

> Short Guide to the Information Privacy Principles

December 2006



Office of the
Victorian Privacy
Commissioner

Privacy Victoria
Level 11
10-16 Queen Street
Melbourne Victoria 3000
Australia

GPO Box 5057
Melbourne Victoria 3001
Australia

| | |
|------------|-----------------|
| Telephone | +61 3 8619 8719 |
| Local Call | 1300 666 444 |
| Facsimile | +61 3 8619 8700 |
| Local Fax | 1300 666 445 |

www.privacy.vic.gov.au
enquiries@privacy.vic.gov.au



Office of the
Victorian Privacy
Commissioner

Copyright © Office of the Victorian Privacy Commissioner, 2006

The material included in this publication is designed to give general guidance only. It should not be relied on as legal advice. The Office of the Victorian Privacy Commissioner accepts no liability for loss or damage that may be suffered by any person or entity that relies on information in this publication. No liability is accepted for any information or service which may appear in any other format. Copyright is owned or controlled by the Office of the Victorian Privacy Commissioner unless otherwise indicated. Copyright in materials from third parties may be owned by others. Permission to reproduce their work should be separately sought.

Privacy Victoria wants people to have easy access to information about privacy. The contents of this publication may be copied and used for non-commercial use. The material should be used fairly and accurately and this publication acknowledged as the source. The authors of material, where known, should be credited, consistent with the moral rights provision of copyright law.

Table of contents

| | |
|----------------------------------------------------|----|
| About the Short Guide | 4 |
| Where else to look for help | 5 |
| Distinguishing privacy from related concepts | 7 |
| Key concepts | 8 |
| | |
| Principle 1: Collection | 11 |
| Principle 2: Use and Disclosure | 16 |
| Principle 3: Data Quality | 24 |
| Principle 4: Data Security | 26 |
| Principle 5: Openness | 30 |
| Principle 6: Access and Correction | 32 |
| Principle 7: Unique Identifiers | 37 |
| Principle 8: Anonymity | 40 |
| Principle 9: Transborder Data Flows | 42 |
| Principle 10: Sensitive Information | 46 |

About the Short Guide

The Guidelines to the *Information Privacy Principles, Ed. 02* ('the Guidelines') published in September 2006 deal with the interpretation and application of the Information Privacy Principles (IPPs) in the Victorian *Information Privacy Act 2000* (IP Act).

The Guidelines are intended for people working with the IPPs in the IP Act. The IPPs are relevant for all Victorian public sector employees, including those from Victorian government departments, local councils, statutory offices, government schools, universities and TAFEs.

This *Short Guide* is intended as a quick summary of the major points discussed in the Guidelines. It also contains information on what additional information can be found in the Guidelines.

For comprehensive guidance about the IPPs, the Guidelines should be consulted, not this *Short Guide*.

Where else to look for help

To assist the Victorian public sector to comply with the IP Act, the Office of the Victorian Privacy Commissioner (OVPC) publishes a range of publications in hard copy and electronically at www.privacy.vic.gov.au. These publications include:

- information sheets;
- case notes;
- guides
- reports;
- audit reports;
- submissions; and
- free training materials.

The website also contains links to other privacy regulators and relevant agencies. The Guidelines refer to relevant case notes and other material published by these other regulators and agencies throughout the text.

OVPC's training program has been developed to assist Victorian public sector organisations to inform staff of the requirements of the IP Act. The program includes:

- generic privacy training materials;
- introductory, advanced and train-the-trainer sessions at OVPC; and
- on-site training sessions for organisations across Victoria.

Most training services are provided free of charge to organisations subject to the *Information Privacy Act*. Email training@privacy.vic.gov.au or telephone 1300 666 444 for more information.

Whether Guidelines are legally binding

The IP Act (and the IPPs in the Schedule to the Act) became enforceable from 1 September 2002.

Under the IP Act, the Privacy Commissioner has the power to issue guidelines and provide advice on the operation of the IP Act and the IPPs. The Guidelines are not legally binding, and do not constitute legal advice about how organisations are to comply in specific circumstances. They are intended to indicate how the Privacy Commissioner interprets and applies the IPPs. The Guidelines indicate the matters the Privacy Commissioner may consider when advising organisations during consultations, when examining acts and practices during an audit, when dealing with complaints, or when conducting an investigation into an apparent breach of the IPPs.

