Applying the legislation

GUIDELINE *Information Privacy Act 2009*

Contracts and other agreements

Increasingly agencies[1] are engaging an external entity (**contracted service provider**) to perform some of their functions or activities.[2] Where agencies enter into service arrangements that involve personal information, chapter 2, part 4 of the *Information Privacy Act 2009* (Qld) (**IP Act**) may require the contracting agency to take all reasonable steps to bind the contracted service provider to comply with the privacy principles.[3]

This requirement does not limit the privacy protections that can be provided for in the service arrangement.[4]

What is a service arrangement?

The obligations in chapter 2, part 4 only apply to a service arrangement. A service arrangement does not need to be a formal contract; it can be any agreement that meets the following criteria:

- the service must be for the purpose of performing one or more of the contracting agency's functions
- the service must be provided either directly to the contracting agency, or to someone else on behalf of the contracting agency; and
- the contracted service provider must not be another Queensland government agency, or an employee of the contracting agency.

When is an agency required to bind a contracted service provider?

An agency must take all reasonable steps to bind a contracted service provider to comply with the privacy principles if:

- the contracted service provider will deal[5] with personal information for the contracting agency, or
- the provision of services under the arrangement will involve:
  - personal information being transferred to the contracting agency; or
  - the contracted service provider providing services to a third party on behalf of the contracting agency.

Checklist

The Contracted service provider checklist in Appendix A will help agencies work out whether they need to take reasonable steps to bind a contracted service provider.

[1] In this guideline, references to an agency include a Minister unless otherwise noted.
[2] This process of contracting out an agency's services or functions to an external provider is commonly referred to as "outsourcing."
[3] Either the Information Privacy Principles (**IPPs**) or National Privacy Principles (**NPPs**), whichever is applicable to the contracting agency, and with section 33 of the IP Act, which concerns the transfer of personal information outside Australia.
[4] Section 35(4) of the IP Act.
[5] Dealing includes receiving, collecting, storing or processing personal information and includes situations where the service provider is simply holding the information.

Exceptions

An agency is **not required** to bind a contracted service provider to comply with the privacy principles if **all** the following apply:

- the contracted service provider receives funding from the contracting agency
- the contracted service provider will not collect any personal information for the contracting agency
- the contracted service provider will not give any personal information it collects while performing the agreement to the agency; and
- the agency will not give any personal information to the contracted service provider.[6]

Note

A contracted service provider that would normally be subject to the *Privacy Act 1988* (Cth), will not be subject to that Act for anything it does in relation to a State Government contract.[7] This will be the case whether or not it is made subject to the IP Act privacy principles.

Even if agencies are not required to bind the contractor to the privacy principles, IPP 4(1)(b) and NPP 4(1) require them to ensure personal information disclosed to third parties in connection with the provision of a service is protected from misuse, loss and unauthorised access, modification or disclosure.

Who is responsible for a breach of privacy?

Once bound, the contracted service provider assumes the privacy obligations[8] as if it were the agency. In the event of a breach, any privacy complaint would be made against the contracted service provider.[9]

If the contracting agency *should* have taken all reasonable steps to bind the contractor and didn't, the contracting agency will be liable for any privacy breaches of the contracted service provider.[10] However, the agency will not be liable if, despite taking all reasonable steps, it was not able to bind the contractor.

Additional privacy considerations

In addition to binding contracted service providers where required by chapter 2, part 4 of the IP Act, agencies must also meet their obligations under the other privacy principles[11].

[6] Section 35(3) of the IP Act.
[7] Section 7B(5) of the *Privacy Act 1988* (Cth).
[8] In relation to personal information held by the service provider for the purposes of performing its obligations under the service arrangement.
[9] Section 36(3) and section 164(2)(b) of the IP Act.
[10] Section 37(2) of the IP Act.
[11] The NPPs for health agencies, the IPPs for all other agencies, and section 33—overseas transfer of personal information—for all agencies.

Giving personal information to contractors

The privacy principles create rules for both the use and disclosure of personal information.[12] When engaging an external contractor, an agency will need to consider—

- the service being provided; and
- who will control any personal information provided to the professional

—to work out whether giving personal information to the contractor will be a use or a disclosure.

