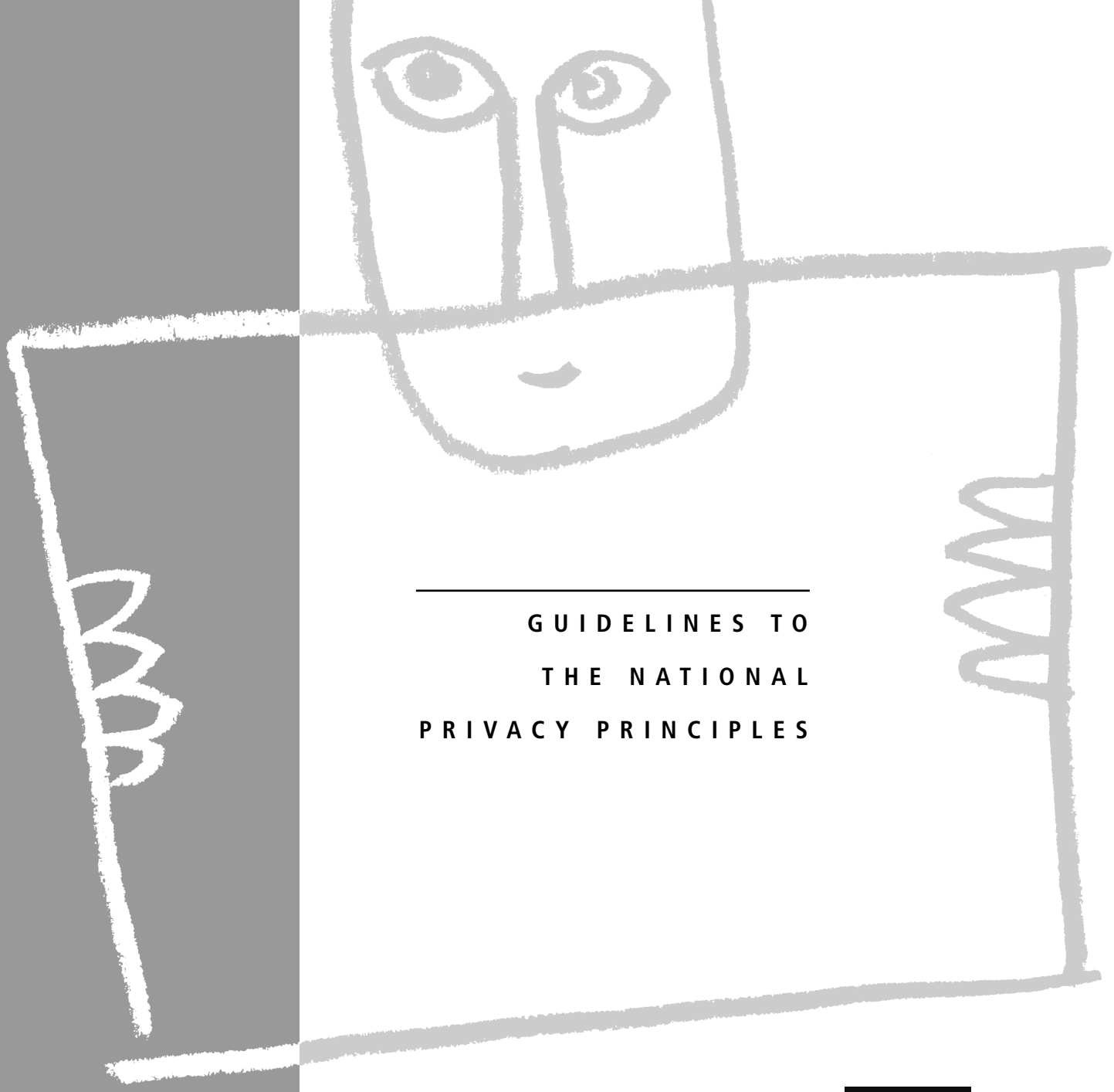

GUIDELINES TO THE NATIONAL PRIVACY PRINCIPLES

OFFICE OF THE
FEDERAL
PRIVACY
COMMISSIONER

SEPTEMBER 2001

ISBN 1-877079-04-9

Director
Promotion and Education
Office of the Federal Privacy Commissioner
GPO Box 5218
Sydney NSW 1042

Table of Contents

Introduction **1**
Background 1
Application of the *Privacy Act 1988* 2
Help with compliance 4

Summary of NPP Obligations **7**

National Privacy Principles **8**

Key Concepts **21**

Guidelines to the National Privacy Principles 26

NPP 1 and NPP 10 – Collection 27
NPP 1.1 Collection must be necessary 27
NPP 1.2 Collection must be fair and lawful 27
NPP 1.3 Informing individuals when collecting directly 28
NPP 1.4 Collecting directly from the individual 31
NPP 1.5 Collecting from third parties 32
NPP 10 Collecting sensitive information 33

NPP 2 – Use and disclosure 35
NPP 2.1(a) Primary and related purposes 35
NPP 2.1(b) Secondary use and disclosure with consent 37
NPP 2.1(c) Direct marketing 38
NPP 2.1(d) Research and statistics relevant to public health or safety 39
NPP 2.1(e) Serious threats to life, health or safety 40
NPP 2.1(f) Unlawful activity 40
NPP 2.1(g) Required or authorised by law 41
NPP 2.1(h) Enforcement bodies 41
NPP 2.3 Primary purpose and related companies 41
NPP 2.4–2.6 Disclosing health information to a responsible person 42

NPP 3 – Data quality 43
NPP 3 Accurate, complete and up-to-date 43

NPP 4 – Data security 44
NPP 4.1 Protecting personal information 44
NPP 4.2 Destroying or de-identifying personal information 45

NPP 5 – Openness 47
NPP 5.1 A policy in a document 47
NPP 5.2 Giving more information about personal information management 48

NPP 6 – Access and correction 49
NPP 6.1 Access to personal information 49
NPP 6.2 Commercially sensitive decision-making processes 52
NPP 6.3 Access through an intermediary 53
NPP 6.4 Charging for access 53
NPP 6.5 Correcting personal information 53
NPP 6.6 Disputed accuracy 53
NPP 6.7 Giving reasons for denying access 54

NPP 7 – Identifiers 55
NPP 7.1 Adoption of identifiers 55
NPP 7.2 Use and disclosure of identifiers 55

NPP 8 – Anonymity 57
NPP 8 Dealing with people anonymously 57

NPP 9 – Transborder data flows 58
NPP 9 Sending personal information overseas 58

TIP

This symbol appears in the margin next to tips for compliance.

Introduction

Background

New privacy provisions

New privacy provisions in the *Privacy Act 1988* (Cth) (the Privacy Act) affecting private sector organisations came into effect on 21 December 2001. Organisations covered by 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 (Commissioner). If they are not bound by a privacy code the National Privacy Principles (NPPs) in the legislation will apply to them. The NPPs aim to ensure that organisations that hold information about people handle that information responsibly. They also give people some control over the way information about them is handled.

The NPPs are drafted in a way that is technology neutral. The result is that the NPPs apply equally to conventional, electronic and digital environments. This neutrality also aims to ensure that the legislation will not date and will work in practice now and for many years to come.