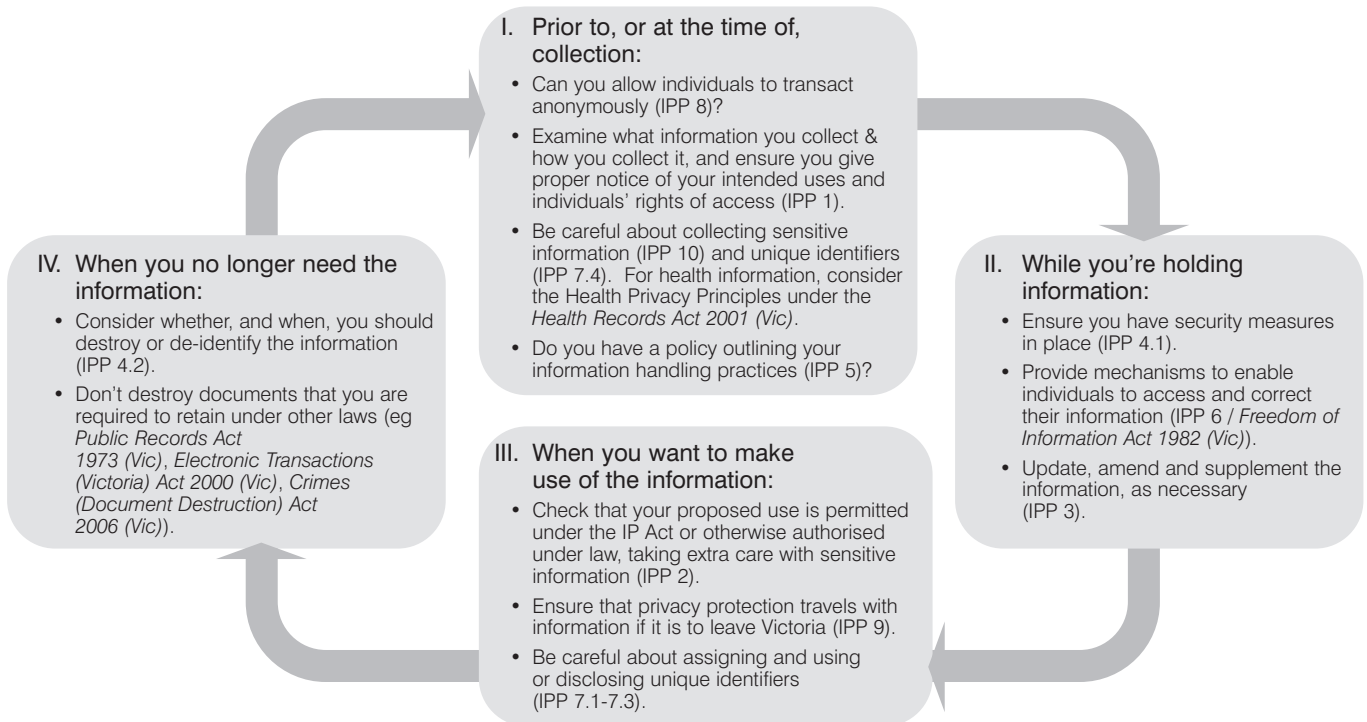
The Short Guide and the Guidelines may be updated electronically from time to time, and will be available on the Office's website (www.privacy.vic.gov.au).

Compliance with the IPPs and the Act is ultimately up to each organisation. Organisations should consult their privacy officer or unit as required, and may wish to seek independent legal advice where appropriate. Officers from the Office of the Victorian Privacy Commissioner are available to take enquiries and provide guidance (tel. 1300 666 444).

Considering the IPPs in context

In practice, the IPPs often interact. In dealing with them in the context of the IP Act, it is better to assemble the facts of a case, identify the issues that those facts seem to raise, and then work through the IPPs to consider which apply and how.

Having an understanding of the particular data, laws and practices relevant to the information flows places you in a better position to assess how your organisation can comply with the IP Act.



Objects of the IP Act

The IPPs should be applied with the objects of the IP Act (section 5) in mind. They are:

- a to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;
- b to promote awareness of responsible personal information handling practices in the public sector; and
- c to promote the responsible and transparent handling of personal information handling in the public sector.

National consistency

In May 1998, Ministers from across Australia (including Victoria) agreed to adopt the National Fair Handling Principles as the basis for a national benchmark. The Victorian IPPs were adapted from these Principles.

