Plain English Guidelines to Information Privacy Principles 4-7

Advice to agencies about storage and security of personal information, and access to and correction of personal information

Privacy Commissioner, February 1998

 ISBN 0 642 22215 0.

Contents

Introduction

Many of the IPPs reflect ideas set out in the Organisation for Economic Cooperation and Development's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (the OECD guidelines). These were promulgated in 1980. In 1984, Australia committed itself to taking the guidelines into account in domestic legislation. The Privacy Act assists in meeting this commitment.

IPPs are minimum standards only

The IPPs set out minimum standards for **Agencies**. Compliance with the IPPs is a legal obligation, but minimal compliance will not always be an appropriate approach for an **Agency** to take. In developing new programs and policies, **Agencies** are encouraged always to look for the least privacy-intrusive way of meeting their objectives. Especially where sensitive information is concerned, or where mishandling of **personal information** may have serious consequences, more care to protect individuals' privacy may be appropriate than is required by the letter of the IPPs.

How can I get more advice about the IPPs?

The Privacy Commissioner has published various guidelines and documents on the *Privacy Act*. These include:

- *Guidelines to IPPs 1-3*
- *Guidelines to IPPs 8-11*
- *Outsourcing and Privacy*

Contains model privacy clauses for contracts in which the **Agency** engages outsiders to perform functions that involve handling **personal information**. Copies are available from the Privacy Commissioner's Office.

Information about the application of the IPPs in any particular Commonwealth or ACT **Agency** can also be obtained from that **Agency**'s Privacy Contact Officer.

General privacy enquiries can be made to the Privacy Commissioner's Office.

Advice about Agency obligations under the Freedom of Information Act

In most **Agencies** the first point of contact for advice about the Freedom of Information Act is the **Agency**'s legal area, although many Privacy Contact Officers also handle FOI matters.

The Information Law Branch of the Attorney-General's Department may be able to provide advice on more complex FOI matters.

Advice about Agency obligations under the Archives Act

Information about the Archives Act may be found in the *Australian Archives Handbook*, in the Act itself, and on the Australian Archives Internet web page at http://www.aa.gov.au.

When do the IPPs apply?

IPPs 4 to 7 - together with Principles 8 and 9 - apply to all **personal information**, regardless of when the information was collected. IPPs 1, 2, 3, 10 and 11 apply only to information collected after the commencement of the Privacy Act on 1 January 1989.

Meaning of words

The meanings used here are based on the definitions in sections 6 and 10 of the Privacy Act.

*"**Agency**"*

Agencies are generally Commonwealth government organisations, including:

- Commonwealth government departments;
- bodies and tribunals set up for a public purpose by Commonwealth laws.

Agencies also include:

- contracted case managers under the Employment Services Act;
- Australian Capital Territory government organisations;
- hearing service providers under the Hearing Services Administration Act.

In 1997 the Government announced its intention to amend the Privacy Act to cover contractors handling **personal information** on behalf of the Commonwealth. When passed, this legislation will affect the definition of **"Agency**".

State, Northern Territory, and local government organisations are not "**Agencies**". Some organisations, even if set up by Commonwealth laws, are also not "**Agencies**". These include incorporated companies; incorporated societies; and incorporated associations.

"personal information"

The Privacy Act only covers **personal information**. The Privacy Commissioner takes the view that this is information or an opinion that can identify a living person.

Although information about dead people is not technically considered to be **personal information**, **Agencies** are encouraged to respect the sensitivities of family members when using or disclosing it.

"record"

A record is a:

- document
- database
- photograph or video

The Privacy Act lists a number of exceptions to this definition. For example, "generally available publications" are not records.

"record-keeper"

A record-keeper is an **Agency** that possesses or controls a record of **personal information**. If one **Agency** possesses a record, but another **Agency** controls it, each **Agency** is a record keeper.

Information Privacy Principle 4

IPP 4, titled ***Storage and security of personal information***, states:

A record-keeper who has possession or control of a record that contains **personal information** shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

This embodies the principle that a person whose information is held by a government **Agency** has a right to expect that the **Agency** will hold it securely, and will ensure that access to the information is permitted only for legitimate purposes.

IPP 4(a) - security safeguards

IPP 4(a) obliges an **Agency** to protect the **personal information** it holds with such safeguards as are reasonable in the circumstances. If it does not, it breaches IPP 4, even if no loss, unauthorised access, use, modification or disclosure actually takes place.

Existing guidance on security standards

A number of Commonwealth government **Agencies** provide advice on security issues and it would not be appropriate for the Privacy Commissioner to try to duplicate or replace these sources of advice. The *Protective Security Manual* (PSM) is issued by the Protective Security Coordination Centre within the Attorney-General's Department. It sets out standards for protective security for Commonwealth **Agencies**, including physical security and computer security. The PSM makes it clear that the head of each **Agency** is responsible for the **Agency's** security and, in particular, for developing and implementing an **Agency** Security Policy together with a Systems Security Policy for the **Agency's** computer systems.

The PSM sets out minimum standards and is a basis for developing **Agency** specific protective security policies and procedures, including policies and procedures to protect **personal information**. If an **Agency** properly develops and implements protective security policies and procedures for **personal information** in line with the PSM, it will minimise its risk of breaching IPP 4. The PSM also directs **Agencies** to sources of specialist advice on other security issues. Most **Agencies** have appointed an **Agency** Security Adviser who is available to provide advice on security issues.