International trend of new provisions

The NPPs in the new private sector provisions and the Information Privacy Principles (IPPs) covering federal public sector agencies in the Privacy Act, reflect the ideas that have been developed internationally and, in particular, the Organisation for Economic Cooperation and Development's (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980)*. A growing number of other countries, including New Zealand, Hong Kong, Canada and many European nations, have also adopted privacy laws.

National consistency

The new private sector provisions, including the NPPs, aim as far as possible to establish a nationally consistent approach to handling of personal information in the private sector that is to be applied across jurisdictions and across industries.

The information economy

The importance of responsible information practices has been increasing over recent years. The information economy, and the technology that underpins it, has developed rapidly. This has made it cheaper and easier than ever before to collect, store, analyse, compare and share personal information. The information economy presents Australia with great opportunities. There is no doubt that our future prosperity depends on effective use of information; but there are also risks. Research shows that people are often uncertain about what will be done with information about them and this can make them reluctant to take up the opportunities offered by new technology.

Application of the Privacy Act

Coverage of the Act

The new privacy provisions will apply to businesses (including non-profit organisations) with an annual turnover of more than $3 million and health service providers.

Businesses with an annual turnover of $3 million or less are exempt from the new laws unless one of the following statements is true for the business:

- it is related to another business (for example its holding company or a subsidiary) that has an annual turnover of more than $3 million;
- it provides a health service and holds health records;
- it discloses personal information for a benefit service or advantage;
- it provides someone else with a benefit, service or advantage to collect personal information;
- it is a contracted service provider for a Commonwealth contract.

If any of these circumstances apply to a business with an annual turnover of $3 million or less, it is covered by the new privacy legislation from 21 December 2002, unless it provides a health service in which case it must comply from 21 December 2001.

The Privacy Act also provides for exemptions from coverage in the following circumstances:

- the journalism activities of media organisations; and
- an act done or practice engaged in, by an organisation that is or was an employer of an individual, if the act or practice is directly related to:
    - (a) a current or former employment relationship between the employer and the individual; and
    - (b) an employee record held by the organisation and relating to the individual.

For more information about the exemptions under the Privacy Act see *Information Sheet 12 – 2001 Coverage of and Exemptions from the Private Sector Provisions*. This is available at www.privacy.gov.au on the Office's web site.

For information about how the NPPs apply to information an organisation has already collected on the date the private sector scheme commences, see *Information Sheet 10 – 2001 Application of the Privacy Act to Information Already Held* which is also available from the Office's web site.

The Privacy Act already regulates credit providers and credit reporting agencies in the way they handle consumer credit information. Provisions in the Privacy Act also regulate private sector organisations in possession or control of tax file number information. These requirements will continue to apply in addition to the new provisions.

Result of an interference with privacy

If an individual thinks an organisation has interfered with his or her privacy they can complain to the Commissioner. When the Commissioner receives a complaint the individual must in most cases be referred back to the organisation to give the organisation a chance to resolve the complaint directly (see section 40(1A)).

If the individual and the organisation cannot resolve the complaint between themselves, the Office conciliates the complaint using letters and phone calls, or in some cases, face-to-face meetings. In the majority of cases, the complaint is resolved this way. As a last resort, the Commissioner can make a formal determination. If an organisation does not comply with the determination either the Commissioner or the complainant can seek to have it enforced by the Federal Court. The Commissioner may also investigate an act or practice that may be a breach of privacy even if there is no complaint (section 40(2)).

If an organisation has decided to be bound by a privacy code that has its own complaint handling procedures the individual would complain to the privacy code adjudicator. A privacy code adjudicator or the complainant can seek to have a determination enforced by the Federal Court. The Commissioner has the power to review a complaint heard by a privacy code adjudicator.

Help with compliance

This booklet

This booklet gives organisations a quick guide to helpful information about the NPPs. It is set out in the following sections:

- The first section of this booklet is a summary of obligations under the NPPs. The summary aims to give organisations a general idea of their obligations. However, to get a complete picture of their obligations, organisations will need to read the NPPs themselves.
- The second section sets out the NPPs as they appear in Schedule 3 of the Privacy Act.
- The third section has some key concepts.
- The final section has guidelines that the Commissioner has developed under section 27(1)(e) to help organisations to comply with the NPPs and to avoid interfering with an individual's privacy. The guidelines indicate some factors the Commissioner may take into account when handling a complaint. The guidelines are advisory only and not legally binding.

Information sheets

For organisations that want more detailed explanations, good practice or compliance tips, the following information sheets are available:

- Overview of the Private Sector Provisions;
- Preparing for December 2001;
- Openness;
- Access and Correction;
- Access and the Use of Intermediaries;
- Security and Personal Information;
- Unlawful Activity and Law Enforcement;
- Contractors;
- Handling Health Information for Research and Management;
- Application of the Privacy Act to Information Already Held;
- Privacy Codes; and
- Coverage of and Exemptions from the Private Sector Provisions.

The guidelines have cross-references to relevant information sheets. These are available at www.privacy.gov.au on the Office's web site.

Other guidelines

The Office has also developed other guidelines. These include *Code Development Guidelines* for organisations considering developing a privacy code, and *Guidelines on Privacy in the Private Health Sector* for health service providers. These are available at www.privacy.gov.au on the Office's web site.

Other information

These guidelines and the information sheets are also available in Word, PDF and html versions at www.privacy.gov.au on the Office's web site. There is also a whole range of other information about the new private sector scheme at this site. The Office has a toll free hotline at 1300 363 992.

Summary of NPP obligations*

- ❑ If it is lawful and practicable to do so, give people the option of interacting anonymously with you.
- ❑ 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.
- ❑ Get consent to collect sensitive information unless specified exemptions apply.
- ❑ 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.
- ❑ 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 and the direct marketing provisions of NPP 2.1(c) do not apply.
- ❑ 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.
- ❑ 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.
- ❑ 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.
- ❑ 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.
- ❑ Only adopt, use or disclose a Commonwealth Government identifier if particular circumstances apply that would allow you to do so.
- ❑ Only transfer personal information overseas if you have checked that you meet the requirements of NPP 9.

*This is a summary only and NOT a full statement of obligations. These are set out in the NPPs themselves.

NATIONAL PRIVACY PRINCIPLES

Privacy Act Schedule 3 – National Privacy Principles

1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the **secondary purpose**) other than the primary purpose of collection unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if

the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure – the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or
(ii) a serious threat to public health or public safety; or

(f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or

punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the carer) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is ***responsible*** for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a stepchild and a foster child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3 Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4 Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6 Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information – providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) in the case of health information – providing access would pose a serious threat to the life or health of any individual; or

(c) providing access would have an unreasonable impact upon the privacy of other individuals; or

(d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;
by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to

the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or
(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2).

7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999)* is not an ***identifier***.

8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10 Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) if the information is collected in the course of the activities of a non-profit organisation – the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

KEY CONCEPTS

Key concepts

This only includes some of the concepts and terms in the NPPs. If you cannot find a term here you should find it in section 6 of the Privacy Act which is linked at www.privacy.gov.au on the Office's web site. Where terms are defined in the Privacy Act, the relevant section is indicated.