Use

Generally, if an agency *uses* personal information to seek advice about, or engage a contractor to deal with, a matter involving an individual, it will be directly related to why their personal information was originally collected. Use for a directly related purpose is permitted by the privacy principles.[13]

If the agency is engaging the contractor to do something on the agency's behalf, and the agency will maintain control of the personal information it provides, then it will be a *use*[14] of personal information.

Example

The agency enters into an agreement with SuperQuik Collections to recover a debt from Bob and they give SuperQuik a copy of the relevant information about Bob's debt. The agency's agreement with SuperQuik states that SuperQuik will only use Bob's information to recover the debt, will ensure it's stored and handled securely, and will return all of Bob's information at the end of the agreement.

Disclosure

If the agency will not retain control of the personal information it gives to the contractor it will generally be a *disclosure*[15] of personal information, which may breach the privacy principles.[16]

Contractors engaging subcontractors or specialists

If an agency approves, and the personal information is protected, the contractor giving personal information to another party outside the agency can also be a use.

[12] National Privacy Principle 2 (NPP 2) for health agencies; Information Privacy Principle 10 (IPP 10 - use) and Information Privacy Principles 11 (IPP 11 - disclosure) for other agencies.
[13] IPP 10(1)(e) and NPP 2(1)(a) - see IPP 10(1) or NPP 2(1) for a full list of permitted uses of personal information.
[14] Section 23(3) of the IP Act defines 'use'; also see [whatever key privacy concepts use ends up being called]
[15] Section 23(2) of the IP Act defines 'disclosure'; also see [whatever key privacy concepts disclosure ends up being called]
[16] Refer to NPP 2(1) or IPP 11(1) for a full list of when personal information can be disclosed.

Contracting agency using personal information concurrently with the contracted service provider

In some circumstances, the contracting agency may intend to retain and continue using copies of personal information given to the contracted service provider[17]. Under IPP 10 and NPP 2, an agency must not use personal information for a purpose other than that for which it was obtained, unless a permitted exemption applies.

If the function for which the personal information was obtained is now being undertaken solely by the contracted service provider, any use of the personal information by the contracting agency will constitute a secondary use and will need to be permitted under one or more of the exceptions in IPP 10 or NPP 2.[18]

Early engagement with service providers

While not required by the IP Act, assessing a service provider's capacity for privacy compliance prior to engagement can help determine if they have the ability and resources to meet the IP Act's privacy obligations.

One approach is to check whether the contractor has been assessed and accredited against an industry quality assurance framework that includes an appropriate privacy standard.[19]

Another approach is to include information about the privacy principle compliance requirement in material inviting offers. This ensures potential service providers are aware of the privacy obligations which attach to the contract. Agencies may also wish to specify demonstrated capability to comply with the privacy principles as one of the evaluation criteria in the invitation documentation.

Privacy considerations when drafting a service arrangement

Privacy Impact Assessments

Conducting a Privacy Impact Assessment (**PIA**) will provide a clear understanding of how personal information will flow in the outsourcing arrangement. This will help inform what provisions should be included in the service arrangement. For further information on conducting a PIA, please refer to Conducting a Privacy Impact Assessment.

Deed of privacy

A Deed of Privacy can be used to protect privacy in outsourcing arrangements. A template with sample clauses that agencies can adapt or build on to suit their

[17] For example, the contracted service provider may have been provided with copies of the information or they may be able to access the contracting agency's database remotely.
[18] An exception to this is where there were two or more purposes for the agency obtaining the personal information and only one of these purposes is outsourced. The agency's use of the personal information for the remaining purpose(s) still constitutes a use for the primary purpose and accordingly, would not trigger IPP 10 or NPP 2 obligations.
[19] For example, the *Human Services Quality Framework* is a quality system for measuring the quality of disability services, community care, child safety and community services, which requires that an organisation has an effective information management system that maintains appropriate controls of privacy for stakeholders.

specific circumstances when drafting service arrangements is available here: Deed of Privacy.

The template is intended to serve as a starting point to address areas such as storage, use, and disclosure of personal information and data breach notification. It does not cover all privacy considerations that may arise when drafting a service arrangement.

Standard Terms

The Queensland Government Service Agreement - Standard Terms for Social Services provides another example of how privacy consideration can be addressed in a service arrangement.

Contractor's employees

Agencies could consider requiring the contractor's employees to sign a Deed of Confidentiality, addressing, for example:

- how personal information is to be handled; and
- that the contractor's employees will attend training in privacy awareness and compliance[20].

