A Guide to Privacy for Small Business

***NOTE: updated with minor amendments 27 November 2007.*

This Guide gives a brief introduction to Commonwealth privacy law for those small businesses that need to comply with the *Privacy Act 1988*. The Guide does not describe the law in detail. It is intended to provide useful pointers.

Small businesses may wish to look at other information produced by the Office of the Privacy Commissioner or to seek legal or other advice if they are unsure about what the Privacy Act requires in more complex cases.

The Privacy Act currently protects personal information handled by large businesses and health service providers of any size. The Privacy Act also applies to some small businesses.

Is your small business one with an annual turnover of $3 million or less that is:

- ☐ a health service provider; or
- ☐ trading in personal information (e.g. buying or selling a mailing list); or
- ☐ related to a larger business (a related body corporate);
- ☐ a contractor that provides services under a Commonwealth contract; or
- ☐ a reporting entity for the purpose of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act); or
- ☐ an operator of a residential tenancy database?

If you could answer yes to any of these, your small business may need to comply with the Privacy Act. The terms used above are explained in detail in the Meaning of Terms.

If you are not sure whether your small business needs to comply with the Privacy Act, you should complete our Privacy Checklist for Small Business before you go any further, or get more advice from your lawyer or other adviser.

Contact the Office of the Privacy Commissioner on 1300 363 992 or go to www.privacy.gov.au for a copy of the Privacy Checklist or for more information.

Some information about the Privacy Act

The Privacy Act protects personal information about individuals handled by organisations (including small businesses and not for profit organisations) subject to the Privacy Act. The ten National Privacy Principles (NPPs) in the Privacy Act set the minimum standards for handling personal information.

Small businesses subject to the legislation will need to consider how they are to

implement the provisions. They may choose to be bound by a privacy code approved by the Federal Privacy Commissioner. If they are not bound by a privacy code the NPPs in the legislation will apply to them. More information about Privacy codes can be found in the Meaning of Terms.

Personal information

Personal information is information or an opinion that identifies an individual or allows their identity to be readily worked out from the information. It includes information such as a person's name, address, financial information, marital status or billing details. Some personal information is sensitive information. This includes information about ethnicity, religion and health. Sensitive information is explained further in Meaning of Terms.

NPPs

The NPPs are principles or rules about collecting, using and disclosing personal information.

The NPPs also cover keeping information secure, paying attention to data quality and accuracy, being open about collection and information handling practices, providing anonymity where possible and protection when transferring personal information overseas.

There are some special rules about handling sensitive information including health information.

People have rights under the NPPs to know what information a small business holds about them and to access and correct the information.

A summary of the NPPs can be found on page 10.

Other Exemptions

As well as exemptions for most small businesses the Privacy Act also has exemptions for the media and for political parties.

The Privacy Act does not apply to employment records used for employment purposes in your business.

Information Sheet 12-2001 Coverage of and Exemptions from the Private Sector Provisions, available from the Office website, gives more information about the types of businesses and practices to which the Privacy Act applies.

Privacy Act Enforcement

The Privacy Act gives individuals the right to complain if they think a business, including a small business subject to the Act, has not complied with the NPPs in handling personal information about them.

The Privacy Commissioner can investigate, conciliate and, if necessary make determinations about complaints. The Privacy Commissioner will usually only investigate a complaint if the individual has first tried to resolve it directly with the small business concerned.

Remedies for a privacy complaint might involve an apology, a change in practice or compensation.

For more information go to Information Sheet 13-2001 The Federal Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act available from the Office website www.privacy.gov.au**.**

A Privacy Plan – Getting your small business ready to comply with the Privacy Act

Where do I start?

What you need to do to ensure your small business complies with the Privacy Act may be different from other small businesses. It will depend on the size and the type of business you run and the kind of personal information you collect.

Make a privacy plan

Making a privacy plan is a good place to start. A plan could include the following steps:

1. Make someone responsible for privacy

This could be you, your office manager or someone in another position depending on the size of your business.

2. Become familiar with the NPPs

Get to know and understand the NPPs. The NPPs set out the minimum standards for the way you must handle personal information in your small business.

3. Do a 'privacy stocktake' in your small business

Look at how you handle personal information in your small business, from the time you collect the information to the time you dispose of it. See how your procedures measure up to the obligations in the NPPs.