Access

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

Children and young people

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. Determining the decision-making capabilities of a young person can be a complex matter, often raising other ethical and legal issues. Organisations will need to address each case individually.

As a general principle, a young person is able to give consent when he or she has sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person; for example if the child is very young or lacks the maturity or understanding to do so themselves. It should be noted that in some States, contracts with people under the age of 18 are not valid.

It may be desirable for organisations that target children or young people to specifically address issues of consent and rights of access to the personal information of children and young people in the information policy that NPP 5 requires them to have. Such a policy might contain general guidelines about how the organisation will make decisions relating to young people and children and the factors it will take into account. The policy might also deal with parental involvement, particularly factors that would indicate that a parent should be involved in the decision-making process.

KEY CONCEPTS

Collection

An organisation collects personal information if it gathers, acquires or obtains personal information from any source and by any means. Collection includes when an organisation keeps personal information it has come across by accident or has not asked for.

Consent

Consent means voluntary agreement to some act, practice or purpose. It has two elements: knowledge of the matter agreed to, and voluntary agreement. Consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation. Consent is invalid if there is extreme pressure or coercion.

Only a competent individual can give consent although an organisation can ordinarily assume capacity unless there is something to alert it otherwise. Competence means that individuals are capable of understanding issues, forming views based on reasoned judgments and communicating their decisions. The general law about competence and incapacity will apply to the issue of consent.

Contractors

The Privacy Act treats the acts and practices of employees (and those 'in the service of' an organisation) in performing their duties of employment as those of the organisation (see section 8(1)(a)). Contractors performing services for an organisation are not considered to fall within this provision. However, where there is a particularly close relationship between an organisation and a contractor it may mean that the actions of the contractor could be treated as having been done by the organisation for the purposes of section 8 of the Privacy Act.

When the parties to a contract are regarded as separate entities under the Privacy Act an organisation that gives personal information to a contractor is disclosing information and the contractor is collecting the information. In practical terms, this means that the organisation may need to have clauses in the

contract for the protection of personal information the organisation discloses to the contractor in order to meet its obligations under the NPPs.

Where the contractor is not an 'organisation' for the purposes of the Privacy Act and so not covered by the NPPs it would be advisable for the organisastion to take measures to protect the personal information it discloses to the contractor.

What are reasonable steps under NPP 1.3 and NPP 1.5 for the organisation and a contractor may depend on the nature of the relationship between the organisation and the contractor, including the contractual provisions in place.

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

Disclosure

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

Enforcement body

Enforcement bodies are listed in the definitions in section 6(1) of the Privacy Act. They are also listed in *Information Sheet 7 - 2001 Unlawful Activity and Law Enforcement*.

Organisation

The NPPs apply to businesses and bodies that fall within the definition of 'organisation' in section 6C of the Privacy Act. Section 6C says that 'organisation' means: an individual; or a body corporate; or a partnership; or any other unincorporated association; or a trust; that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

KEY CONCEPTS

Personal information

Personal information is 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 (section 6). It includes all personal information regardless of its source.

Personal information relates to a natural living person. A natural person is a human being rather than, for example, a company, which may in some circumstances be recognised as a legal 'person' under the law.

The NPPs apply to the collection of personal information by an organisation for inclusion in a record or a generally available publication, but apart from this, the NPPs only apply to personal information an organisation has collected that it holds in a record.

Related body corporate

A related body corporate is defined in section 50 of the *Corporations Act 2001* (Cth) to mean that where a body corporate is:

- a holding of another body corporate;
- a subsidiary of another body corporate; or
- a subsidiary of a holding company of another body corporate;

the first mentioned body and the other body are related to each other.

Sensitive information

Sensitive information is a subset of personal information. It means information or opinion about an individual's 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 (section 6).

Use

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

GUIDELINES TO THE NATIONAL PRIVACY PRINCIPLES

Guidelines to the National Privacy Principles

These guidelines are to be read together with the NPPs.

These Guidelines to the National Privacy Principles are issued under section 27(1)(e) of the Privacy Act. The guidelines are advisory only and are not legally binding. (The NPPs in Schedule 3 of the Privacy Act and also set out in this booklet do legally bind an organisation).

The guidelines are based on the Office's understanding of how the Privacy Act works. They provide explanations of some of the terms used in the NPPs and are intended to help organisations apply the NPPs in ordinary circumstances. Organisations may need to seek separate legal advice on the application of the Privacy Act to their particular situation. The guidelines indicate some factors the Commissioner may take into account when handling a complaint. Complying with the guidelines will help minimise the risk of breaching the Privacy Act, but will not guarantee it.

Nothing in the guidelines limits the Commissioner's freedom to investigate complaints or to apply the NPPs in the way that seems most appropriate to the facts of the case being dealt with.

GUIDELINES TO NPP 1 AND NPP 10 – COLLECTION

NPP 1 and NPP 10 – Collection

NPP 1.1 Collection must be necessary

NPP 1.1 aims to limit the information that an organisation collects to that which is necessary for its functions and activities.

The Commissioner interprets 'necessary' in a practical sense. If an organisation cannot in practice effectively pursue a legitimate function or activity without collecting personal information, then the Commissioner would ordinarily consider it necessary for that function or activity. It would not ordinarily be acceptable for an organisation to collect personal information on the off chance that it may become necessary for one of its functions or activities in the future.

TIP

Tips for compliance

Identify what personal information your organisation collects (or proposes to collect) and for which of its functions and activities the information is necessary. You may find that de-identified information would do just as well in some cases or that it would be lawful and practicable for individuals to interact with your organisation anonymously.

NPP 1.2 Collection must be fair and lawful

In general, the Commissioner interprets 'fair' to mean without intimidation or deception. This would usually require an organisation not to collect personal information covertly but there will be some circumstances – for example, investigation of possible fraud or other unlawful activity, where covert collection of personal information by surveillance or other means would be fair.

TIP

Tips for compliance

Look at the ways your organisation collects personal information. Check that people are aware that your organisation is collecting it. If they are not, your organisation is encouraged to ensure that all members of your staff are educated in responsible information handling practices; or you may decide not to collect the personal information at all.

NPP 1.3 Informing individuals when collecting directly

Practicability and timing of giving NPP 1.3 information

Deciding whether giving NPP 1.3 information at or before the time of collection is not 'practicable' depends on the circumstances and requires balancing a number of possible factors. An organisation could put off giving NPP 1.3 information until after the time of collection if there are practical problems in doing so that the organisation cannot overcome by any reasonable means.

TIP

Tips for compliance

In assessing whether it is impracticable to give NPP 1.3 information at or before the time of collection, an organisation could consider a number of factors including:

- the time at which it is possible to make the individual aware of NPP 1.3 matters;
- the sensitivity of the personal information involved;
- the privacy implications for the individual of not receiving the information at or before the time of collection;
- what is accepted industry practice (by consumers and industry);
- the cost to the organisation of giving the information at or before the time of collection; and
- the benefits or otherwise to the individual of receiving the information at or before the time of collection.