The Australian Security Intelligence Organization (ASIO) has an advisory role for Commonwealth **Agencies** on matters relating to protective security.

One of the functions of the Defence Signals Directorate (DSD) is to "provide advice on request to Government Departments and authorities in relation to other sensitive official information unrelated to national security but which for privacy, financial or other reasons requires protection from unauthorised disclosure ..." . DSD publishes *Australian Communications - Electronic Security Instructions*, which give detailed advice to **Agencies** in relation to computer security. Where DSD guidelines do not apply, reasonable steps to secure data held on computer media or transmitted over telecommunications networks would include normal commercial IT practices, unless the data was particularly sensitive.

If advice is needed on the physical security of existing or proposed facilities, **Agencies** may contact the Protective Security Coordination Centre of the Attorney-General's Department for advice and referral to an appropriate organisation.

Managing the security of personal information

The best way for an **Agency** to avoid breaches of IPP 4 is to establish systems to control the way the **personal information** it holds is used and disclosed. An **Agency's** security systems must take into account a range of considerations, and it is not possible for these guidelines to try to lay down detailed rules for the design of such systems. There are, however, several steps an **Agency** may take to minimise the chances of breaching IPP 4.

Each **Agency** should have a documented policy on the security of **personal information** which is accessible to all staff, which explains what security measures need to be taken, and which specifies in each case what needs to be done, when and by whom. The policy should cover physical, computer and communications security, needs to be more than a statement of principle, and should give practical advice on situations that regularly arise in particular areas of the organisation. Each **Agency** should also put in place systems to ensure that only authorised staff have access to **personal information**. Computer operating systems should provide for appropriate access controls, using industry standard software.

There should be a contact officer available to discuss cases where the appropriate security measures are not clear. The **Agency** Security Adviser would be a logical choice, but other officers may be appropriate depending on the size of the **Agency** or its range of functions.

An **Agency** should establish systematic channels for scrutinising requests or classes of requests for information from outside the **Agency**. In some cases the best way of doing this may be to pass requests through a central area. Non-routine disclosures should have to be authorised by one of a small number of staff at an appropriately senior level.

Agencies should conduct regular audits of physical and computer security and follow up the results.

Staff should be trained in good security practices, including the **Agency's** security policy. Security and other Privacy Act requirements should form a standard part of an **Agency's** operation, with training included in induction packages and other internal training courses.

Common security problems identified in audits

Staff of the Privacy Commissioner's office regularly conduct audits of Commonwealth **Agencies** to assess their compliance with the IPPs. A number of problems with the security of information, which put the **Agency** at risk of breaching IPP 4, regularly come to the auditors' attention. Other problems have been identified by a computer security survey conducted by the office of the Privacy Commissioner, and issued to participating **Agencies** in December 1995. The list which follows is not exhaustive, but represents a minimum level of safeguards in selected areas.

Physical security

Filing cabinets, safes and compactuses containing records of **personal information** should not be left unlocked.

All paper records containing **personal information** should be held on official **Agency** files and recorded on the **Agency** registry system. Files should have security classifications reflecting the importance or sensitivity of the records held on them. Storage and access arrangements should reflect the security classification. Movements of files should be recorded on the **Agency** registry system, particularly if the files are being forwarded to another office or moved interstate. Where microfiche records are still in use, a register should be kept to ensure that none are missing. Thermal paper faxes are unstable and should be copied onto plain paper before filing to avoid potential loss of data.

A clean desk policy, under which all papers are required to be securely stored at the end of the working day rather than left on the desk, is good practice. This reduces the risk of **personal information** being left lying around and being seen or taken by unauthorised people.

Personal information about real people should not be used in training material. At a minimum, fictitious names should be used, and care should be taken to ensure that the person cannot be identified from the context.

Irrelevant **personal information**, or unrelated **personal information** about third parties, should not be included in any files. If such information is kept, there is a risk that it may be wrongly disclosed or used.

An **Agency** should have in place appropriate disposal arrangements for records containing **personal information**, in line with the General Disposals Authorities issued under the Archives Act, and any other disposals authorities applying to the **Agency**. Destruction of records needs to be secure.

An **Agency** should pay close attention to the level of clearance and supervision needed by cleaning and other contract staff who have access to areas in which **personal information** is kept, particularly if access is after hours and unsupervised. (For advice about contracts with IT consultants, cleaners etc, see under IPP 4(b) below.)

If it is **Agency** policy that identification badges be worn, this should be strictly enforced. Former **Agency** staff should not be allowed to retain access privileges in relation to premises or information resources.

Computer security

Each individual officer should have his or her own password for access to the computer system. Screen savers should also be equipped with passwords unique to the individual user. Computer systems should require that passwords be changed regularly; not be obvious words; and be of a certain length. It should be impossible for a user to alternate between two favoured passwords. Passwords must be kept securely and not disclosed to other staff members. Unsuccessful logon attempts should be logged and monitored.

Computer systems should have automatic logout facilities so that they cannot be left permanently logged on. It should be impossible to bypass screen savers.

The **Agency** should be able to monitor access to databases containing **personal information** by the use of audit trails - who is accessing the database, when and how often. Where this is not possible, **Agencies** should consider what other controls could be used to limit the possibility of unauthorised access.