Once you have a good idea of what happens to the personal information you collect and handle, plan any changes you need to make so that you comply with the NPPs.

Some of these changes may just be minor improvements on the way you already handle personal information. In some cases, for example, where you already hold a stock of printed forms, the plan may be implemented over time.

Remember: if you have AML/CTF obligations you will also have privacy obligations for these activities. Have you worked out what your privacy obligations are in terms of the personal information you are collecting for AML/CTF purposes?

4. Develop or review your complaints handling process

Generally, the more you understand about the way you collect personal information in your small business and the more open you are about the way you collect, use and disclose that information the less likely it is you will get a privacy complaint.

- Have a process in place so that if you do get a complaint about the way you have handled personal information you are prepared.
- Keep a record of any complaints, how you handled them and any changes you made to the way you handle personal information as a result of a complaint.

5. Train your staff

Your staff need to know about privacy too. Often, they may be the first point of contact, dealing with the customers, collecting personal information and answering enquiries. Make your staff aware that the way you handle personal information in your small business may change. Involve staff in the stocktake and review process. Start training.

The next section in the Guide includes information about the NPPs and compliance tips.

The NPPs: some information and compliance tips

In this section we give you some information about what the NPPs require and some tips to help you comply with the NPPs. A summary of the NPPs can be found on page 10. The Guidelines to the National Privacy Principles contain more detailed advice and information about complying with NPPs.

NPPs 1, 8 and 10 — collection of personal information, anonymity and rule for sensitive information

The main obligations of the collection principles are: to collect only necessary information; collect fairly; do what is reasonable to give people notice about the collection (whether collecting from the person or from someone else); allow individuals to be anonymous wherever possible; and get consent to collect sensitive information.

See page 15 for more information on what you need to tell people. You can fill in the details on the table to create your own collection notice.

Compliance Tips

- Know what personal information your small business collects and why. This includes information:
    - collected on forms, informal notes or opinions and images in photos or film; and
    - collected directly from the individual or from someone else.

- Information collected from third parties is not always good quality. As far as possible collect personal information directly from the individual.
- Do not trick individuals into giving you information or collect more information than you actually need. For example, you may need to know an individual's income but you may not need copies of their bank statements.
- Do not collect any information at all if you don't need to.
- From time to time review your collection processes and staff understanding of collection and privacy.

NPP 2 Use and Disclosure of personal information

- Use: what happens to the personal information within a small business.
- Disclosure: the transfer of personal information to a third party outside the small business.

The main obligations of the use and disclosure principle are, generally, only to use or disclose personal information in ways that are related to the reason you collected the information and which individuals would reasonably expect to happen, or with the consent of the individual to the use or disclosure.

You may use or disclose personal information if you think that an unlawful activity has occurred or to protect the health and safety of any person.

Get consent before sending your own direct marketing material. If you can't, give the individual the chance to opt-out when you do send the material and make sure they know how to contact you.

Never use sensitive information for direct marketing.

Compliance Tips

- NO SURPRISES for the individual!
- You can ask an individual for consent to send them direct marketing material when you collect information.
- If individuals do opt-out when you send them direct marketing material, do not contact them again for this purpose.
- Do not disclose personal information to another organisation for them to send unrelated direct marketing without the individual's permission.
- You can disclose information at the individual's request, for example, to an accountant, lawyer or relative. Get clear, consent from the individual, in writing or other method that is robust enough to satisfy you of the person's identity.

NPP 3 Data Quality — making sure personal information is quality information

The main obligation of the data quality principle is to take reasonable steps to check that at the time you collect, use or disclose personal information, it is of sufficient quality — accurate, complete and up-to-date — for the purpose.

Compliance Tips

- Put yourself in the individual's shoes and think about what could happen to the individual if the information is wrong. For example, poor quality information can cause serious or even life-threatening problems. Good quality information on the other hand could increase customer confidence in your business.
- Look at what you can do in your small business to check and update personal information at the time you are collecting, using and disclosing information.
- Wherever possible, collecting the information directly from the individual is best. It's a good quality check!

NPP 4 Security — looking after personal information you collect

The main obligations of the security principle are to keep personal information safe when it is in use and to dispose of it securely when you are finished with it. You are probably already doing this.