Reasonable steps

Where the circumstances of collection make a matter listed in NPP 1.3 obvious, the 'reasonable step' might not involve any active measures because the circumstances speak for themselves. For example, in many cases the identity of the organisation collecting the personal information could be obvious from the circumstances. It may be less obvious on the Internet and when other electronic technologies are used.

In some circumstances where an organisation has already recently informed an

individual of NPP 1.3 matters about a particular kind of collection it may not be necessary to inform them of the same information about a collection of the same kind a few days later. The main point is that the individual needs to be made aware of these matters: the NPPs do not require an organisation to give an individual the same information each time they have contact with the individual in relation to the same matter. However, if there were some change in the circumstances relevant to NPP 1.3 since the organisation was last in contact, it would need to take reasonable steps to make an individual aware of it.

Deciding what are reasonable steps involves balancing a number of possible factors, including the importance to the individual of having the relevant knowledge and the cost to the organisation in providing that information.

Related corporations and reasonable steps

In the case of related companies, the organisation in the group that originally collects information from an individual must take reasonable steps under NPP 1.3(d) to tell the individual at the time of collection that it intends to disclose information about them to related companies.

NPP 1.3(a) and (b)

These require an organisation collecting personal information directly from an individual to take reasonable steps to ensure that the individual is aware of the collecting organisation's identity and the fact that the individual is able to get access to the information.

TIP

Tips for compliance

Where an organisation collects personal information on a form it could satisfy its obligations under NPP 1.3 by a statement on the form. In the case of a form on a web site, the information could be on the same page as the form or prominently linked to it; for example, it could come up before the individual completes the transaction.

Where an organisation collects personal information over the counter, it could prominently display a brief notice covering all the relevant information and give the individual more detailed information in a leaflet it hands over at the time.

If an organisation collects personal information using a cookie, web bug or other means, it could give the NPP 1.3 information in a statement clearly available on the web site; for example, it could be linked directly from the homepage and other pages that make use of the devices.

Where an organisation collects personal information over the phone, it may be possible to use automated messages to provide information about NPP 1.3 matters. In other cases, it may not be practicable to cover all the NPP 1.3 matters at the time of collection. In such cases, the organisation could give the individual information about these matters as soon as possible, for example, in any confirmatory documents.

NPP 1.3(c) Informing individuals about the purposes of collection

An organisation could keep the description of the purposes reasonably general as long as the description is adequate to ensure that the individual is aware of what the organisation is going to do with information about them. The organisation does not have to describe internal purposes that form part of normal business practices, such as auditing, business planning or billing.

TIP

Tips for compliance

Given the importance of primary purpose in assessing appropriate use or disclosure, this would be a good opportunity for an organisation to outline its view of the primary purpose of collection.

NPP 1.3(d) Informing individuals about usual disclosures

'Reasonable steps' to inform an individual about the disclosures an organisation usually makes would ordinarily mean either giving general descriptions of sets of people and organisations (for example, 'State Government licensing authorities', 'health insurers' and 'list renters') or to list each member of the set.

An organisation does not need to mention disclosures that the NPPs permit, but in practice happen only rarely. For example, it does not need to mention disclosures under warrant or to intelligence agencies.

NPP 1.3(e) Informing individuals of any legal obligation to collect

This means an organisation must take reasonable steps to tell the individual about any law that requires the individual to provide, or the organisation to collect, personal information in the particular situation. In describing the law the organisation need not specify the exact piece of legislation (although it would be desirable to do this where possible). A statement like 'taxation law requires us to collect this' would ordinarily be adequate.

NPP 1.3(f) Informing individuals of consequences of not giving personal information

An organisation need not describe all possible consequences of not providing personal information. Ordinarily an organisation would need to describe significant (and non-obvious) consequences. Often this would mean that the organisation makes clear which items are essential to fulfil the primary purpose of collection. An example of such a statement might be 'if you don't tell us this, we won't be able to process your application' or 'if you don't tell us this, we won't enter you in the competition'.

NPP 1.4 Collecting directly from the individual

NPP 1.4 aims to ensure that where it is reasonable and practicable to do so an organisation will collect information about an individual only from that individual.

TIP

Tips for compliance

Review your current practices to check whether you collect personal information directly or indirectly. Where you collect it indirectly consider whether it would be reasonable and practicable to collect it directly instead.

Deciding whether or not it is reasonable and practicable to collect personal information directly from the individual depends on the circumstances and involves balancing a number of possible factors including:

- whether it is possible to collect the information directly;

- whether a reasonable individual might expect information about them to be collected directly or indirectly;
- how sensitive the information is;
- the cost to an organisation of collecting directly rather than indirectly;
- the privacy consequences for the individual if the information is collected indirectly rather than directly; and
- what is accepted practice (by consumers and the industry).

NPP 1.5 Collecting from third parties

The aim of NPP 1.5 is to ensure that an individual knows what happens to information about them regardless of whether the information is collected directly or indirectly.

If an organisation collects information from a generally available publication NPP 1.5 may not apply depending on the circumstances.

The steps an organisation would need to take to make an individual aware of the matters listed in NPP 1.3 when it is not collecting directly from them will depend on the circumstances. Deciding what are reasonable steps where an organisation collects personal information indirectly involves balancing factors of a similar kind to those outlined for NPP 1.4.

TIP

Tips for compliance

An organisation collecting personal information indirectly could ask the organisation originally collecting the information to give the NPP 1.3 information about the indirectly collecting organisation as well. Depending on the circumstances, this could mean that the originally collecting organisation may need to include the name of the organisation that is going to indirectly collect the individual's information, the fact that the individual can get access to that information, the purposes for which the indirectly collecting organisation collects the information and who else the indirectly collecting organisation might give the personal information to.

NPP 10 Collecting sensitive information

NPP 10.1(a) Collecting sensitive information with consent

Ordinarily an organisation would need clear evidence that an individual had consented to it collecting sensitive information. If, at the same time, the organisation has given the individual comprehensive information on NPP 1.3 matters, including proposed uses and disclosures, an organisation is likely to have a strong basis for assuming it also has the individual's consent to such proposed uses and disclosures.

TIP

Tips for compliance

If an organisation seeks to meet an individual's special needs, it could do this in a number of ways that do not necessarily involve collecting sensitive information. For example, it could collect information about the language the individual speaks or the individual's specific dietary preferences or requirements rather than ask about the individual's racial or ethnic origin or disability.

NPP 10.1(b) – (e) Collecting sensitive information without consent

An example of where an organisation might be required by law to collect sensitive information under NPP 10.1(b) would be where there is a law that requires a blood bank to collect information about an individual's sexual practices if they wish to give blood.

Individuals may be legally incapable of consenting to the collection of sensitive information about themselves for the purposes of NPP 10.1(c) because of their mental or psychological state, or their age. Individuals may be legally incapable of giving consent regardless of whether a court or competent tribunal has made a formal determination about their capacity. In the case of a young person, ability to give consent is to be determined on a case-by-case basis. An example of a life or health emergency where NPP 10.1(c) might apply is where an individual is badly injured and an organisation needs to find out an individual's blood type.

