

Outsourcing: Agency Obligations under the Privacy Act

The *Privacy Amendment (Private Sector) Act 2000* (the Amendment Act) amends the *Privacy Act 1988* (the Privacy Act) and came into effect on 21 December 2001. The Privacy Act now establishes National Privacy Principles (NPPs) as minimum privacy standards to which some private sector organisations will be subject (Schedule 3). It also contains provisions for organisations to develop privacy codes that can operate in place of the legislative framework (Part IIIAA).

Importantly, the Privacy Act imposes obligations on Commonwealth agencies when entering into contracts to provide services to or on behalf of the agency to apply the information privacy principles (IPPs), some of the NPPs (NPPs 7–10) and the requirements of section 16F of the Privacy Act. Breaches of any of these principles and that section will be an interference with privacy under section 16 of the Privacy Act and complaints may be investigated by the Privacy Commissioner who has power to award damages against the contractor, called in the legislation a *contracted service provider* (CSP) (section 6), and in some situations, to substitute the agency for the CSP (sections 50A and 50B).

ORGANISATIONS SUBJECT TO THE PRIVACY ACT 'Organisation' for the purposes of the Privacy Act is defined in section 6C to mean an individual, body corporate, partnership, unincorporated association or a trust that is not exempt. There are a number of

exemptions. The Privacy Commissioner has described in PCO Information Sheet 12–2001 the different entities as follows:

Individuals

The Privacy Act does not cover the collection, use and disclosure of personal information by an individual unless it is done in the course of running a business. The Privacy Act does not apply to personal information that individuals collect, hold, use or disclose for the purposes of their personal, family or household affairs. The activities of individuals operating a business in their own names may be subject to the Privacy Act unless the business is a small business operator or one of the other exemptions applies.

Bodies corporate

A body corporate is any entity that has a legal personality under Australian law or the law of another country. For example in Australia this would include entities registered as a company under the Corporations Law; incorporated associations; and can include not for profit entities.

Partnerships

Any act done or practice engaged in by one of the partners in a partnership is deemed to be an act or practice of the organisation. Obligations under the Privacy Act are imposed on each partner but may be discharged by any of the partners.

Unincorporated associations

An unincorporated association would include a cooperative. The Privacy Act also covers acts or practices engaged in by an individual when undertaken in the capacity of a member of the

committee of management. Obligations under the Privacy Act are imposed on each member of the committee of management but may be discharged by any of the members of that committee.

Trusts

For the purposes of the Privacy Act, an act done or practice engaged in by a trustee is taken to have been done or engaged in by the trust. The Privacy Act imposes obligations on each trustee but they may be discharged by any of the trustees.

EXEMPT ENTITIES Exempt entities are:

- Commonwealth government agencies including federal government departments, bodies and tribunals set up for a public purpose by federal government laws
- state or territory public sector bodies including government departments, agencies, authorities, universities and local government. However, state or territory bodies that are incorporated companies, societies or associations are deemed to be organisations and subject to the legislation – these bodies may be prescribed out of the coverage of the Privacy Act
- a registered political party which is defined as one that is registered under Part XI of the *Commonwealth Electoral Act 1918*. The acts and practices of political representatives are also not subject to the Privacy Act, and
- small business operators.

(PCO Information Sheet 1–2001)

Small business operators can voluntarily ‘opt in’ to the scheme in the legislation (section 6EA).

EXEMPT ACTS AND PRACTICES Where an organisation is covered by the Act,

certain acts and practices

of the organisation will be exempt (section 7B).

Exempt acts and practices are:

- non business acts and practices

- acts and practices by an employer organisation which relate to a current or former employment relationship or employee records
- if the organisation is a CSP for a Commonwealth contract (whether or not the organisation is a party to the contract), and the organisation would be a small business operator if it were not a CSP, any act done or practice engaged in otherwise than for the purpose of meeting an obligation under a Commonwealth contract, and
- acts and practices of media organisations in the course of journalism (the phrase ‘in the course of journalism’ is not defined).

SMALL BUSINESS Small business operators are exempt. Section 6D defines a small business to be one that has an annual turnover of \$3m or less. However, entities are not small business operators if they:

- provide a health service to another individual and hold health information (except in an employee record)
- disclose personal information about another individual to anyone else for a benefit, service or advantage
- provide a benefit, service or advantage to collect personal information about another individual from anyone else
- are a CSP for a Commonwealth contract (even if they are not a party to the contract)
- are prescribed by regulation not to be a small business
- ‘opt in’ to the legislation.