Remote terminals should have security features as strong as central site terminals which allow access to the same classes of **personal information**. Access to portable computers and any **personal information** they contain must be secured.

Shared drives on Local Area Networks and Wide Area Networks should be controlled so that **personal information** on the drive can be accessed only by authorised staff.

Computer data storage systems should be backed up regularly to minimise the chance that **personal information** may be lost through system failure. Backups need to be securely stored, preferably offsite.

Programmers should not have access to production databases which contain **personal information**.

Access privileges assigned to staff should be reviewed regularly to determine if they are still appropriate, particularly when staff move from area to area within the **Agency**. **Agencies** could consider setting up procedures so that access is automatically removed or downgraded to a lesser level when an officer changes areas, with renewed or increased access subject to a request from the receiving area. When staff leave an **Agency**, their computer logon should be deleted immediately and they should be denied access to **Agency** records.

Agencies which provide access to the Internet should ensure that files containing **personal information** are protected against unauthorised external access.

Security of communications

Wherever practical, **personal information** should not be transmitted across public networks, by fax or e-mail etc, in plain text. Particularly when handling sensitive **personal information**, **Agencies** should consider using encryption to protect it during transmission. Where this is not feasible, **Agencies** may consider related techniques such as splitting the data into meaningless groupings for transmission and reconstituting the information at the destination point. At a minimum, recipients of faxes should be advised in advance that a message containing **personal information** is being sent, and receipt should be confirmed.

IPP 4(b) - records given to people outside the Agency

Under IPP 4(b), if an **Agency** gives **personal information** to a person or organisation in connection with the provision of a service to the **Agency**, it must do everything reasonably within its power to prevent unauthorised use or disclosure of the information. This provision will usually apply when information processing is outsourced, especially in the IT area.

The Privacy Commissioner's publication *Outsourcing and Privacy*, sets out clauses recommended for inclusion in contracts for IT and other services. In summary, the clauses oblige the contractor to:

- protect the **personal information** it holds in connection with the contract;use the information only for purposes set out in the contract;
- not disclose any **personal information** except with written authorisation from the **Agency**;
- not transfer any **personal information** outside Australia without approval from the **Agency**;
- ensure that any employee or subcontractor's employee signs an undertaking not to access, use, disclose or retain **personal information** except in performing their duties;
- notify the **Agency** if any of the privacy clauses have been breached;
- acknowledge that certain provisions of the Crimes Act 1914 may apply to its handling of **personal information** to which it has access;
- comply with reasonable **Agency** requests originating from the exercise of the Privacy Commissioner's functions under the Privacy Act;
- indemnify the Commonwealth for any liability arising from a breach by the contractor of the privacy clauses; and
- together with the **Agency**, follow agreed procedures for dealing with complaints relating to the contract services.

To include such clauses in contracts which involve giving the contractor **personal information** would generally be regarded as being reasonably within an **Agency's** power. Failure to do so risks breaching IPP 4(b). The contract should also provide for **Agency** monitoring of observance of these clauses by the contractor.

IPP 4(b) can also apply when the Commonwealth enters into:

- a service delivery agreement with a State government that involves a Commonwealth **Agency** providing **personal information** to a State **Agency**; or
- cooperative arrangements with other governments or private sector organisations, for example, coordinated health care arrangements, that involve a Commonwealth **Agency** providing **personal information** to the other parties.

In these circumstances, the agreement or arrangements should include explicit undertakings from the recipients that **personal information** provided by the Commonwealth **Agency** will be afforded the

same level of privacy protection as it would in the hands of the **Agency**. These undertakings may be expressed in the same terms as the clauses in *Outsourcing and Privacy* discussed above.

Information Privacy Principle 5

IPP 5, titled ***Information relating to records kept by record-keeper***, states:

A record-keeper who has possession or control of records that contain **personal information** shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) whether the record-keeper has possession or control of any records that contain **personal information**; and
(b) if the record-keeper has possession or control of a record that contains such information:
    (i) the nature of that information;
    (ii) the main purposes for which that information is used; and
    (iii) the steps that the person should take if the person wishes to obtain access to the record.

A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

A record-keeper shall maintain a record setting out:

(a) the nature of the records of **personal information** kept by or on behalf of the record-keeper;
(b) the purpose for which each type of record is kept;
(c) the classes of individuals about whom records are kept;
(d) the period for which each type of record is kept;
(e) the persons who are entitled to have access to **personal information** contained in the records and the conditions under which they are entitled to have that access; and
(f) the steps that should be taken by persons wishing to obtain access to that information.

A record-keeper shall:

(a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and
(b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

IPP 5 reflects the fact that, in order to be able to exercise their other rights in relation to the **personal information** that **agencies** hold about them, people must be able easily to find out:

- the existence of **personal information** systems that affect them;
- the nature and extent of those systems;
- the main purposes and uses of those systems; and
- how to gain access to **personal information** held in them.

IPP 5.1 - letting people find out about personal information held

Under IPP 5.1, an **Agency** must take reasonable steps to allow any person to find out whether it has any records that contain **personal information**, and if so, the nature of that information; the main

purposes for which it is used; and the steps that a person should take if they want to obtain access to it.

