planning and due diligence

3.1 Governance — Roles and responsibilities

a)	Will official information be available to CSP personnel outside of the outsourcing party's facilities?	Yes	No
If yes –			
	Have the key security point(s) of contact in the CSP who are responsible for protective data security been identified?	Yes	No
	Has the CSP provided a list of all their personnel (including subcontractors) who will have access to official information?	Yes	No
b)	Will the CSP only access official information from within the outsourcing party's facilities?	Yes	No
If yes –			
	Has a point of contact within the outsourcing party in relation to protective data security matters for CSP personnel been appointed?	Yes	No
	Do the outsourcing arrangements require pre-acceptance of proposed CSP personnel prior to allowing access to the facilities?	Yes	No

3.2 Governance — Training and awareness

a)	Are CSP personnel required to complete initial and/or ongoing protective data security training and awareness programs?	Yes	No

3.3 Governance — Incident management and reporting

a)	Have clear arrangements been established for the handling of data security breaches?	Yes	No
In particular –			
	Has an incident management processes been put in place?	Yes	No
	Has the CSP agreed to report all incidents involving the outsourcing party's information within specified timeframes?	Yes	No
	Has the CSP agreed to provide the outsourcing party full and free access to their facilities and systems for the purposes of investigating protective data security breaches?	Yes	No
	Are there consequences for the CSP if a serious protective data security breach occurs?	Yes	No

3.4 Governance — Business continuity

a)	Are there negative impacts that could arise if information affected by the outsourcing arrangement is lost or not available for a period of time?	Yes	No
	If yes, have business continuity measures been put in place to address this risk?	Yes	No

3.5 Governance — Compliance and oversight

a)	Will the outsourcing arrangement be ongoing or in place for an extended period of time?	Yes	No
If yes –			
	Will there be periodic compliance checks?	Yes	No
	Will the CSP provide annual attestations of compliance with security requirements?	Yes	No

3.6 Governance — Transfer of data back to outsourcing party on termination or completion of contract

a)	Will official information that is not publicly available be provided to or generated by the CSP?	Yes	No
If yes –			
	Will the CSP provide an attestation at the conclusion of the contract that all information has been returned or disposed of?	Yes	No
	Will the CSP return or decommission any security measures provided by the outsourcing party?	Yes	No
	Will the CSP allow audit of their systems/facilities to ensure data has been removed?	Yes	No

3.7 Information Security — Protective markings and hardcopy documents

a)	Will the CSP be required to observe protective markings that have been applied to documents and to apply protective markings to new documents where appropriate?	Yes	No
b)	Are the specific security measures imposed by the CSP in relation to hardcopy information equal to, or stronger than, the outsourcing party's internal measures for similar information?	Yes	No

3.8 Personnel Security — Employment screening

a)	Have, or will, all CSP personnel with access to official information undergone/undergo an appropriate level of initial and ongoing screening?	Yes	No

3.9 ICT security

a)	Will official information be collected by or provided to the CSP electronically?	Yes	No
If yes –			
	Will appropriate measures be in place to manage the security of the data while in transit?	Yes	No
b)	Will official information be stored and/or accessed electronically by the CSP?	Yes	No
If yes –			
	Does (or will) the CSP have appropriate controls in place to manage access to systems containing official information?	Yes	No
c)	Will the CSP be responsible for disposing of electronic information?	Yes	No
If yes –			
	Will the CSP comply with data disposal requirements and any record keeping requirements (including those relating to the sanitisation of faulty hard drives or other ICT equipment)?	Yes	No

3.10 Physical security

a)	Do the CSP's physical security measures meet or exceed the outsourcing party's own internal requirements for similar information?	Yes	No

Step Four — IPP planning and due diligence

**** Complete Step 4 only if your outsourcing arrangement involves personal information.***

4.1 Liability for compliance with the IPPs

a)	Has the CSP assumed liability for their compliance with the IPPs?	Yes	No
If yes –			
	Is the PDPA enforceable against the CSP?	Yes	No

4.2 Training and awareness

a)	Are CSP personnel required to complete initial and/or ongoing privacy training and awareness programs?	Yes	No

4.3 Data security (IPP 4 and VPDSF)

a)	Can the CSP ensure adequate data security for personal information?	Yes	No

4.4 Ensuring personal information is accurate, complete and up to date (IPP 3)

a)	Will there be processes in place to ensure personal information is accurate, complete and up to date?	Yes	No

4.5 Privacy policies (IPP 5)

a)	Does the CSP have, or will it have, a privacy policy in place?	Yes	No
b)	Does the outsourcing party's privacy policy adequately explain information flows under the outsourcing arrangement and identify who is responsible for IPP compliance?	Yes	No

4.6 Collection notices (IPP 1)

a)	Does the CSP have, or will it have, adequate collection notices in place?	Yes	No

4.7 Transferring personal information to and from the CSP (IPP 2)

a)	Will the outsourcing party disclose personal information to the CSP? (Will the CSP collect personal information from the outsourcing party?)	Yes	No
If yes –			
	Is the CSP's collection consistent with IPP 1.4?	Yes	No
	Is the outsourcing party's disclosure consistent with IPP 2.1?	Yes	No

4.8 Sensitive information (IPP 10)

a)	Will the CSP collect sensitive information during the course of the outsourcing arrangement?	Yes	No
If yes –			
	Are there measures in place to ensure compliance with IPP 10?	Yes	No