Accordingly, in applying the Victorian IPPs, organisations may wish to consider how other jurisdictions have interpreted like privacy principles that were similarly based on the National Fair Handling Principles. Caution must of course be exercised where the wording and application of these principles differ, and where a contrary or inconsistent view has been expressed in Victoria – whether by the Victorian Privacy Commissioner or by a court or tribunal interpreting the Victorian law.

Distinguishing privacy from related concepts

Privacy and confidentiality

Confidentiality is a concept that is related to, but different from, privacy. An obligation of confidence is generally owed by the recipient of information to the provider of the information. Privacy is the right of the subject of the information, no matter who provided and who received the information. Confidentiality often deals with information other than personal information. Confidentiality is about controlling the disclosure of information, while privacy obligations go wider to encompass collection, quality and disposal.

The IP Act will not override a duty of confidence, nor will IPP 2 (use and disclosure) provide any authority for disclosure of information that is already required to be held in confidence.

Privacy and secrecy

Governments and corporations may have secrets, but not privacy. Privacy is a condition for individual human beings. Privacy is a human right and longstanding societal value.

Governments may use secrecy to serve other public interests, such as: protection of national security; integrity of law enforcement investigations; and facilitation of “frank and fearless” advice, including contending and controversial options, prior to final decision.

The IP Act and IPPs should not be administered by the public sector in such a way as to avoid legitimate scrutiny and accountability or to impede the free flow of information in ways not required by the IP Act to protect the public interest in privacy.

Information privacy and FoI

FoI and privacy laws differ in three important ways:

- a FoI is fundamentally about compelling disclosure. Privacy compels discretion.
- b Under FoI, every person has a legally enforceable right to seek access to documents held by government, whether or not the documents relate to the requester. Privacy only confers a right of access on the person who is the subject of the personal information. FoI includes mechanisms for addressing the privacy of third parties whose information is about to be disclosed to a requester.
- c FoI deals mostly with access and correction. Privacy is wider and more subtle, also addressing collection, use, storage, quality, sharing and disposal of personal information.

The interaction of FoI and privacy, and the operation of the Access and Correction Principle, is discussed further in the Guidelines under IPP 6.

Key concepts

The IP Act and the IPPs use some key words and phrases. Your starting point for interpreting words and phrases is section 3 of the IP Act. If the word or phrase is not defined, then the next checkpoint is the dictionary to find the word's ordinary, everyday meaning. In some cases, the meanings of key terms are considered by tribunals and courts, and case law should be consulted as appropriate.

Personal information

If the information you are dealing with does not fall within the definition of “personal information” in section 3 of the IP Act, then the IP Act and its IPPs do not apply.

The definition of personal information is:

information
or an opinion
(including information or an opinion forming part of a database),
that is recorded in any form
and whether true or not,
about an individual
whose identity is apparent,
or can reasonably be ascertained
from the information or opinion
but does not include information of a kind to which the *Health Records Act 2001* applies.

Health information

The *Health Records Act 2001* (Vic) protects the privacy of health information. Health information is also part of the Commonwealth *Privacy Act's* definition of sensitive information.

Living natural persons

The IP Act defines “individual” to mean a natural person. Corporations and other types of “legal persons” do not have privacy rights under the IP Act, only humans do.

The IP Act protects the privacy of living persons only, not deceased persons. Bear in mind, however, that information about a deceased person may include personal information about the living.

Recorded

Unlike the *Health Records Act 2001* (Vic) and the federal *Privacy Act 1988*, the IP Act requires personal information to be “recorded”.

The Act will apply to conversations about information that has already been recorded, as well as to conversations that are subsequently recorded (eg, where notes are made of the discussion).

In any form

The definition of personal information is very broad. Personal information need not be merely words on paper. It may be in stored messages (such as email and voicemail), captions on screens or in posters or other signage, images (especially photos), sounds or be latent in a material item but reasonably ascertainable (eg, DNA in human tissue).

Whether identity is apparent or can be reasonably ascertained

Whether an individual's identity is apparent or can reasonably be ascertained will depend on both the information and the circumstances in any given case.

In examining whether identity is apparent or may reasonably be ascertained, it is appropriate to consider how information from other sources may be used in conjunction with the recorded information or opinion to ascertain identity. Consider whether identity can reasonably be ascertained, not whether anyone – the organisation holding it or a third party – intends to try.