Subcontractors

The obligations in chapter 2, part 4 only allow for contractors to be bound to comply with the privacy principles, not subcontractors. If an individual's privacy is breached by a subcontractor, they cannot make a privacy complaint under the IP Act[21] against the subcontractor.

Agencies should consider imposing contractual obligations on the bound contracted service provider such as:

- prohibiting the use of a subcontractor; or
- requiring any subcontract to include the requirement that the subcontractor comply with the privacy principles[22].

Alternatively, the agency could consider:

- specifically stating in the service arrangement that the bound contracted service provider retains full liability for any privacy breaches by the subcontractor.[23]
- requiring the bound contracted service provider enter into a Deed of Privacy with the subcontractor. A Deed of Privacy cannot make the subcontractor subject to the IP Act, but it can set out the consequences of any privacy breach and the compensation or redress available.

[20] This may be provided by the contracted service provider or by the agency, whichever is appropriate, and detailed in the service arrangement. Some agencies may have in-house privacy compliance training that would be suitable for the contractor's employees, particularly where the contractor may be natively subject to the *Privacy Act 1988* or to no privacy law at all.
[21] Under section 165 of the IP Act.
[22] This will not bind the subcontractor to the IP Act, but it will contractually obligate them to comply with the privacy principles.
[23] In part, this obligation already exists through the operation of IPP 4(1)(b) and NPP 4.

Limits on use and disclosure

The privacy principles provide a number of exemptions that allow the use and disclosure of personal information for purposes other than that for which it was collected. These exceptions also apply to bound contracted service providers. For example, a contracted service provider may be able to use personal information for a purpose not related to the service arrangement if they obtain the agreement of the individual whom the personal information is about.[24]

The contracting agency may wish to include a provision setting out that, if a bound contracted service provider relies or intends to rely on any of the exceptions in IPPs 10 and 11 or NPP 2, it must notify the agency first.

Transfer of personal information outside of Australia

A bound contracted service provider is subject to section 33 of the IP Act, which sets out when personal information can be transferred outside Australia.[25] To ensure that there is no breach of this provision, the service arrangement could further limit or specifically outline in which circumstances personal information can be transferred outside of Australia.

Privacy complaints

If an individual believes a bound contracted service provider[26] has not complied with the privacy principles in relation to their personal information, they can make a privacy complaint.[27] It is recommended that the service arrangement specify who will be responsible for handling privacy complaints and how privacy complaints will be managed.[28]

Data breach notification

Although the IP Act does not impose any mandatory data breach notification requirements, prompt notification will allow the agency to minimise the negative impacts resulting from the breach.

Agencies should consider including a provision in the service arrangement that specifies when and how the bound contracted service provider is required to notify the agency of a data breach.[29]

Examples of potential data breaches include:

- lost or stolen laptops, portable storage devices, or physical files containing personal information
- an agency mistakenly providing personal information to the wrong person
- databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the organisation; or

[24] Under IPP 10(1)(a).
[25] Refer to Sending personal information out of Australia for more information.
[26] Section 164(2)(b) of the IP Act.
[27] See Chapter 5 of the IP Act.
[28] Including complaints about sub-contractors, where appropriate.
[29] In this guideline, data breach means when personal information held by an agency or bound contracted service provider is lost or subjected to unauthorised access, use, modification, disclosure or other misuse.

- employees accessing personal information outside the requirements of their employment.

If the breach is systemic and rectification is not possible, the agency may consider whether this would provide grounds to terminate the service arrangement.

Access and amendment

The IP Act provides individuals with the right to access and amend their personal information. These rights are primarily set out in chapter 3 of the IP Act.

Despite being bound to comply with the privacy principles, bound contracted service providers are not an agency and therefore chapter 3 does not apply to them. Documents in their possession, however, may be subject to that right if the agency retains control[30] of them.

It is important that the service arrangement sets out which documents and information the agency owns/controls.[31] It should also set out that these documents must be provided to the agency upon request.

Privacy performance review

The service arrangement may permit a performance review of the contracted service provider's compliance with the privacy obligations in the IP Act.

Performance monitoring could include:

- regular surveys, reports and/or audits on how the contracted service provider is meeting its privacy obligations; and
- reports on the number of privacy breaches and/or complaints received and on its response to these data breaches and/or handling of these complaints.