4.9 Access and correction (IPP 6)

a)	Have clear arrangements been established for the handling of access and correction requests?	Yes	No
b)	Is information about how to make an access and/or correction request (and who it should be directed to) available to the public?	Yes	No

4.10 Complaint handling

a)	Have clear arrangements been established for the handling of complaints?	Yes	No
b)	Is information about how to make a privacy complaint (and who it should be directed to) available to the public?	Yes	No

4.11 Handling privacy breaches

a)	Have clear arrangements been established for the handling of privacy breaches?	Yes	No
In particular –			
	Is the CSP required to notify the outsourcing party if a privacy breach occurs?	Yes	No
	Is the outsourcing party able to direct the CSP to take action to mitigate any consequences of a breach?	Yes	No
	Will the CSP be required to notify CPDP of the breach?	Yes	No

4.12 Handling personal information at the end of the contract

a)	Have arrangements been made for the return, destruction or permanent de-identification of personal information at the conclusion of the contract? (See 3.6 above)	Yes	No

Step Five — Ongoing steps during performance of the contract

5.1 Ongoing monitoring and assurance

a)	Has the outsourcing party arranged for an appropriate level of ongoing monitoring and assurance of VPDSF and IPP compliance over the course of the contract?	Yes	No

Step Six — At the conclusion of the contract

6.1 Destruction or transfer of official information held by the CSP

a)	Has the outsourcing party confirmed that all requirements for destruction or return of data have been complied with and secured all relevant attestations?	Yes	No

6.2 Final audit/report from the CSP

a)	If appropriate, has a final audit of the CSP been undertaken to ensure that all official information has been securely returned or disposed of and is accounted for?	Yes	No

6.3 Renewing and extending contracts

a)	Is the contract being renewed or extended?	Yes	No
If yes –			
	Do the existing terms adequately deal with privacy and data security?	Yes	No

Glossary

Availability: the desired state that allows authorised persons to access defined information for authorised purposes at the time they need to do so.

Business Impact Level (BIL): numerical measures of scaled consequences, identifying the potential impact arising from a compromise to the confidentiality, integrity or availability of information. BILs are also referred to as a consequence table.

Confidentiality: the limiting of official information to authorised persons for approved purposes. The confidentiality requirement is determined by considering the potential consequences of unauthorised disclosure of the official information.

Contracted service provider (CSP): a person or body who provides services under a State contract.

Dissemination Limiting Marker (DLM): a protective marking that indicates access to official information should be limited. DLMs are to be used when a security assessment of potential compromise of confidentiality of the information identifies that disclosure is limited or prohibited by legislation, or where special handling is required and dissemination of the information needs to be controlled.

Information privacy: refers to an individual's right to determine for themselves who has access to their personal information and how it is used.

Information Privacy Principles (IPPs): refers to the 10 principles contained in Schedule 1 of the *Privacy and Data Protection Act 2014* that set out the minimum requirements for the collection and handling of personal information in the Victorian public sector.

Integrity: the assurance that official information has been created, amended or deleted only by the intended authorised means and is correct and valid.

Official information: a term used in this document to refer to both *public sector data* and *personal information*.

Outsourcing: the contracting out of functions or activities.

Outsourcing party: an organisation that contracts out the performance of functions or activities to another person or body.

Personal information: defined in the *Privacy and Data Protection Act 2014* as information or an opinion (including information or an opinion forming part of a database), 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, but does not include information of a kind to which the *Health Records Act 2001* applies.

Protective data security: a risk management process designed to safeguard official information assets and services in a way that is proportionate to threats and supportive of business; uses a combination of procedural, physical, personnel, information and ICT security measures to protect against security threats.

Public sector body: a term used in this document to collectively refer to organisations to which Part 3 of the PDPA applies, and agencies and bodies to which Part 4 of the PDPA applies.

Public sector data: any information (including personal information) obtained, received, or held by an agency or body to which Part 4 [of the PDPA] applies.

Sensitive information: defined in the *Privacy and Data Protection Act 2014* as information or an opinion about an individual's –

(a) racial or ethnic origin; or
(b) political opinions; or
(c) membership of a political association; or
(d) religious beliefs or affiliations; or
(e) philosophical beliefs; or
(f) membership of a professional or trade association; or
(g) membership of a trade union; or
(h) sexual preferences or practices; or
(i) criminal record – that is also personal information.

State contract: a contract between an organisation (as defined in s. 3 of the *Privacy and Data Protection Act 2014*), person, agency or body (to which Part 4 or 5 of the *Privacy and Data Protection Act 2014* applies), and another person or body under which services are provided to one party (the outsourcing party) by the other party (the contracted service provider) in connection with the performance of the functions of the outsourcing party.

Subcontracting: when a contracted service provider subsequently outsources the functions or activities they have been engaged to provide to the original outsourcing party.

Victorian Protective Data Security Framework (VPDSF): the overall scheme for the security of Victoria's public sector data, as required under section 85 of the *Privacy and Data Protection Act 2014*.

Victorian Protective Data Security Standards (VPDSS): 18 standards that cover governance and the four security domains for the security, confidentiality and integrity of public sector data and access to public sector data. The standards form part of the VPDSF.

Notes

This page is intentionally left blank.

Commissioner for Privacy and Data Protection

VICTORIA State Government