This reflects the idea that in general the government should not secretly keep **personal information** about individuals. Access to records - or, in rare circumstances, acknowledgment of the fact that a class of record is held at all - may be withheld if that is required or authorised by a law of the Commonwealth that provides for access by persons to documents (see IPP 5.2). But every **Agency** should have a general policy of openness about the types of **personal information** that it holds and what it uses them for.

Reasonable steps an **Agency** should take include maintaining a statement describing the nature of the **personal information** it holds, in line with IPP 5.3. An **Agency** should also let people making enquiries know that the statement is available for their inspection. IPP 5.4 requires an **Agency** to make the statement available for inspection by members of the public, and to give a copy of the statement to the Privacy Commissioner in June of each year. The Commissioner compiles these statements and publishes them annually in the **Personal information** Digest, pursuant to s.27(1)(g) of the Privacy Act. For more detail see the section on IPP 5.4 below.

An **Agency** should make sure that staff in general, and enquiries staff in particular, are aware of the statement the **Agency** maintains under IPP 5.3, and can direct people to it.

IPP 5.2 – exceptions

IPP 5.2 says that an **Agency** does not have to tell a person about **personal information** it holds or controls, if it is required or authorised not to do so by a Commonwealth law that provides for access to documents.

In effect, IPP 5.2 normally refers to the *Freedom of Information Act 1982* and the *Archives Act 1983*. If either of these Acts authorises an **Agency** not to reveal the existence of particular **personal information** or a particular class of **personal information**, then IPP 5.2 does not oblige the **Agency** to reveal it. For sources of information about the FOI Act and the Archives Act, see *Other sources of information* in the Introduction to these guidelines.

A requirement or authorisation for the purposes of IPP 5.2 must be specifically about access to documents. For example, a general provision that a statutory office holder or the head of an **Agency** may do anything necessary or convenient to be done for or in connection with? a function does not meet this criterion.

IPP 5.3 - maintaining statements of personal information held

This requires that each **Agency** which has possession of or control over records of **personal information**, shall maintain, for each type of record containing **personal information**, a statement of:

(a) the nature of the records kept by or on behalf of the **Agency**;
(b) the purpose for which the records are kept;
(c) the classes of people about whom the records are kept;
(d) the period for which the records are kept;
(e) who is entitled to have access to **personal information** in the records and the conditions under which they are entitled to have access; and
(f) steps that should be taken by people wishing to obtain access to the records.

Note that the statement is required to cover only “records” containing **personal information**. So information that is not in a record - for example, information in a generally available publication or the collections of a library or museum - need not be covered by the statement. (See the definition of “record” above.)

Statement to be maintained throughout the year

The Privacy Commissioner publishes these statements annually in the **Personal information** Digest (see IPP 5.4(b) below). But each **Agency** is required by IPP 5.3 to maintain its statement throughout the year, not just to update it once a year in time for its annual return to the Privacy Commissioner. Whenever a new class of record is collected or the details of an existing class change, an **Agency** should amend its statement to reflect this.

Standard format for statements

The Privacy Commissioner’s office has developed a standard format for these statements, which includes all the items necessary to fulfill **Agencies’** responsibilities under IPP 5. **Agencies** are required to set out, for each type of record, the following things.

Name of the class of records

This should be the full name, not an in-house abbreviation. Each class of record represents a separate file, database or type of record as defined by the Agency itself. Some Agencies choose to describe their personal information holdings in considerable detail. Others choose to group together similar records **under a single more inclusive description.**

Purpose of the records

This should say what the records are actually used for, not simply that they are used to administer a particular Act. It is however usually desirable to name relevant legislation. If there is more than one use, they should all be listed. An example would be”The purpose of these records is to maintain application details and decisions made under the *Generic Decisions Act 1998*. The records are also used for the compilation of statistics in relation to decisions under the Act”.

General content

For example, “name” or “date of birth” or “employment history” or “educational qualifications” or “complaint details”. Preface with “Content may include”:.

Sensitive content

Examples include “mental health”, “disabilities”, “racial or ethnic origin”, “criminal convictions”, “religious affiliations” “political affiliations”, and “tax file numbers”. Preface with “Sensitive content may include:”.

Classes of people whose personal information is included in the records **(IPP 5.3(c))**

For example, “voters” or “recipients of benefit X” or “temporary employees” or “unsuccessful applicants for licence Y”. If the records relate to more than one class of people, list them all. Preface with “The **personal information** on these records relates to:”.

Internal access

Describes which of the **Agency's** staff, by position or function, are entitled to have access to **personal information** in this class of records. The description should be as specific as possible: words like "staff in relevant areas' are not sufficient. Preface with: 'The following **Agency** staff have access to this **personal information**:'. An example would be "...Regional departmental clerical staff, up to the level of Determining Officer, involved in making decisions under the *Generic Decisions Act 1998*; Regional Managers and appeals staff if a review of a decision is sought".

Period of retention

This should outline for how long the records are kept. For instance, "the records are kept indefinitely" or "the records are destroyed *x* years after action is completed" or "the records are kept for *y* years, then transferred to Australian Archives under Records Disposal Authority *xyz*". **Agencies** should avoid vague forms of words like "the records are retained in line with the Archives Act".

Disclosure

Describes other people or organisations to whom **personal information** from this class of records is usually disclosed. Preface with "Some of this information is disclosed to:" or, if there are no usual disclosures, put "This information is not usually disclosed to other persons or organisations."