A small business operator which is also a CSP will be subject to the Privacy Act in respect of the performance of that contract. That is, it cannot benefit from the small business exemption for contractual matters (section 6D(4)(e)).



**CONTRACTED
SERVICE PROVIDERS**

Contracted service provider is defined in section 6 of the Privacy

Act in the following terms:

‘*Contracted service provider*, for a government contract, means:

- (a) an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency or a state or territory authority under the government contract; or
- (b) a subcontractor for the government contract.’

The Privacy Act defines *government contract* as a Commonwealth contract or a state contract. It defines *Commonwealth contract* as a contract to which the Commonwealth or an agency is or was a party, under which services are to be, or were to be, provided to an agency (section 6).

Section 95B of the Privacy Act sets out the requirements for Commonwealth contracts, including prohibiting a breach of the IPPs by the CSP, or where this applies, by a subcontractor.

A *subcontract* is defined very widely to include not only the initial subcontract but any further subcontract as well (section 6). The requirement for inclusion of matters in the Commonwealth contract applies whether the agency is entering into the contract on behalf of the Commonwealth or in its own right (section 95B(5)).

**OBLIGATIONS OF
AGENCIES FOR CSPs**

The Privacy Act requires agencies to take contractual measures to

ensure that CSPs, including subcontractors, do not breach the IPPs (section 95B). It is, generally speaking, the IPPs and not the NPPs which apply to CSPs although NPPs 7 to 10 will also apply. This is because a CSP is an organisation under section 6 and the IPPs displace only NPPs 1 to 6. NPPs 7 to 10 have no equivalent IPPs. The CSP’s privacy obligations are primarily derived from the contract.

Although agencies are only required to include in privacy clauses in their contracts obligations which are consistent with the agency’s own obligations under the Privacy Act, it is a good practice to refer to the CSP’s obligations in respect of NPPs 7–10 and section 16F of the Act. There is no equivalent of these NPPs and 16F in the IPPs. In this way, the CSP has a complete picture of its privacy obligations arising out of the activities which it carries out under the contract.

In the situation where a CSP is not providing services directly to the Commonwealth but to a third party, section 95B of the Privacy Act still applies as the definition of a CSP covers not only the provision of services directly to the agency concerned, but also the provision of services to third parties on behalf of an agency where the provision of those services is in connection with the performance of the functions of the agency (section 6(a)). Where the service to be provided under the contract is not connected with the performance of the functions of the agency, then the provisions of the legislation, including section 95B, do not apply. This will be the situation where an agency such as the Department of Health and Ageing enters into a contract to provide Commonwealth funds under a funding agreement to a body to provide services (for example, the building of a health centre for members of the community). If the provision of those services is not a function of the agency, then the recipient of the funding would not be a CSP for the purposes of the Privacy Act. This is not to say that the agency may not as a matter of good practice include clauses requiring the funding recipients to observe the privacy principles.

**STATE, TERRITORY
AUTHORITIES**

The definition of *organisations* does not include a state or territory authority (sections 6(1) and 6C(3)). As state and territory authorities are not organisations, they cannot be CSPs for the purposes of the Privacy Act. This means that a state or territory authority providing services under a contract with an agency is not

covered by the Privacy Act. Notwithstanding this exclusion, agencies need to be mindful of the obligation under IPP 4(b) to ensure that everything reasonable is done to prevent unauthorised use or disclosure of personal information. For this reason, particularly where that state or territory authority is not subject to state or territory privacy legislation, the agency should as a matter of good practice negotiate the inclusion of privacy clauses having the same effect as if the authority were an organisation under the Act.

SECTION 95B The obligations under section 95B extend to a CSP who is not within Australia. (Section 5B of the Privacy Act gives extra territorial operation to the Act.) The Privacy Commissioner has jurisdiction to investigate a complaint made in relation to services or activities of overseas CSPs (section 5B(4)). Although the effect of this is to allow the Commissioner to take action overseas to investigate complaints and to allow the ancillary provisions of Part 5 of the Act to operate (investigation and determination by Privacy Commissioner), enforcement of the provisions of the contract overseas may be difficult.