A 'non-profit organisation' under NPP 10.1(d) means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade

or trade union aims. If the organisation has other aims, NPP 10.1(d) does not apply.

An example of where NPP 10.1(e) might apply is where an individual has made a claim under their life insurance policy and the insurer is preparing to dispute the claim and it needs to collect health or other sensitive information about the claimant and about witnesses in order to prepare its case.

NPP 10.2 Collecting health information to provide a health service

The rules dealing with obligations of professional confidentiality must be binding on the health service provider organisation, and must be established by competent health or medical bodies. Competent bodies might include medical boards and other rule-making bodies recognised in Federal or State/Territory legislation. Binding rules are rules that must be followed, and generally, will give rise to some sort of adverse consequence if breached.

NPP 10.3 Collecting health information for research, statistical and management purposes

An organisation can collect health information for these purposes if de-identified information would not achieve the relevant purpose, it is impracticable to seek the individual's consent *and* it complies with other specified requirements.

For more information about NPP 10.3 see *Information Sheet 9 – 2001 Handling Health Information for Research and Management*.

GUIDELINES TO NPP 2 – USE AND DISCLOSURE

NPP 2 – Use and disclosure

NPP 2 sets out the general rule that an organisation must only use or disclose personal information for the primary purpose of collection. Use and disclosure for a secondary purpose is not allowed except where such use or disclosure falls within the exceptions listed in NPP 2.

NPP 2.1(a) Primary and related purposes

Primary purpose

Determining the primary purpose of collection should always be possible. Where an organisation collects personal information directly from the individual the context in which the individual gives the information to the organisation will help identify the primary purpose of collection. When an individual provides and an organisation collects personal information, they almost always do so for a particular purpose – for example, to buy or sell a particular product or receive a service. This is the primary purpose of collection even if the organisation has some additional purposes in mind.

How broadly an organisation can describe the primary purpose will need to be determined on a case-by-case basis and it will depend on the circumstances.

Where an organisation collects personal information indirectly a guide to its primary purpose of collection could be what the organisation does with the information soon after it first receives it.

Related and directly related purposes within reasonable expectations

To be related, the secondary purpose must be something that arises in the context of the primary purpose.

If personal information is sensitive information the use or disclosure must be directly related to the primary purpose of collection. This means that there must be a stronger connection between the use or disclosure and the primary purpose for collection.

Individual's reasonable expectations

The test for what the individual would 'reasonably expect' would be applied from the point of view of what an individual with no special knowledge of the industry or activity involved would expect.

The NPPs are not intended to prevent personal information about individuals acting in a business capacity from being exchanged in the normal course of a business. In these circumstances, ordinarily it is likely to be within individuals' reasonable expectations that information about them in their business role will be used and disclosed for generally accepted business purposes. For example, exchange of business cards and use of them for later business contacts would ordinarily be consistent with the NPPs.

TIP

Tips for compliance

Working out what is the primary purpose and what is a related secondary purpose within the individual's reasonable expectations may not always be easy. In some circumstances, distinguishing between primary purpose and related secondary purposes may not be necessary, because in neither case does the organisation need consent for the use or disclosure.

The point is to keep in mind the aim of the NPPs which is ensuring organisations generally only use or disclose personal information in ways that individuals would reasonably expect.

When thinking about whether a use or disclosure falls within the primary purpose or a related or directly related purpose within the individual's reasonable expectations an organisation could, where relevant consider:

- the context in which it is collecting the personal information;
- the reasonable expectations of the individual whose information it is;
- the form and content of information the organisation has given about why it is collecting the individual's information (for example under NPP 1.3 and 1.5);
- how personal, confidential or sensitive the information is; and
- any duties of care or other professional obligations an organisation might have (although care would be needed if these are not within the person's reasonable expectations).

TIP

Where sensitive personal information is involved, the organisation would in general need to take a more conservative approach to what the individual would reasonably expect.

An organisation may run a greater risk of an individual making a complaint where there is a difference between the individual's and the organisation's understanding of the primary purpose or what might be reasonably expected to be done with the personal information. Organisations will reduce this risk by ensuring individuals are informed about the organisation's intended primary purpose and of its proposed uses or disclosures. This is likely to be particularly important where these uses or disclosures would not be obvious to an individual with no special knowledge of the industry or activity. The risks are greatest where an organisation collects personal information indirectly.

NPP 2.1(b) Secondary use and disclosure with consent

This allows an organisation to use or disclose personal information for a secondary purpose if it has the individual's consent. Consent to the use or disclosure can be express or implied. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation. For example, it may be possible to infer consent from the individual's failure to opt out provided that the option to opt out was clearly and prominently presented and easy to take up. If the organisation's use or disclosure has serious consequences for the individual, the organisation would have to be able to show that the individual could have been expected to understand what was going to happen to information about them and gave their consent. In such situations it would ordinarily be more appropriate for the organisation to seek express consent.

TIP

Tips for compliance

An organisation would have the most difficulty establishing consent to a use or disclosure where it wishes to rely on a failure to object to a use or disclosure to imply consent. Whether consent can be implied from a failure to object will often depend on whether there are circumstances in which it would be reasonable to conclude that the individual had the necessary knowledge and would have opted out if they objected to the use or disclosure.

An organisation will be in an increasingly better position to establish that the individual consented the more it can satisfy the following points:

- it is likely that the individual received and read the information about the use or disclosure;
- the chance to opt out of the offer is clearly stated and likely to be understood by the individual and the individual is likely to be aware of the implications of not opting out;
- the opting in or opting out is freely available and not bundled with other purposes;
- receiving the chance to opt out involves no financial cost to, and little effort from, the individual;
- opting out involves little effort from, and no or virtually no cost to the individual;
- the consequences of failing to opt out are harmless;
- if the individual opts out later, the individual is fully restored, where possible and appropriate, to the circumstances they would have been in if they had opted out earlier.

The greater the number of methods an organisation makes available to the individual to take the chance to opt out and the smaller the amount of time and cost involved on the part of the individual in taking up the opt out, the more likely it is that an opt out is easy to take up.

It is unlikely that consent to receive marketing material on-line could be implied from a failure to object to it. This is because it is usually difficult to conclude that the message has been read and it is generally difficult to take up the option of opting out as it is commonly considered that there are adverse consequences to an individual from opening or replying to email marketing – such as confirming the individual's address exists. This may also apply where material is distributed using other automated processes. (This would not prevent an organisation from seeking opt in consent on-line if NPP 2.1 allowed it.)

NPP 2.1(c) Direct marketing

This allows organisations to use non-sensitive personal information for direct marketing where, among other things, it is impracticable to seek the individual's consent and where the individual is told that they can opt out of receiving any more marketing from the organisation.

This principle only applies to the use of non-sensitive information for direct marketing and does not permit an organisation to disclose personal information for the purpose of direct marketing.

Impracticable to seek consent

Considering whether it is impracticable to seek the individual's consent involves balancing a number of factors that could include:

- how often the organisation is in contact with an individual;
- the way an organisation communicates with an individual;
- the consequences for the individual of receiving the information without having consented; and
- the cost to the organisation of seeking consent.