Compliance tips

- Have secure computer passwords and lockable filing cabinets.
- Check an individual's identity when they ask for access to the personal information you hold about them.
- Keep personal information away from those who do not need to see it - staff as well as customers.
- Destroy information securely. Do not dump it in a street bin.
- Raise security awareness with your staff. Review procedures from time to time.

Information Sheet 6-2001 Security and Personal Information has more tips for security compliance and is available from the Office website.

NPP 5 Openness — giving information about the way you handle personal information

The main obligation of the openness principle is to have ready, in a document, some information about the way you handle personal information in your small

business and to give more details if you are asked.

A privacy policy in a document

The following information about your small business in a document would be a good start:

- your small business is bound by the NPPs or a privacy code; or
- any exemptions under the Privacy Act that apply to the personal information your small business handles; and
- that an individual can get more information about how your small business manages the personal information if they ask.

Compliance Tips

- The privacy policy in a document could be a flyer that you can give to someone, or a sign on the wall or a counter. Just make sure it's there and easily seen, read or referred to, if you are asked.
- If you operate online put a privacy policy on your website.

Giving more information about personal information management

You could be asked, for example, for more details about security, or services you may contract out or how to get access to information. It will depend on what the individual wants to know.

Compliance Tips

- You can give this information verbally or in writing.
- It's alright to say you don't know if someone asks you a tricky question about the way you handle personal information but you will need to find out about it and tell them.

Information Sheet 3-2001 Openness also has more information about openness, available at the Office website www.privacy.gov.au.

NPP 6 Access and correction — inspecting personal information and making corrections

The main obligations of this principle are to: give individuals access to all the personal information you hold about them unless an exception applies; take steps to correct the information if it is wrong or give the individual reasons why you can't; if an individual asks, attach a statement saying they disagree with the information.

Don't overcharge individuals when giving access and don't charge for making a request for access.

Compliance Tips

- Make sure you are using the health and safety, legal obligation or business needs exceptions correctly before you say no to a request for access.
- Check the identity of the individual asking for access to the personal information you hold about them.
- The principle doesn't prevent you making notes in your customer record, just be aware that your customer can have access to ALL the information you hold about them, even those 'off-the-cuff' notes about difficult customers.
- Access can be given in different ways, including photocopies, letting the person take notes and printouts or e-mails of electronic information.
- Correct poor quality information as soon as possible.

Information Sheet 4-2001 Access and Correction has more information about what may affect access, ways of giving access and how to respond if someone asks for access.

Information Sheet 5-2001 Access and the Use of Intermediaries gives more information about using another person to give access.

Both these information sheets can be found at the Office website www.privacy.gov.au.

NPP 7 Identifiers — limits the way Commonwealth identifiers can be handled

The main obligations in this principle are to only adopt, use or disclose a Commonwealth identifier such as a Medicare, Veteran's Affairs or passport number in limited circumstances. There may be some special health, safety, legal or law enforcement reasons which allow you to use or disclose Commonwealth identifiers.

An individual's name or ABN number is not an identifier.

Compliance Tips

- The NPPs do not stop you looking at documents that include Commonwealth identifiers such as passports, Centrelink or Medicare cards to establish the identity of a person, but you cannot use or disclose the number unless the special reasons apply.

NPP 9 Transborder Dataflows — sending personal information overseas

The main obligation in this principle is to make sure that personal information transferred overseas is protected, as far as possible, in the way it is protected in

Australia.

Compliance tips

- If you are not sure that the country to which you are sending the personal information has similar privacy protection to Australia you may want to get legal advice.

- If in doubt, get consent to the transfer of personal information overseas at the time you collect information.

A Summary of the National Privacy Principles

See below for a summary of the NPPs. This is a summary only of the ten NPPs and not a full text of the obligations. A full statement of the NPPs is available on our website or by contacting our Office.

NPP 8 Anonymity

- If it is lawful and practicable to do so, give people the option of interacting anonymously with you.

NPP1 Collection

- Only collect personal information that is necessary for your functions or activities.
- Use fair and lawful ways to collect personal information.
- Collect personal information directly from an individual if it is reasonable and practicable to do so.
- At the time you collect personal information or as soon as practicable afterwards, take reasonable steps to make an individual aware of:
    - why you are collecting information about them;
    - who else you might give it to; and
    - other specified matters.
- Take reasonable steps to ensure the individual is aware of this information even if you have collected it from someone else.