The obligation of CSPs under the contract to abide by the IPPs, NPPs 7–10 and section 16F will continue to apply in relation to relevant information after the contract has come to an end. The Privacy Act allows the Privacy Commissioner to investigate complaints about acts or practices of a CSP under a Commonwealth contract after that contract has expired. It is important that the CSP is aware of this and that proper arrangements are made in the contract generally for such things as ongoing storage of information. Where a CSP no longer exists, then it is possible for the Privacy Commissioner to substitute the agency for that CSP when investigating a breach and in determining an award of damages or compensation.

The section 95B obligation is prospective. Section 95B came into effect on 21 December 2001 so the

specific requirement in that section for agencies to include privacy clauses in contracts does not apply to contracts in existence before 21 December (that is, section 95B itself has no retrospective application).

However, Item 37 of the Amendment Act (which is an application provision so will not be found in the consolidated Privacy Act) says:

Under subsection 6A(2) or 6B(2) of the *Privacy Act 1988* (as amended by this Schedule), a Commonwealth contract may prevent an act or practice from being a breach of an NPP or an approved privacy code (as appropriate) regardless of whether the contract was made before or after the commencement of that subsection.

Additionally, the definition of ‘contracted service provider’ in section 6 of the Privacy Act would seem to include pre-21 December 2001 contracts.

There was no legislative requirement prior to 21 December 2001 to make CSPs subject to the Privacy Act and its IPPs. Including privacy clauses in contracts before 21 December 2001 was based on the obligation in IPP 4(b) on an agency.

On that basis, agencies should have been complying with this obligation (and the Privacy Commissioner’s outsourcing guidelines) by including privacy clauses in contracts entered into before 21 December.

The Amendment Act (Item 53, an application provision) provides that an act or practice of an organisation may constitute an interference with the privacy of an individual under section 13A(1)(c) of the Privacy Act whether the contract was made before or after the commencement of section 13A. The effect of this is that although section 95B does not expressly apply to contracts already in existence before 21 December 2001, a CSP under a Commonwealth contract which included privacy obligations can nevertheless be held to be in breach and directly accountable for such a breach.

APPLICATION OF NPPs 7–10 AND 16F

In addition to the eleven IPPs, a CSP is also subject to four NPPs (NPP 7–10)

which do not have any equivalent in the IPPs. NPPs 7–10 are concerned with identifiers, anonymity, transborder data flows and sensitive information.

Sensitive information is defined (section 6) as follows:

- (a) information or an opinion about an individual's:
 - (i) racial or ethnic origin; or
 - (ii) political opinions; or
 - (iii) membership of a political association; or
 - (iv) religious beliefs or affiliations; or
 - (v) philosophical beliefs; or
 - (vi) membership of a professional or trade association; or
 - (vii) membership of a trade union; or
 - (viii) sexual preferences or practices; or
 - (ix) criminal record;that is also personal information; or
- (b) health information about an individual.

NPP 10 prohibits the collection of sensitive information except in certain circumstances.

There is also an obligation under section 16F in relation to direct marketing. A CSP is subject to these NPPs and section 16F even if it is not otherwise subject to the NPPs because, for example, it does not come within the definition of an 'organisation'.

INCONSISTENCIES

An act done or practice engaged in by a CSP

which is for the purposes of meeting directly or indirectly an obligation under the contract will not breach an NPP or an approved privacy code. So in this sense, NPPs can be varied by the contract and a breach of an NPP will not have occurred if the contract obliges the CSP to do something which would be inconsistent with the CSP's obligations under an NPP to which the CSP is bound (section 6A(2)). A similar situation will apply where an approved code is in force displacing the NPPs (section 6B(2)).

The clauses in a Commonwealth contract dealing with privacy will prevail even where they are inconsistent with any of NPPs 7–10 or a code to which the CSP may be subject (sections 6A(2) and 6B(2)). The section is set out in terms of excepting from a breach an act or practice engaged in by an organisation that is a CSP for the purposes of meeting (directly or indirectly) an obligation under the contract. To take advantage of this exception, there must be an *obligation* under the contract for the CSP to do that act or carry out that practice. It is not sufficient if the act or practice is merely authorised or discretionary.

In addition, this exception from breach of the NPPs requires that the act or the practice is authorised by a provision of the contract which is inconsistent with the NPP or approved privacy code. To ensure that both the agency and the CSP are aware of the intended exceptions from the principles or code, it would be useful to identify the particular provisions of the contract which contain such obligations.