The question of impracticability would generally be considered at the time of the proposed use of the personal information for direct marketing – not the time the personal information was collected.

As the cost of emailing is negligible, ordinarily it will not be 'impracticable' to seek consent where an organisation chooses on-line methods of contact or communication. This means that generally an organisation could not rely on NPP 2.1(c) for techniques such as email marketing or SMS marketing. The option of using 2.1(b) is still available. However, in most cases, this will require express consent.

TIP

Tips for compliance

An organisation does not necessarily need to rely on NPP 2.1(c) for use of personal information for direct marketing. An organisation could get the individual's consent at the time of collection to use information about them for direct marketing or the use might be related to the primary purpose and within the individual's reasonable expectations.

NPP 2.1(d) Research and statistics relevant to public health or safety

In considering whether the use or disclosure is 'necessary', organisations must consider if de-identified information would be sufficient for the purpose. If de-identified information is sufficient, then identified information cannot be used or disclosed under this principle.

Research and statistics 'relevant' to public health or safety means that the research is about public health or public safety or the compilation or analysis of statistics is in relation to public health or public safety.

In assessing whether it is 'impracticable' to seek consent, this would ordinarily mean more than simply the incurring of some expense or effort in seeking consent. For example it may be impracticable to seek consent where the organisation is unable to locate the individual, despite making reasonable efforts.

For more information about how the NPPs apply to the use or disclosure of health information for research and statistical purposes see *Information Sheet 9 – 2001 Handling Health Information for Research and Management.*

NPP 2.1(e) Serious threats to life, health or safety

This exception is aimed at emergency situations where there is a serious threat to health and safety and using or disclosing personal information will help reduce that threat. Serious and imminent threats to an individual's life, health or safety may be a threat to the individual the organisation is dealing with or another person. Ordinarily a serious threat would be a threat of bodily injury, threat to mental health, illness or death. 'Imminent' means the threatened harm is about to happen. Threats to finances and reputation or a threat of stress or anxiety would not ordinarily be serious threats to life or health.

TIP

Tips for compliance

Think about whether the proposed use or disclosure will reduce the threat. Also think about whether there are alternative reasonable ways to reduce the threat (for example, by seeking consent to the use or disclosure) – this helps in working out whether the disclosure is necessary. Organisations considering using or disclosing personal information to reduce threats to public health or public safety may find it useful to discuss the threat in general terms (and whether the proposed use or disclosure is likely to reduce the threat) with a relevant authority dealing with public health or safety, for example a health department.

NPP 2.1(f) Unlawful activity

This acknowledges that one of an organisation's legitimate functions is to

investigate and report on suspected unlawful activity. Ordinarily but not in all cases, the suspected unlawful activity would relate to the organisation's operations. For further guidance on this see *Information Sheet 7 – 2001 Unlawful Activity and Law Enforcement*.

NPP 2.1(g) Required or authorised by law

The Privacy Act does not override specific legal obligations relating to use or disclosure of personal information. 'Law' includes Commonwealth, State and Territory legislation, as well as common law. If an organisation is required by law to use or disclose personal information it has no choice and it must do so. If an organisation is authorised by law to use or disclose personal information it means the organisation can decide whether to do so or not. The authority is there but the organisation can decide. For more information on this see *Information Sheet 7 – 2001 Unlawful Activity and Law Enforcement.*

NPP 2.1(h) Enforcement bodies

This allows an organisation to use or disclose personal information where it reasonably believes this is reasonably necessary for a range of functions or activities carried out by, or on behalf of, an enforcement body (see section 6 for what is an enforcement body). Unless the law prohibits it, the organisation must make a written note of such a use or disclosure (see NPP 2.2). For more information on this see *Information Sheet 7 – 2001 Unlawful Activity and Law Enforcement.*

NPP 2.3 Primary purpose and related companies

NPP 2.3 clarifies the way NPP 2.1 works where related corporations share personal information. The Privacy Act has special provisions to deal with 'related bodies corporate' (related companies). Section 13B allows one company to share non-sensitive personal information with another related company without the disclosure and the collection being a breach of privacy. However, the effect of NPP 2.3 is that the primary purpose at the first point of contact with the group follows the personal information. A company that has received personal information from a related company would have to assess, using the primary

purpose of collection at the first point of contact, whether a use it wishes to make or a disclosure beyond the corporate group it proposes would meet the requirements of NPP 2.

NPP 2.4 – 2.6 Disclosing health information to a responsible person

NPP 2.4 applies only to organisations that provide a health service and only to health information. 'Health service' and 'health information' are defined in section 6 of the Privacy Act. NPP 2.4 permits a provider of a health service to disclose health information in some circumstances where the individual is unable to give consent and where the disclosure is not contrary to any known wish of the individual. A disclosure under this principle is only permitted to ensure the individual receives appropriate care or treatment or where it is necessary for compassionate reasons. NPP 2.5 and 2.6 describe the people such a disclosure might be made to - for example, a guardian, close relative or friend.

More detail on NPP 2.4 – 2.6 is contained in the *Guidelines on Privacy in the Private Health Sector.*

GUIDELINES TO NPP 3 – DATA QUALITY

NPP 3 – Data quality

NPP 3 Accurate, complete and up-to-date

The aim of NPP 3 is to prevent the adverse consequences for people that might result from an organisation collecting, using, or disclosing inaccurate, incomplete or out-of-date personal information.

Organisations would only need to take reasonable steps to confirm the accuracy, completeness and currency of the personal information they hold at the time they collect, use or disclose it. They do not need to check it at other times. However, an organisation may be obliged to correct personal information it holds should the individual to whom the information relates establish that it is not accurate, complete or up-to-date (see NPP 6.5).

TIP

Tips for compliance

To comply with this principle the main focus for organisations could be on areas where inaccurate, incomplete or out-of-date personal information is most likely to have a detrimental affect on people.

What are reasonable steps will vary depending on the circumstances. Factors to consider include:

- how likely it is that the personal information is complete, accurate and up-to-date;
- whether this kind of personal information changes over time;
- how recently the organisation collected the personal information;
- how reliable the personal information is likely to be;
- who provided the personal information; and
- what the organisation uses the personal information for.

If an organisation uses personal information soon after it is collected from the individual, it may not need to check it. If it collects the personal information from someone else, there may be a greater need for the organisation to take appropriate action to confirm that it is accurate, complete and up-to-date.

GUIDELINES TO NPP 4 – DATA SECURITY

NPP 4 – Data security

NPP 4.1 Protecting personal information

NPP 4.1 requires an organisation to take reasonable steps to protect the personal information it holds from misuse and loss, and from unauthorised access, modification or disclosure.

Protecting the security of personal information could consist of maintaining:

- physical security – by adopting measures to prevent unauthorised entry to premises, systems to detect unauthorised access and secure containers for storing paper-based personal information;
- computer and network security – by adopting measures to protect computer systems and networks for storing, processing and transmitting personal information from unauthorised access, modification and disclosure;
- communications security – by protecting communications via data transmission, including email and voice, from interception, and preventing unauthorised intrusion into computer networks; and
- personnel security – by adopting procedural and personnel measures for limiting access to personal information by authorised staff for approved purposes and controls to minimise security risks to an organisation's IT systems.