Access for people to whom the records relate

Describes how the subjects of the **personal information** held on this class of records can get access to the information about them. This should give the position (preferably the title of the position or the section in which it is located) and phone number, but not the name, of a contact person able to deal with requests for access to **personal information** held in the class of records. Sometimes there may be a different contact officer for each State or for different sub classes of information.

Agencies should follow this form of words: "Individuals can obtain information regarding access to their **personal information** by contacting the [*position*] on [*phone number*], or by writing to [*position and postal address*].

Example of an IPP 5.3 statement

The following is an example of an IPP 5.3 statement for a particular class of records.

Complaint and Investigation Files

The purpose of these records is to record details of complaints, relevant investigation and **Agency** action.

Content may include: name, address, date of birth, occupation, gender, marital status, names and status of partners or relatives and any other type of information dependent on the individual case.

Sensitive content may include: physical or mental health, disabilities, sexual life, racial or ethnic origin, criminal convictions, criminal intelligence, religious affiliations, political affiliations, tax file numbers, relationship details and any other type of information dependent on the individual case.

The **personal information** on these records relates to complainants, respondents, witnesses and authorised agents.

The following **Agency** staff have access to this **personal information**: Senior Executives, Complaints Officers and Records Manager.

The records are kept between 3 years and permanently, depending on the nature of the case.

This information is not usually disclosed to other persons or organisations.

Individuals can obtain information regarding access to their **personal information** by contacting the Privacy Contact Officer.

Common classes of records

As personnel records are common to most **Agencies**, a generic description of personnel records has been developed in order to reduce duplication in the **Personal information** Digest. **Agencies** are free to include this description in their IPP 5.3 statement. When an **Agency** provides its statement to the Privacy Commissioner under IPP 5.4(b), it may simply refer to the generic description, rather than reproducing it.

IPP 5.4 - making available the statement of personal information held

IPP 5.4(a) - making the statement publicly available

Each **Agency** is required by IPP 5.4(a) to make the statement of **personal information** held available for public inspection. This requirement may often be met by making available copies of the **Personal information** Digest, which contains the statement provided by the **Agency** to the Privacy Commissioner each year.

IPP 5.4(b) - giving the Privacy Commissioner a copy of the statement

Section 27(1)(g) of the Privacy Act requires the Privacy Commissioner to maintain, and to publish annually, a record (to be known as the **Personal information** Digest) of the matters set out in records maintained by record keepers in accordance with IPP 5.3.

To allow the Privacy Commissioner to do this, IPP 5.4(b) requires each **Agency** to provide its statement of **personal information** held to the Commissioner in June of each year. The timing of the return is therefore a legal requirement with which all **Agencies** must comply.

Prior to 1997, Digests were published in book form and in the Commonwealth Managers' Toolbox. The Digest is now only available in electronic form (including the Toolbox CD-ROM).

Information Privacy Principle 6

IPP 6, titled ***Access to records containing personal information***, states:

Where a record-keeper has possession or control of a record that contains **personal information**, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Because of the qualification in the second part of the Principle, IPP 6 gives the same right of access to information as is available under the *Freedom of Information Act 1982*. The right of access to **personal information** is an important privacy right, but in its implementation the Privacy Commissioner will generally defer to the FOI administrative machinery. See *Complaints about access* below.

The Freedom of Information Act

The *Freedom of Information Act 1982* is the main piece of Commonwealth legislation dealing with access to documents. Under the FOI Act, an **Agency** must release requested documents (whether or not they contain **personal information**) unless they fall within certain exemption categories. If a record containing **personal information** is an exempt document under the FOI Act, the **Agency** is not obliged by IPP 6 to give the subject of the information access to the record. The FOI Act also authorises **Agencies** not to grant access to some other types of documents - including documents open to public access for a fee, and documents available for purchase. Sections 12 and 13 of the FOI Act set out these categories of documents.

For sources of information about the FOI Act, see *Other sources of information* above.

The Archives Act

The Archives Act is another "law of the Commonwealth that provides for access by persons to documents". When an **Agency** transfers its records to the Australian Archives, the **Agency** continues to the be the "record-keeper" for the purposes of the IPPs (s10(4) of the Privacy Act). Australian Archives acts as custodian of the records.

Normally, records more than 30 years old held by the Australian Archives are open to access by the public. However, the Archives Act provides that some categories of records are exempt from such access (s.33) on similar grounds to the exemptions in the FOI Act. Particular exemptions include information:

- whose disclosure would be a breach of confidence (s.33(1)(d));
- whose disclosure would involve the unreasonable disclosure of information relating to the personal affairs of any person (s.33(1)(g)); and
- whose disclosure would unreasonably affect a person adversely in relation to his or her business, financial or professional affairs (s.33(1)(j)).

For sources of information about the Archives Act, see *Other sources of information* above.

Complaints about access

Because the FOI Act sets up a detailed procedural framework for obtaining access to information, including **personal information**, held by the Commonwealth government, the Privacy Commissioner has not set up separate administrative systems for IPP 6. If an **Agency** receives a request under IPP 6 for **personal information** from the subject of the information, it should deal with it under its normal access processes, which will include, but may not be restricted to, FOI. The FOI Act provides for internal review of decisions to refuse access and for subsequent appeal to the Administrative Review Tribunal.

Section 41(1) of the Privacy Act provides that:

The Commissioner may decide not to investigate or not to investigate further an act or practice about which a complaint has been made under section 36 if the Commissioner is satisfied that:...