Similarly, if the CSP has obligations under the contract which are inconsistent with section 16F (direct marketing), this should also be identified. Where the contract does not oblige the CSP to do direct marketing, the attention of the CSP could be drawn to section 16F by a clause prohibiting the CSP from using information collected under the contract for direct marketing purposes.

An advantage in actually identifying the provisions of the contract which are inconsistent with an NPP or code is that the Privacy Act provides that where a person so requests, a party to a Commonwealth contract must inform the person in writing of the content of any provision in the contract that is inconsistent with an approved code binding a party to the contract or with an NPP (section 95C).

A common situation would be where a CSP is obliged under a contract with a Commonwealth agency to provide the agency with the names and addresses of the individuals to whom it provides the

service or to assign to each individual customer, and report by, an agency identifier (for example, a Centrelink Reference Number).

NPP 7 provides in essence, that a CSP must not adopt as its own identifier of an individual, an identifier that has been assigned by an agency. NPP 8 states that wherever it is lawful and practicable, individuals must have the opportunity of remaining anonymous. Where the obligations under the contract are inconsistent with the obligations under the NPPs then the contract obligations prevail.

NPP 9 is concerned with transborder dataflows and prohibits an organisation from transferring personal information about an individual to someone who is in a foreign country. Some exceptions do apply. The CSP may be obliged to forward information (for example, on communicable diseases) to an international health organisation. That obligation would be inconsistent with NPP 9. The contract obligation would override or vary the NPP.

NPP 10 prohibits the collection of sensitive information about an individual except in quite specific cases. There will be circumstances where a CSP is obliged to collect information which does not come within the exceptions in NPP 10. In such circumstances, the inconsistency between the obligation in the contract and NPP 10 would have the effect that the CSP would not be in breach of the NPP.

OTHER NPPs A CSP may be subject to all the NPPs (or an approved code) in its own right because it falls within the definition of an organisation. Telstra is in such a position (except for its competitive commercial activities). The provisions relating to CSPs do not have any effect in relation to other non-CSP activities of an organisation.

COMPLAINT HANDLING All complaints in relation to the acts or practices of CSPs are to be handled by the Privacy Commissioner who has the power to investigate all complaints even where the CSP is subject to an

approved code that provides for its own complaint handling procedure (section 40A).

The CSPs are liable for their own acts and practices. To ensure that people are able to find out what privacy standards apply, agencies and CSPs are required to release on request details of privacy clauses in their contracts (section 95C).

The outsourcing agency is to be given notice by the Privacy Commissioner of any determination against a CSP (section 53A).

The complaint handling powers under Part 5 of the Privacy Act apply also to complaints about CSPs. The Privacy Commissioner has the same powers in relation to CSPs as the Privacy Commissioner has in relation to agencies, including the power to enter premises to obtain information and to take evidence under oath. Where the Commissioner makes a formal determination under section 52 of the Privacy Act, this may include:

- a declaration that the CSP should redress any loss or damage suffered by the complainant; and
- a declaration that the complainant is entitled to a specific amount by way of compensation for any loss or damage suffered.

The Privacy Commissioner may proceed in the Federal Court or the Federal Magistrates Court to enforce any determination.

In circumstances where an individual is unable to obtain a remedy from a CSP (for example, the CSP dies, ceases to exist or becomes bankrupt) the Commissioner can substitute the agency for the CSP (section 50A). This ensures that the agency remains ultimately responsible for the acts and practices of its CSPs. Before making such a decision, the Commissioner is required to give the agency the opportunity to appear before the Privacy Commissioner and to make oral or written submissions concerning the proposed substitution (section 53B).

MODEL CLAUSE: PROTECTION OF PERSONAL INFORMATION¹

The following model clause is provided to assist Commonwealth agencies in discharging their responsibilities under section 95B of the Privacy Act. Agencies are reminded that changes to these clauses may be necessary to reflect particular situations. If any difficulties are experienced with implementation of the clause please contact AGS.

X.1 This clause applies only where the Consultant deals with personal information when, and for the purpose of, providing [services] under this Contract.