Reasonable steps

What are reasonable steps to secure personal information will depend on the organisation's particular circumstances. Some relevant factors could include:

- the sensitivity of the personal information the organisation holds;
- the harm that is likely to result to people if there is a breach of security;

- how the organisation stores, processes and transmits the personal information (for example, paper-based or electronic records);
- the size of the organisation (the larger the organisation, the greater the level of security likely to be needed).

TIP

Tips for compliance

Steps that an organisation could take to comply with NPP 4.1 include:

- risk assessment – identifying the security risks to personal information held by the organisation and the consequences of a breach of security;
- security policy – developing a policy that implements measures, practices and procedures to reduce the identified risks to security;
- staff training – training staff and management in security awareness, practices and procedures;
- monitor and review – monitoring compliance with the security policy, periodic assessments of new security risks and the adequacy of existing security measures;
- looking at Australian and international standards as a guide; and
- depending on the size of the organisation and the information it collects, perhaps having an external privacy audit conducted.

NPP 4.2 Destroying or de-identifying personal information

NPP 4.2 requires an organisation to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose under NPP 2. Purposes under NPP 2 could include a legal requirement to keep the personal information.

Reasonable steps would not necessarily involve detailed culling of existing personal information. However, if an organisation does not have in place systems for destroying or de-identifying personal information that is no longer needed, NPP 4.2 would require it to progressively develop such systems.

TIP

Tips for compliance

Destruction of records containing personal information should be by secure means. Ordinarily, garbage disposal or recycling of intact documents are not secure means of destruction and should only be used for documents that are already in the public domain. Reasonable steps to destroy paper documents that contain personal information include shredding, pulping or disintegration of paper.

The reasonableness of steps taken to destroy personal information contained in electronic records will depend on the medium on which the data is stored and the available methods for erasing data.

De-identification of personal information

De-identification involves the removal of any information by which an individual may be identified from a record. De-identification must be permanent, which means that an organisation is not able to match the de-identified information with other records to re-establish the identity of people. Reasonable steps would also include ensuring that the de-identified information cannot be re-identified in the hands of an organisation receiving the data.

TIP

Tips for compliance

The test for whether information is identifiable is whether the identity of the individual is apparent, or may reasonably be ascertained, from the information using the definition of 'personal information' in section 6 of the Privacy Act.

A de-identification procedure would not be complete if, from the resulting information, the identity of an individual may be reasonably ascertained. Reasonable steps to de-identify information could include:

- considering the capacity of the organisation to re-identify the information;
- careful consideration of the identifying nature of every aspect of the information; and
- setting up safeguards that ensure that future collection or uses will not re-identify the information.

An organisation may need to include in contractual arrangements with a receiving organisation that it will not re-identify the information.

GUIDELINES TO NPP 5 – OPENNESS

NPP 5 – Openness

NPP 5.1 A policy in a document

In most cases a documented general policy that sets out:

- whether an organisation is bound by the NPPs or a privacy code approved by the Commissioner, and if this is the case, a reference to the privacy code;
- any exemptions under the Privacy Act that apply to the personal information the organisation holds or to any of its acts or practices; and
- that an individual can get more information on request about the way the organisation manages the personal information it holds;

would be enough to meet the requirement of NPP 5.1. The organisation must make the document available to anyone who asks for it.

TIP

Tips for compliance

It is often the case that the more open an organisation is about its information handling practices the less complaints it is likely to receive and the fewer the requests from individuals for access to information the organisation holds about them.

Additional information that an organisation could have in the document include:

- the kinds of personal information the organisation holds;
- the main purposes for which the organisation holds the information;
- whether it contracts out services that involve disclosing personal information;
- how an individual can complain about a breach of privacy including a contact number in the organisation the individual can ring;
- the organisation's contact details; and
- how the organisation handles requests for access to personal information.

For more information about openness see *Information Sheet 3 – 2001 Openness*.

NPP 5.2 Giving more information about personal information management

This principle aims to give the individual a fuller understanding of the sort of personal information an organisation holds and the way it handles that information.

TIP

Tips for compliance

Depending on the circumstances an organisation could decide whether to let the individual know this information either verbally or in writing.

Reasonable steps

What is reasonable will be different for each organisation. It will depend on the circumstances and what information the individual has asked for.

See *Information Sheet 3 – 2001 Openness* for more information on NPP 5.2 including:

- other information that could be provided under NPP 5.2; and
- reasonable steps and NPP 5.2.

GUIDELINES TO NPP 6 – ACCESS AND CORRECTION

NPP 6 – Access and correction

NPP 6.1 Access to personal information

NPP 6 gives an individual a right of access to all the personal information that an organisation holds about them, although there are some exceptions.

Ways an organisation could give access to an individual would include allowing them to inspect records, take notes or giving them a photocopy or printout.

There are a limited number of situations where an organisation may deny an individual access to the personal information an organisation holds about them. Where such an exception applies to a request for access, an organisation would ordinarily need to give the individual access to the parts of the record that are not exempt.

Time frames for access

An appropriate time to take for an organisation to respond to an individual's request for access will be influenced by various factors. These may include the method of communication, the type or amount of personal information requested, how the personal information is held, how complex an organisation's functions and activities are and how the personal information is to be provided to the individual making the request.

In the case of a large organisation where giving access may be a reasonably complex matter and access is not given over the phone or by electronic means, the following response times, based on public sector freedom of information legislation, are offered as a useful starting point for organisations:

- If the individual has made a written request for access, acknowledging the request as soon as possible or at least within 14 days could, in many cases, be appropriate.
- If granting access is straight forward, it would often be appropriate for an organisation to grant access within 14 days, or if giving it is more complicated, within 30 days.

TIP

Tips for compliance

As part of its privacy practice an organisation would need to take the minimum steps necessary to ensure that the individual seeking access is in fact the individual the personal information is about, otherwise the organisation may make a disclosure in breach of NPP 2.

NPP 6.1(a) A serious and imminent threat

Serious threats would include a threat to the life or health of any person; for example bodily injury, threat to mental health, illness or death. Imminent threat means the threat is about to happen.

NPP 6.1(b) Serious threats

Where health information is involved, an organisation would be able to deny access where there is a serious threat. The serious threat does not have to be imminent. It could happen at any time.

TIP

Tips for compliance

Public Health Acts give some indication of the range of conditions and threats that have been considered to be significant enough to warrant legislating about them in the interest of public health.

NPP 6.1(c) Unreasonable impact on the privacy of others

Access to a document containing personal information about people other than the individual requesting access need not be denied altogether. For example, in such a case, it may be possible to delete the other individual's personal information from the document before it is released to the individual who made the request.

TIP

Tips for compliance

Information that could have an unreasonable impact on another person's privacy can include more than information such as name and address. It could include any information in the document from which the identity of the person could be reasonably ascertained.