NPP 10 Sensitive information

- Get consent to collect sensitive information unless specified exemptions apply.

NPP 2 Use and Disclosure

- Only use or disclose personal information for the primary purpose of collection unless one of the exceptions in NPP 2.1 applies (for example, for a related secondary purpose within the individual's reasonable expectations, you have consent or there are specified law enforcement or public health and public safety circumstances).

Note that: If the information is sensitive the uses or disclosures allowed are more limited. A secondary purpose within reasonable expectations must be directly related to the purpose of collecting the information and the direct

marketing provisions of NPP 2.1(c) do not apply.

NPP 3 Quality

- Take reasonable steps to ensure the personal information you collect, use or disclose is accurate, complete and up-to-date. This may require you to correct the information.

NPP 4 Security

- Take reasonable steps to protect the personal information you hold from misuse and loss and from unauthorised access, modification or disclosure.

- Take reasonable steps to destroy or permanently de-identify personal information if you no longer need it for any purpose for which you may use or disclose the information.

NPP 5 Openness

- Have a short document that sets out clearly expressed policies on the way you manage personal information and make it available to anyone who asks for it.
- If an individual asks, take reasonable steps to let them know, generally, what sort of personal information you hold, what purposes you hold it for and how you collect, use and disclose that information.

NPP 6 Access

- If an individual asks, you must give access to the personal information you hold about them unless particular circumstances apply that allow you to limit the extent to which you give access – these include emergency situations, specified business imperatives and law enforcement or other public interests.

NPP 7 Identifiers

- Only adopt, use or disclose a Commonwealth Government identifier if particular circumstances apply that would allow you to do so.

NPP 9 Transfer overseas

- Only transfer personal information overseas if you have checked that you meet the requirements of NPP 9.

Meaning of Terms

access - This involves a small business giving an individual information about themselves held by the small business. Giving access may include allowing an individual to inspect personal information or giving a copy of it to them.

benefit, service or advantage - This includes income, financial concessions, subsidies or some other return to the small business. For example, where a small business sells its customer list to a marketing company or gives its own list in return for another list.

collection - A small business collects personal information if it gathers, acquires or obtains personal information from any source and by any means. Collection includes when a small business keeps personal information it has come across by accident or has not asked for.

Commonwealth contracted service provider - This means small businesses that provide services to Commonwealth agencies under contract or subcontract. The Privacy Act does not apply to contracts small businesses may have with State or territory governments.

consent - People must understand what they are agreeing to and agree voluntarily. The consent is not valid or acceptable if there is extreme pressure or coercion, for example, where consent is given under threat.

consent can be express or implied

Express consent is given explicitly: verbally or in writing.

Implied consent: consent may reasonably be understood in the circumstances from the conduct of the person and the small business.

contractors - Under the Privacy Act, acts and practices of employees (and those 'in the service of' a small business) in performing their duties of employment are treated as those of the small business (see section 8(1)(a)).

This does not usually apply to contractors performing services for a small business unless there is a particularly close relationship between a small business and a contractor. In that case, the actions of the contractor could be treated as having been done by the small business for the purposes of section 8 of the Privacy Act.

If the small business and the contractor are regarded as separate entities under the Privacy Act, a small business that gives personal information to a contractor is disclosing information and the contractor is collecting the information. This means that for a small business to comply with the NPPs it may need to have clauses in the contract to protect the personal information the small business discloses to the contractor.

Where the contractor is not a 'small business' under the Privacy Act and is not covered by the NPPs it would be advisable for the small business to take steps to protect the personal information it discloses to the contractor.

For more information about how the NPPs apply where a small business contracts out a function or activity to a separate entity see Information Sheet 8-2001 Contractors.

disclosure - In general terms a small business discloses personal information when it releases it to others outside the small business. It does not include giving individuals information about themselves (this is 'access' see above).

health service provider - Health includes physical, emotional, psychological and mental health. Health service providers: assess, record, maintain or improve a person's health; diagnose or treat a person's illness or disability; or dispense on prescription a drug or medicinal preparation by a pharmacist.

personal information - The Privacy Act says personal information means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This includes information or an opinion forming part of a database.