The definition of personal information is very broad. When in doubt about whether information fits the definition, err on the side of treating information as personal information and turn your mind to the IPPs.

Consent

The concept of consent is central to privacy.

Consent is not pre-eminent as a basis on which information can be collected, or used. The IPPs include provisions for non-consensual collection and uses/disclosures. Consent is of particular utility to agencies to satisfy both their own information needs and their obligations under the IP Act. If you need to use or disclose someone's personal information, it may be easiest to simply ask for his or her consent to do so.

Elements of consent

The essential elements of consent are that the:

- individual has the **capacity** to consent;
- consent must be **voluntary**;
- consent must be **informed**;
- consent must be **specific**; and
- consent must be **current**.

These elements are discussed in the Guidelines. Assessing these factors will depend on the circumstances of each case.

Capacity

An individual may not be capable of giving consent. Age or physical or mental disability may prevent the person communicating. He or she may not understand the general nature and effect of giving or withholding consent. If you are uncertain that the person has capacity, do not rely on any purported consent.

Capacity to consent (under IPPs 1, 2 and 9) and to make access and correction requests (under IPP 6) is addressed in section 64. Where a person is incapable of consenting or making a request for access or correction, an authorised representative may do so on his or her behalf.

Voluntary

An individual must be free to exercise genuine choice. Consent must be given without coercion or threat and with sufficient time to understand the request and, if appropriate, obtain advice. Giving "notice" that a collection, use or disclosure is to occur is not the same as obtaining "consent".

Informed

The individual must have full knowledge of all relevant facts, including:

- a the personal information to be collected or used or disclosed;
- b the purpose or purposes it will be put to;
- c who will get the information, to whom it may be passed on, and what use the recipient(s) will make of the information;
- d the consequences of giving consent, or of failing to give consent.

Specific

Consent must be specific enough in all the circumstances. If the information given is too broad or vague, the consent may not be specific enough to be regarded as valid consent for the particular use or disclosure the organisation makes.

Generally, the more privacy-invasive the proposed use or disclosure, the more specific the required information and consent should be.

Current

Consent has a use-by date. Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely.

Purpose

The purpose of an action is the reason for which it is intentionally done.

Unless you know what the organisation intends to do with the personal information it collects, you cannot readily assess or assert its necessity (IPP 1.1) or even perhaps its lawfulness and fairness (IPP 1.2).

Determining the purpose also helps you to ascertain the required standard of data quality (IPP 3) and whether additional steps should be taken to secure the data (IPP 4.1).

Necessary

“Necessary” does not mean unavoidable, essential or indispensable. What is clear is that “necessary” requires more than what may be administratively convenient or desired.

Reasonable, reasonably

To be reasonable is to be fair, proper and moderate. A reasonableness test implies the application of reasoned and objective judgment to the circumstances. It implies taking a balanced view.

Practicable

“Practicable” connotes an element of reason and prudence. Practicable means capable of being done, feasible. When the reasonableness or practicability of doing something is at issue, cost is one consideration but it is not the only one or even the primary one.

The Guidelines also discuss:

- Examples of personal information
- Anonymised, de-identified & coded information
- Distinguishing sensitive information from delicate information
- Bundled consents
- Implied consent
- Opting in vs. opting out of direct marketing
- Function creep

Principle 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) to whom (or the types of individuals or 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 IPP 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.

Collection is a fundamental part of the IP Act and goes to the heart of information privacy protection. It is essential that organisations get it right.

The first steps should always be, “what information do you need to carry out your function or activity?”, “can you achieve your purpose without collecting personal information?” and “can the information be anonymous or de-identified?”

The best privacy safeguard is to not collect what you do not need. If you unnecessarily collect personal information, you will then have to comply with all the other IPPs in relation to that information.

The purpose of collection governs use and disclosure (IPP 2) which starts from the assumption that information is used/disclosed for the primary purpose it was collected.

IPP 10, on collection of sensitive information, supplements IPP 1, and the two are best considered together. IPP 10 is intended to provide safeguards additional to IPP 1 by limiting the circumstances in which sensitive information is collected.

Broadly put, the basic standards are:

- a Collect only what you need.
- b Do it lawfully, fairly, directly and not unreasonably intrusively.
- c Tell people you are doing it and why.