NPP 6.1(d) Frivolous or vexatious requests

Frivolous and vexatious requests could include those that are:

- trivial and made for amusement's sake; or
- made as a means of pursuing some unrelated grievance against the organisation; or
- repeated requests for access to the same personal information.

TIP

Tips for compliance

Often, a request for access would not be frivolous or vexatious just because it is irritating. Organisations are encouraged to take a narrow approach to this exception.

NPP 6.1(e) Existing or anticipated legal dispute resolution proceedings

An organisation would not have to grant an individual access to the personal information in circumstances where legal dispute resolution proceedings are under way or anticipated and where discovery would not grant access to the personal information.

NPP 6.1(f) Access would prejudice negotiations

An organisation would not have to provide access to an individual's information if it would show the organisation's intentions and would prejudice or interfere in some negative way in the organisation's negotiations with the individual.

NPP 6.1(g) Access would be unlawful

This exception would cover circumstances where providing access to personal information would be a breach of confidence under the law, for example a breach of legal professional privilege.

NPP 6.1(h) Denial of access is required or authorised by law

The law in question might be State, Territory or Commonwealth law. If an organisation is required by a law to refuse access it has no choice. It must refuse

access. If an organisation is authorised by law to refuse access it means the organisation can decide whether to do so or not. The authority is there but the organisation can decide.

NPP 6.1(i) Prejudice to investigation of unlawful activity

Organisations are not required to provide access to personal information where unlawful activity is reasonably suspected, for example fraud or theft, and access would prejudice investigations into that activity.

NPP 6.1(j) and (k) Enforcement activities

An enforcement body may ask an organisation not to provide an individual with access to certain personal information when that information will itself prejudice an investigation carried out by, or on behalf of, an enforcement body or a security function.

For more information on these circumstances see *Information Sheet 7 – 2001 Unlawful Activity and Law Enforcement.*

NPP 6.2 Commercially sensitive decision-making processes

This exception to the access principle would cover commercially sensitive decision making processes but would not permit an organisation to deny access to the factual personal information on which those decisions have been based or other personal information it holds. In most cases an individual seeks access for an explanation of why an organisation has made an adverse decision. An organisation could usually meet this concern by explaining (as far as possible) the reasons for its actual decision and giving the raw data. This exception might apply where an organisation has used a credit-scoring tool that is commercially sensitive and it does not want to make the score card factors and their weightings available.

Organisations can only rely on the exception to only give an explanation for a commercially sensitive decision where NPP 6.2 does apply.

NPP 6.3 Access through an intermediary

Use of intermediaries

This principle requires an organisation to consider using a mutually agreed intermediary if reasonable. There will be some cases, for example investigations of fraud or theft, where no form of access to the information the individual is asking for will be appropriate. In other circumstances an organisation would be able to consider using an intermediary as an alternative to complete denial of access. For more information about intermediaries see *Information Sheet 5 – 2001 Access and the Use of Intermediaries.*

NPP 6.4 Charging for access

This principle aims to prevent an organisation from charging an excessive amount to discourage persons from making requests for access. An organisation cannot charge an individual for lodging a request for access.

For more information about charges and access see *Information Sheet 4 – 2001 Access.*

NPP 6.5 Correcting personal information

This principle requires that an organisation take reasonable steps to correct information about an individual where that information is not accurate, up-to-date and complete. What is reasonable will depend on the circumstances. For example, an organisation might not be obliged to correct personal information that is inaccessible and never likely to be used even if it is of poor quality.

NPP 6.6 Disputed accuracy

If an individual and an organisation are unable to agree about whether personal information is accurate, up-to-date and complete, the organisation must, at the request of the individual take reasonable steps to associate with the personal information the individual's claim that it is not accurate, complete and up-to-date.

NPP 6.7 Giving reasons for denying access

NPP 6.7 requires an organisation to give an individual its reasons for denying access or refusing to correct personal information. The organisation should endeavour to tell the individual which exception under NPP 6.1 it is relying on to refuse access. However, this would not be required where such a disclosure would prejudice an investigation against fraud or other unlawful activity.

GUIDELINES TO NPP 7 – IDENTIFIERS

NPP 7 – Identifiers

NPP 7 seeks to ensure that increasing use of Commonwealth government identification does not lead to a de facto system of universal identity numbers, and to prevent any loss of privacy from the combination and re-combination of the data.

For these reasons tax file number legislation already restricts the way an organisation can collect, use or disclose a tax file number.

A Commonwealth government identifier is a unique combination of letters and numbers, such as a Medicare number, which Commonwealth government agencies or contracted service providers allot to an individual.

NPP 7.1 Adoption of identifiers

Unless prescribed by regulation, NPP 7.1 prohibits an organisation from collecting a particular Commonwealth government assigned identifier from all the people with whom it deals and then using that identifier to organise and match other personal information organised by reference to that same identifier. In other words, an organisation is not permitted to adopt a government identity number as if it were its own identity number.

NPP 7.2 Use and disclosure of identifiers

NPP 7.2 aims to prevent organisations from using Commonwealth government assigned identifiers in a way that is inconsistent with the purpose for which they were originally issued. This NPP limits the circumstances in which an organisation can use or disclose a Commonwealth government identifier to those in which such use or disclosure is:

- necessary for the organisation to fulfil its obligations to the agency that assigned the identifier to the individual, or
- in the interest of health or safety or authorised or required by or under law, or in certain other public interests (NPP 2.1(e) - (h)); or

- under regulations that allow use or disclosure of the identifier by a certain organisation in certain circumstances.

GUIDELINES TO NPP 8 – ANONYMITY

NPP 8 - Anonymity

NPP 8 Dealing with people anonymously

Unless there is a good practical or legal reason to require identification, organisations must give people the option to operate anonymously.

Anonymity is an important element of privacy. In some circumstances, it will not be practicable to do business anonymously. In others there will be legal obligations that require identification of the individual. This principle is not intended to facilitate illegal activity.

GUIDELINES TO NPP 9 – TRANSBORDER DATA FLOWS

NPP 9 – Transborder data flows

NPP 9 Sending personal information overseas

NPP 9 outlines the circumstances in which an organisation can transfer personal information it holds outside Australia. This principle is based on the restrictions on international transfers of personal information set out in the European Union Directive 95/46.

In the simplest terms, NPP 9 prevents an organisation from disclosing personal information to someone in a foreign country that is not subject to a comparable information privacy scheme, except where it has the individual's consent or some other circumstances including where:

- the transfer is for the benefit of the individual and the organisation can show grounds for a belief that if it were practicable to obtain consent the individual would be likely to give it; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party.

Transfers within an organisation

NPP 9 does not prevent transfers of personal information outside Australia by an organisation to another part of the same organisation, or to the individual concerned. Section 5B provides for the Act to operate extra-territorially in these circumstances.

Related companies

A company transferring personal information overseas to a related company must comply with NPP 9.

Given that transferring personal information overseas may remove it from the protection of Australian law, an organisation relying on NPP 9(a) and NPP 9(f)

may need to be in a position to give evidence about the basis on which it decided that it has met the requirement of 'reasonable belief' or 'reasonable steps'.

TIP

Tips for compliance

Getting a legal opinion would be a good way for an organisation to get such evidence.