(e) the act or practice is the subject of an application under another Commonwealth enactment and the subject-matter of the complaint has been or is being dealt with adequately under that enactment; or
(f) the act or practice could be made the subject of an application under another Commonwealth enactment for a more appropriate remedy.

While each complaint must be considered on a case by case basis, the Privacy Commissioner has generally declined to investigate complaints under IPP 6 where FOI processes have not been exhausted.

Review of the FOI Act

In January 1996, the report of the review by the Australian Law Reform Commission and the Administrative Review Council of the federal Freedom of Information Act was tabled in Parliament (*Open Government: a review of the federal Freedom of Information Act 1982*). The report recommended several amendments to the FOI and Privacy Acts to ensure the continued smooth operation of the overlap between the two Acts in respect of access to, and amendment of, **personal information**. At the time these guidelines were released, the government was still considering the report's recommendations. **Agencies** should bear in mind that future amendments to the Privacy Act or the FOI Act may change the interaction between the two.

Information Privacy Principle 7

IPP 7, titled *Alteration of records containing **personal information***, states:

1. A record-keeper who has possession or control of a record that contains **personal information** shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

   (a) is accurate; and
   (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

(a) the record-keeper of a record containing **personal information** is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and
(c) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

IPP 7 sets out the principle that **Agencies** should take all reasonable steps to ensure that the **personal information** they hold is of high quality. Not only should people have the ability to access **personal information** about them but they should be able to have that information corrected if it is wrong.

IPP 7: Australian citizens or permanent residents

Section 41(4) of the Privacy Act provides:

Where an act or practice may be an interference with the privacy of an individual solely because it may breach Information Privacy Principle 7, the Commissioner shall not investigate the act or practice except to the extent that it is an interference with the privacy of a person who is, or persons each of whom is:

(a) an Australian citizen; or
(b) a person whose continued presence in Australia is not subject to a limitation as to time imposed by law.

This provision applies whether the act or practice has come to the Commissioners' attention through a complaint, or by some other means.

IPP 7.1 and 7.2 - records to be accurate, relevant, up to date, complete, not misleading

The **Agency** is responsible for the quality of the **personal information** it holds. IPP 7.1 requires each **Agency** to take all reasonable steps to ensure that the **personal information** it holds is accurate and, given the purpose of the information, is relevant, up to date, complete and not misleading. It is therefore the responsibility of each **Agency** to ensure that the **personal information** it holds is of high quality.

These are continuing obligations. An **Agency** must take *reasonable* steps to ensure the quality of the **personal information** it holds throughout the period it holds the information, not just when the information is collected.

Reasonable steps

Reasonable steps include correcting deficiencies in data quality that are brought to an **Agency's** attention, but will also usually include some proactive measures. In deciding what steps are reasonable to ensure the quality of the data, an **Agency** should consider the following matters.

How likely it is that the information is of high quality.

This will usually depend on the original source of the information and on any checks done since the **Agency** obtained the information. If the information is not likely to be of high quality, for example, if it is has been provided anonymously, more checking would be reasonable.

What the information may be used for.

If significant decisions may be made on the basis of the information, it is more important to make sure it is of high quality.

What consequences could follow if inaccurate information is used.

If the consequences of holding low quality information are serious, for the subject of the information, or the **Agency**, or for a third party, more thorough checks are likely to be reasonable.

The cost or difficulty of available steps to ensure accuracy.

If it is cheap and easy to check the information being held, then it would usually be a reasonable step to do so. If checks are very costly, they are likely to be reasonable only if the information is of low quality or the consequences of holding wrong information are serious.

Accurate

An **Agency** is obliged to make whatever corrections, deletions and additions are reasonable to make sure the record is accurate. "Accurate" means factual accuracy. It is difficult to ensure the accuracy of non factual **personal information** like evaluative reports, though the status and origin of non factual **personal information** must be clear (see "Not misleading" below). "Accurate" also means accurate at the time to which the information relates. Whether or not Ms X marries later, Ms X has never married remains accurate provided the time reference of the statement is clear. (See Up to date below.)

Unlike the requirements in IPP 7.1 to ensure **personal information** is relevant, up to date, complete and not misleading, the requirement to ensure accuracy is not qualified by the words "having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose". An **Agency** has an obligation to ensure that the **personal information** it holds is accurate, regardless of the actual or intended use of the information.

Relevant

Personal information that an **Agency** holds must be relevant to the purpose for which it was collected or is to be used (or to a directly related purpose). Strict adherence to IPP 3(c), which requires that an **Agency** take all reasonable steps to ensure that **personal information** collected is relevant to the purpose of collection, will help **Agencies** avoid a risk of breaching IPP 7.1.

It would not usually be a reasonable step for an **Agency** to try to edit every piece of **personal information** it holds as relevance shifts over time. However there are some circumstances where an **Agency** may put itself at risk of holding irrelevant **personal information**.

An example is when information is collected for statistical purposes. It may be important that the data be identified in the initial phase when returns are being checked. But once this has been done, the identifying details may no longer be relevant to the data's longer term statistical uses. If personal identifiers are attached to records kept *only* for statistical purposes, the **Agency** may be at risk of breaching IPP 7.