The contracted service provider's privacy performance and the adequacy of current privacy provisions should be reviewed before extending or renewing a service arrangement.

Obligations after the service arrangement ends

The service arrangement should cover what happens to personal information held by the contractor as part of the service arrangement after it ends. If it is not being destroyed or completely returned to the agency, the service arrangement should include provisions that require the bound contracted service provider to continue to comply with the privacy principles in relation to the personal information it retains.

When bringing a service arrangement to an end, the contracting agency should ensure that personal information held by the contracted service provider is dealt with as required by the service arrangement. The contracting agency should perform an audit or seek a report from the contracted service provider to confirm

[30] Control refers to a situation where a document is not in the agency's physical possession, but the agency has the legal right to determine what happens with the document. For more information refer to *Documents of an agency and Documents of a Minister*

[31] This is important not just for access and amendment applications made under the IP Act, but also for the agency to meet its Public Records Obligations.

all personal information has been securely returned, or disposed of, and is accounted for.

This approach may reduce the risk of personal information being abandoned and then improperly accessed (for example, where data is recovered from a laptop or computer sold at public auction).

Public Records

Records generated or received by the contracted service provider while delivering the function or service under the service arrangement will usually be public records[32] and are the responsibility of the contracting agency.[33] The requirement to retain public records until the expiration of the relevant retention period should be factored in when drafting provisions for the managing records at the completion of the service arrangement.

For example, provisions in the service arrangement may include arrangements for returning documents to the contracting agency (including the format of electronic and other technology-dependent documents), the method by which documents are to be destroyed (where appropriate, under a Retention and Disposal Schedule approved by the State Archivist), and agreed timeframes.

For additional information and assistance please refer to the OIC's guidelines or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

This guide is introductory only and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au.

Published 27 November 2014 and Last Updated 20 September 2019

Changes to legislation after the update date are not included in this document

[32] Under the *Public Records Act 2002* (Qld).
[33] See the Queensland State Archives Public Records Brief: Managing public records during outsourcing, viewable at http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/managing-public-records-during-**outsourcing.**pdf

Appendix A

Contracted Service Provider Checklist

This checklist will assist agencies to determine whether the contract or other arrangement falls into those circumstances.

Is the contract or other agreement a service arrangement for the purposes of the IP Act?

Section 34(2)(b)	Yes	No
Is the contracted service provider providing a service directly to the agency?		
Is the contracted service provider providing a service to someone else on behalf of the agency?		

If you answered **no to both** of these questions, the requirements of chapter 2, part 4 do not apply.

If you answered **yes to either** of these questions, continue to the next question.

Section 34(2)(a)	Yes	No
Is the service for the purposes of performing one or more of the agency's functions?		

If you answered **no** to this question, the requirements of chapter 2, part 4 do not apply.

If you answered **yes**, continue to the next question.

Section 34(2)(c)	Yes	No
Is the contracted service provider acting in the capacity of an employee of the agency (whether temporary, casual, or some other arrangement) in providing the service?		

If you answered **yes** to this question, the requirements of chapter 2, part 4 do not apply.

If you answered **no**, continue to the next question.

Is the contracting agency required to take all reasonable steps to bind the contracted service provider to the privacy principles?

Section 35(3)	Yes	No
Will the contracting agency **provide funding** to the contracted service provider?		
Will the contracted service provider **collect any personal information for** the agency?		
Will the contracted service provider **receive any personal information from** the agency for the purpose of discharging its obligation?		
Will the contracted service provider **be required to give any personal information** it collects to the agency while discharging its obligations?		

If you answered **no to all** of these questions, the agency is not required to take all reasonable steps to bind the contracted service provider to the privacy principles.

If you answered **yes** to any of them, continue to the next question.

Section 35(2)	Yes	No
Will the services being provided under the arrangement involve the contracted service provider dealing[34] with personal information **in any way** for the agency?		
Will the services being provided under the agreement involve the transfer of personal information to the agency?		
Are the services under the agreement being provided to a third party for the agency?		

If you answered **yes to any** of these questions, the agency is required under section 35(1) of the IP Act to take all reasonable steps to bind the contracted service provider to the privacy principles.

[34] Dealing with personal information includes receiving, collecting, storing or processing personal information and includes situations where the service provider is simply holding the information.