X.2 The Consultant acknowledges that it is a 'contracted service provider' within the meaning of section 6 of the *Privacy Act 1988* (the Privacy Act), and agrees in respect of the provision of [services] under this Contract:

- (a) to use or disclose personal information obtained during the course of providing [services] under this Contract, only for the purposes of this Contract;
- (b) not to do any act or engage in any practice that would breach an Information Privacy Principle (IPP) contained in section 14 of the Privacy Act, which if done or engaged in by an agency, would be a breach of that IPP;
- (c) to carry out and discharge the obligations contained in the IPPs as if it were an agency under that Act;²
- (d) to notify individuals whose personal information the Consultant holds, that complaints about acts or practices of the Consultant may be investigated by the Privacy Commissioner who has power to award compensation against the Consultant in appropriate circumstances;

- (e) not to use or disclose personal information or engage in an act or practice that would breach section 16F (direct marketing), an NPP (particularly NPPs 7 to 10) or an APC, where that section, NPP or APC is applicable to the Consultant, unless:
 - (i) in the case of section 16F – the use or disclosure is necessary, directly or indirectly, to discharge an obligation under [clause ?] of this Contract; or
 - (ii) in the case of an NPP or an APC – where the activity or practice is engaged in for the purpose of discharging, directly or indirectly, an obligation under [clause ?] of this Contract, and the activity or practice which is authorised by [clause ?] of this Contract is inconsistent with the NPP or APC;³
- (f) to disclose in writing to any person who asks, the content of the provisions of this Contract (if any) that are inconsistent with an NPP or an APC binding a party to this Contract;⁴
- (g) to immediately notify the agency if the Consultant becomes aware of a breach or possible breach of any of the obligations contained in, or referred to in, this clause X, whether by the Consultant or any subcontractor;
- (h) to comply with any directions, guidelines, determinations or recommendations referred to in, or relating to the matters, set out in Schedule X,⁵ to the extent that they are not inconsistent with the requirements of this clause; and
- (i) to ensure that any employee of the Consultant who is required to deal with personal information for the purposes of this Contract is made aware of the obligations of the Consultant set out in this clause X.

X.3 The Consultant agrees to ensure that any subcontract entered into for the purpose of fulfilling its obligations under this Contract contains provisions to ensure that the subcontractor has the same awareness and obligations as the Consultant has under this clause, including the requirement in relation to subcontracts.

X.4 The Consultant agrees to indemnify the Commonwealth in respect of any loss, liability or expense suffered or incurred by the Commonwealth which arises directly or indirectly from a breach of any of the obligations of the Consultant under this clause X, or a subcontractor under the subcontract provisions referred to in subclause X.3.

X.5 In this clause X, the terms ‘agency’, ‘approved privacy code’ (APC), ‘Information Privacy Principles’ (IPPs), and ‘National Privacy Principles’ (NPPs) have the same meaning as they have in section 6 of the Privacy Act, and ‘personal information’, which also has the meaning it has in section 6 of the Privacy Act, means:

‘information or an opinion (including information or an opinion forming part of a database), whether true or not and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion’.

X.6 The IPPs and the NPPs are set out in Attachment A and B, respectively. [optional]

X.7 The provisions of this clause X survive termination or expiration of this Contract.

Notes to Model Clause

¹ See ‘Guidelines for Commonwealth Contracts’ Information Sheet No. 14 issued by the Federal Privacy Commissioner and available at www.privacy.gov.au.

2. CSPs may have difficulty in complying with IPPs 6 and 7 where access or amendment should not be allowed. In such circumstances agencies should consider accepting a transfer of the records and handling the matter under FOI.
3. Note that section 6A requires that the Consultant be ‘obliged’ to carry out the activity. Where possible the relevant clause numbers should be noted here.
4. Section 95C Privacy Act.
5. This Schedule should include any specific matters, for example, agency and Privacy Commissioner’s guidelines which the agency wishes the CSP to comply with.

For general information please contact Madeline Campbell of our Canberra office on telephone (02) 6253 7408, e-mail madeline.campbell@ags.gov.au or any of the following lawyers:

Canberra	Anne Caine	(02) 6253 7428
Sydney	Jim Heard	(02) 9581 7477
Melbourne	Libby Haigh	(03) 9242 1499
Brisbane	Maurice Swan	(07) 3360 5702
Perth	Peter Macliver	(08) 9268 1100
Adelaide	Sarah Court	(08) 8205 4231
Hobart	Peter Bowen	(03) 6220 5474
Darwin	Jude Lee	(08) 8943 1405

For enquiries regarding supply of issues of the Briefing, change of address details etc, Tel: (02) 6253 7052 or Fax: (02) 6253 7313 or e-mail: ags@ags.gov.au. A copy of this article will be published in the ‘For Clients’ section of our web site: <http://ags.gov.au>.

Approved Postage PP 233744/00042 ISSN 1322-4611