Up to date

This requirement applies to **personal information** which would be taken by a user to reflect the current characteristics of a person. If for example an **Agency** holds information about a person?s *current* marital status, it must take all reasonable steps to ensure that the information is up to date. But date-specific statements do not go out of date. For example, if an **Agency** holds accurate information about a person?s marital status *at a particular point in time*, the **Agency** will not usually have to take any further steps to comply with IPP 7.

In deciding what are reasonable steps to ensure that the **personal information** it holds is up to date, the **Agency** should consider the type of information concerned. For example, a person?s date of birth does not become out of date, but other personal details will change over time.

Complete

An **Agency** must take all reasonable steps to ensure that the **personal information** it holds is complete, given the purpose for which it was collected or is used. That is, **personal information** should not leave out important facts that could have an impact on the way the **Agency** uses it.

An example would be if a person is charged with a criminal offence and acquitted. If an **Agency** records only that the person has been charged, the information is not complete, and may suggest that the person was guilty.

In practice, an **Agency** must balance its obligation to make sure the information it holds is complete with its obligation to ensure that the information it holds is relevant. **Agencies** should not include every available piece of **personal information** in its records simply for the sake of completeness.

Not misleading

An **Agency** must do everything it reasonably can to make sure that, given the purpose of the **personal information**, the information is not misleading. That is, **personal information** must not misinform the reader, either intentionally or unintentionally; lead to wrong impressions; or be likely to be misinterpreted.

Particular care should be taken with subjective opinions, which while sometimes necessary, should be clearly identified as such, and should not be presented as objective fact. The source of the opinion and the evidence on which it is based should be part of the information.

Agencies should also where possible consider the likely users of the **personal information**. Information should be robustly presented; technical terms should be defined; sources should be quoted; and information should whenever possible be clearly labelled and dated.

Applications for amendment

Sometimes the **Agency** will believe that **personal information** it holds is accurate, relevant, up to date, complete and not misleading, but the subject of the information will disagree and ask the **Agency** to change, delete or add to the information in some way. A reasonable step in terms of IPP 7.1 if for the **Agency** to then consider whether some change needs to be made to the information. The request may or may not follow access to the record and this access may or may not have been under the FOI Act. The **Agency**’s obligations are independent of these matters.

Most amendment applications should be dealt with under the FOI Act

In most cases, an application for amendment of **personal information** by the subject of the information should initially be dealt with under the FOI Act or other relevant administrative processes. This is because the FOI Act and **Agency**-specific regimes set out detailed guidelines for dealing with requests for access or correction, so using these processes avoids unnecessary administrative duplication and complexity. But this is a matter of good administration rather than a legal obligation.

Note that even if the **Agency** is not obliged to change the record under the FOI Act, it may still be required by Part V of the FOI Act to attach to the record a statement of the amendment requested.

The Privacy Act includes some additional amendment rights

Under the Privacy Act the right to have records amended is slightly broader than the corresponding right under the FOI Act. There are therefore some situations in which applications for amendment must be dealt with from the outset under IPP 7, rather than the FOI Act. Three such situations are described in the following paragraphs.

The first is where the amendment is sought on the grounds that the information is irrelevant. Part V of the FOI Act provides for amendment and annotation of records containing **personal information** that is incomplete, incorrect, out of date or misleading. Unlike IPP 7, the FOI Act does not provide for the amendment or annotation of irrelevant information.

The second is where a person seeks deletion of **personal information**. Part V of the FOI Act provides for amendment or annotation of a document, but not for deletion except where it is impossible to avoid. A request to delete information from a document must therefore be dealt with under IPP 7, which says that an **Agency** should take reasonable steps "by way of making appropriate corrections, deletions and additions".

The third is where a person seeks amendment of **personal information** in a record to which he or she has not been provided lawful access. The FOI Act (s.48) restricts a person's correction rights to a document of an **Agency** or an official document of a Minister to which access has been lawfully provided to the person, under the FOI Act or otherwise.

The Privacy Act contains no such restriction, and section 35 of the Privacy Act clearly envisages that a person may complain to the Privacy Commissioner if an **Agency** fails to amend a document to which the person has not been provided lawful access (see *Section 35 of the Privacy Act* under IPP 7.3 below).

IPP 7.2 - restrictions on Agency obligations to amend personal information

Under IPP 7.2, the obligation in IPP 7.1 to amend **personal information** is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

The FOI Act is the main Commonwealth law that provides such a right. It places a number of limitations on a person's right to have records amended:

- the person must have been provided with lawful access to the document (s.48);
- the document must have been used, be being used or be available for use for an "administrative purpose" (s.48(b));

- the person must apply in writing (s.49(a));
- the application must specify, as far as practicable which document is sought to be amended, which information in the document they want amended, whether the information they want amended is incomplete, incorrect, out of date or misleading (but not irrelevant), why they think this, and what amendment they want made (s.49(b));
- the application must be sent by post or hand delivered and must specify a return address in Australia (ss.49(c) and (d));
- so far as practicable, the **Agency** must amend the document in a way that does not obliterate the text as it stood before the amendment (s.50(3)) - ie, not delete where that is avoidable.

The Privacy Commissioner regards these limitations as qualifying an **Agency**?s obligation under IPP 7.1, except in situations such as those outlined above, where the request for amendment falls outside the FOI Act, but within IPP 7.

Delete, amend or add?