The information may or may not be true. (section 6)

privacy codes - The NPPs are the default rules which organisations and businesses must comply with. Some organisations and businesses may choose to develop their own Privacy Codes which replace the NPPs. Privacy Codes must meet strict standards in the Privacy Act and be approved by the Privacy Commissioner.

Information Sheet 11-2001 Privacy Codes and the Register gives more information which can be found on our website www.privacy.gov.au**.**

related body corporate (Section 50, Corporations Act 2001) - The Privacy Act defines related body corporate by reference to the Corporations Act. Companies might be related where they are a holding company or a subsidiary of another body corporate.

residential tenancy database - The Privacy (Private Sector) Amendment Regulations 2007 (No.3) states that a residential tenancy database means a database:

a) that stores personal information in relation to an individual's occupation of residential premises as a tenant; and
b) that can be accessed by a person other than the operator of the database or a person acting for the operator.

sensitive information - Special rules apply to the handling of sensitive information. Sensitive information is a subset of personal information. It is information or opinion about a person and includes:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices;
- criminal record or health information about an individual;
- genetic information that is not health information.

trading in personal information - Trading in personal information happens where businesses collect or disclose an individual's personal information for a "benefit, service or advantage"(see above), for example they buy or sell a list of personal information for income, concessions or some other return. The Act does not prevent trading in personal information but does set principles that need to be followed.

The Privacy Act will not apply where the trading happens with the consent of the individual concerned or is authorised or required by law.

Note: In some circumstances sale of the assets of a business that include personal information will also be trading in personal information.

use - In general terms, use of personal information refers to the handling of personal information within a small business including 'the inclusion of information in a publication'.

Resources and Help

Contact details for the Office of the Privacy Commissioner

www.privacy.gov.au

Enquiries Line 1300 363 992 (local call charge)

GPO Box 5218, SYDNEY NSW 2001

Useful information available from the Office includes:

- Website page for Small Business
- A brief overview of The Privacy Act and Small Business – a Snapshot
- Privacy Checklist for Small Business
- Health Information and The *Privacy Act 1988*. A Short Guide for the private health sector
- Guidelines to the National Privacy Principles and Information Sheets 1-15
- The National Privacy Principles
- The Privacy Act
- Frequently asked questions (FAQs)

NPP 1.3 and NPP 1.5 – notice when collecting personal information

NPPs 1.3 and 1.5 require you to give people some information when collecting personal information from them, or about them from some one else. They allow you to consider what is reasonable when providing this information. For example, the information can be given later if it cannot be given at the time. Other factors in deciding what is reasonable include whether people already know this information, if it is obvious, cost and sensitivity of the personal information. The table below sets out: the things you need to tell people; some compliance tips and examples; and room for you to fill in the information for your own business. When complete this will be a collection statement for your business.

What the NPPs say	Some Compliance tips	Examples	Your small busines
the identity of the business and how to contact it	On a form, you might put more contact information then you would supply, for example, if you were collecting over the phone, when organisation name and phone number might be enough.	Solar Adventure Travel 26 Smith Road Smithville 2000 Ph: 62 62 62 62, Fax: 62 71 71 71 ABN: 33 555 666 777	
that he or she is able to get access to the information	This information could be given to individuals when you first deal with them. Another way to provide this detail would be to include it in your privacy policy.	You can access and correct the personal information we hold about you. Contact us via our e-mail solaradventure@seeker.com.au or by phone or mail. See our contact details.	
the purposes for which the information is collected	This can be a general statement, but it must be enough for the person to know what you are going to do with the information.	We use the personal information you give us to process your travel bookings and send you up-to-date information about exciting new travel or adventure opportunities.	
to whom this information is usually passed	A general description of to whom you usually give or sell information, for example, debt collectors or related body corporates. If you only pass information to a few businesses you could list them by name.	We disclose information to other organisations only to help meet your travel needs. These include operators of airlines, road or rail transport organisations and tours.	
any law that requires the particular information to be collected	This may not apply often. A general description of the law will generally be enough.	We need to collect this information to comply with taxation law.	
the main consequences (if any) for the individual if all or part of the information is not	Tell the person what could happen if they do not give you the information your small business needs to provide the service. For example, 'If you don't tell us this information we won't be able to enter you in the competition.'	If you do not provide all the information requested, we might not be able to provide some aspects of the travel service you require.	

What the NPPs say	Some Compliance tips	Examples	Your small busines
provided.			