If an **Agency** decides, either on its own initiative or on the request of the subject of the information, that a record needs to be changed in some way, it must decide whether to delete the record, amend it or add to it.

Where possible, an **Agency** should generally retain both the old information - while clearly marking it as no longer current - and the new information; and should record the date and reason the old information was superseded. This allows the **Agency** to trace changes made to the information for audit purposes, and is useful when reviewing decisions made using the information, or dealing with complaints or enquiries related to it.

There may however be some particularly sensitive cases in which the mere existence of the earlier incorrect information could be detrimental. In such cases, deletion may be the only appropriate option. It is essential if information is deleted that a notation is made of the reason for the deletion, and the officer responsible for the decision.

IPP 7.3 - recording requests for correction, deletion or addition

Under IPP 7.3, if

> a person asks an **Agency** to change (by correcting, deleting or adding to) **personal information** it holds about him or her; the **Agency** does not wish to change the information; and the **Agency** is not obliged to change the information by any Commonwealth law (mainly the FOI Act);

then the **Agency** must take all reasonable steps to attach to the **personal information** a statement by the person of the change he or she has asked for.

If a person asks an **Agency** to change **personal information** and the **Agency** does not wish to make the change, the **Agency** should first consider whether the FOI Act obliges it to make the change. If it does, the **Agency** must make the change and by doing so it will have discharged its responsibility under IPP 7.3.

If it does not, the **Agency** should consider whether it is obliged by the FOI Act (sections 51 to 51E) to attach a statement from the person. If it is obliged to do so, it should attach a statement and by doing so it will have discharged its responsibility under IPP 7.3. If it is not obliged to do so, the **Agency** should consider the request under IPP 7.3.

There will be situations where the **Agency** is not obliged by the FOI Act, but is obliged by IPP 7.3, to attach a statement from the person:

- Where the person has asked for an amendment on the grounds that the information is irrelevant, which is allowed under IPP 7.1 but not under the FOI Act (see under IPP 7.1 above).
- Where the person has asked for an amendment by way of deletion, which is allowed under IPP 7.1 but not generally under the FOI Act (see under IPP 7.1 above).
- Where a person seeks amendment of **personal information** in a record to which he or she has not been provided lawful access (see s.48 FOI Act).
- Where person has made a request for amendment that does not satisfy the technical requirements of s.49 of the FOI Act (see IPP 7.2 above) but does satisfy IPP 7.3.

The Privacy Act imposes no such conditions on requests for annotation. Note that an **Agency** can add its own comments or annotations to a statement attached to a record under IPP 7.3.

How to annotate personal information held on a database

There are a number of options for making annotations to information held in a database. The preferred one is for the statement provided by the person to be directly attached to the relevant information in the database. Other options are for the statement to be included in a field in the particular record, such as a free text comments field, or in a separate file of comments linked to the principal database. The least convenient option would be for the record in the database to be flagged to indicate that a statement provided by the person is associated with the record, and where that statement is to be found.

The important thing is that it should be clear to anyone accessing the information that it has been disputed, on what grounds it has been disputed, and why the **Agency** has decided not to correct, delete or add to the information as the person asked.

Section 35 of the Privacy Act

Section 35 states:

(1) Where:

(a) an application made under subsection 55 (1) of the Freedom of Information Act 1982 for review of a decision under that Act refusing access to a document has been finally determined or otherwise disposed of;
(b) the period within which an appeal may be made to the Federal Court has expired or, if such an appeal has been instituted, the appeal has been determined;
(c) the effect of the review and any appeal is that access is not to be given to the document;
(d) the applicant has requested the **Agency** concerned to amend the document;
(e) the applicant has complained to the Commissioner under this Act about the refusal or failure of the **Agency** to amend the document;
(f) the Commissioner has, as a result of the complaint, recommended under subsection 30(3) of this Act that the **Agency** amend the document, or amend a part of the document, to which the applicant has been refused access; and
(g) as at the end of 60 days after a copy of the report containing the recommendation was served on the **Agency**, the Commissioner:

(i) still thinks that the **Agency** should amend the document in a particular manner; and
(ii) is not satisfied that the **Agency** has amended the document in that manner;

> the Commissioner may direct the **Agency** to add to the document an appropriate notation setting out particulars of the amendments of the document that the Commissioner thinks should be made.

(2) An **Agency** shall comply with a direction given in accordance with subsection (1).

In other words, if:

- a person has pursued all available channels under the FOI Act to get access to a document, without success;
- the person has asked the **Agency** to amend (correct, delete or add to) the document and the **Agency** has not done so;
- the person has complained to the Privacy Commissioner (under IPP 7.1) about the **Agency** not amending the document;
- the Privacy Commissioner has investigated the complaint and recommended that the **Agency** amend the document; and
- 60 days after making the recommendation, the Privacy Commissioner is not satisfied that the **Agency** has amended the document;
- the Privacy Commissioner can direct the **Agency** to annotate the document, setting out the amendment the Commissioner has recommended. The **Agency** is legally obliged to comply.

This section ensures that even if a person cannot gain access to a document concerning them under the FOI Act and cannot succeed in getting the **Agency** to amend the document, the Privacy Commissioner can still require the **Agency** to annotate the document setting out the amendments that the Commissioner thinks appropriate. In practice it is rarely used. Requests for amendment which have the Privacy Commissioner's support are usually resolved without resort to this formal process.