Information collected prior to 1 September 2001

The collection principles (IPP 1 and 10) do not apply to information already collected by organisations prior to the IP Act coming into force (1 September 2001). In contrast, the other IPPs do apply to information already held at that date.

Unsolicited personal information

The IPPs will apply to personal information, whether solicited or not.

The receipt of unsolicited information may trigger the notice requirements in IPPs 1.3 and 1.5, even though the organisation may not intend to use the information about the sender or any third party referred to in the unsolicited communication. However, in some cases, it may be reasonable not to give notice.

IPP 1.1: Necessary for one or more function or activity

IPP 1.1 prohibits organisations from collecting personal information unless the information is necessary for one or more of the organisation's functions or activities.

Necessity

Necessity will be assessed in a practical way. Does the organisation need the personal information in order to discharge the function effectively? Consider whether anonymous information would be sufficient. Can the function be discharged through anonymous transactions?

The collection should be for a specific purpose and the type and extent of information collected should be limited to what is necessary to achieve that purpose (that is, carry out that activity or function).

Function or activity

In state and local government, functions and activities often have a basis in law. An organisation's functions or activities may be specifically listed in the statute that established the organisation. The functions or activities may be broadly expressed in statute, but more refined in regulation, Ministerial Directive or other sources.

Be as clear and specific as possible about the function or activity that the information is needed for – both in your own mind and for the individuals from whom you are collecting information.

IPP 1.2: Lawful, fair, not unreasonably intrusive

IPP 1.2 requires that collection must be by lawful and fair means and not in an unreasonably intrusive way.

Lawful

Collection must be according to law and not contrary to law. This includes criminal and civil law, statute and common law.

The IP Act will not permit collection of information where that collection is prohibited by another law.

IPP 1.2 may also be breached where an organisation lacks power or authority under law to collect personal information or exceeds its power.

Fair

Information may be regarded as having been obtained unfairly where it was collected by trickery or deception or under duress.

In drafting forms, organisations should take care to distinguish compulsory information (required by law to be provided) from other information which is not compulsory to be provided but which the organisation regards as necessary. Organisations should remember that information can be provided by consent, but they should indicate to individuals when provision of information is optional.

It may also be unfair collection if you misrepresent what will be done with the information once collected, such as claiming the information will be treated securely and confidentially when it is intended or proposed that the information be passed on to others.

Similarly, it may be unfair if you initiate monitoring or collection of information for one purpose, giving assurances or undertakings that the information will not be used for any (or certain specified) purposes, and then make such a use/disclosure, especially where:

- a individuals might have objected to the collection had they known its eventual use;
- b less intrusive alternatives were available but had not been considered; or
- c additional safeguards would have been sought in respect of the secondary use.

It is vital to ensure your collection notices (IPP 1.3) and privacy policies reflect your intention when you collect information (see IPP 5).

Collecting information or monitoring individuals without notice and without their consent or knowledge, as in the case of covert surveillance, will be regarded as unfair in most circumstances. There are some situations in which the use of covert surveillance may be justified and not considered unfair, depending on how it is conducted.

Not unreasonably intrusive

In practice, it will often be the case that there are only fine distinctions to be made between a collection that is unnecessary (IPP 1.1) and a collection done in an unreasonably intrusive way (IPP 1.2).

To illustrate this point, a collection may be unreasonably intrusive where excessive or unnecessarily intimate information is collected, or where the collection occurs in a manner that unnecessarily intrudes into a person's home life or unreasonably interferes with a person's bodily integrity. Much will depend on the context and the need that is said to underpin the collection.

The phrase "unreasonably intrusive way" in IPP 1.2 focuses the mind on the method used to collect information, and the necessity test in IPP 1.1 focuses minds on the type and on the amount of information collected.

IPP 1.3: Collection notices

When collecting personal information, IPP 1.3 requires organisations to take reasonable steps to make individuals aware of the following matters:

- a the identity of the organisation and how to contact it;
- b the fact that he or she may access that information;
- c the purposes for which the information is or was collected;
- d the names (or types of) organisations or individuals to whom the information is usually disclosed;
- e any law requiring the collection; and
- f the main consequences (if any) if the person does not provide any or part of the information sought.

IPP 1.3(c): Purposes of collection

IPP 1.3(c) requires organisations to inform individuals of the purposes for which information is collected.

The primary purpose will be what is strictly necessary to discharge the function or undertake the activity. The primary purpose needs to be clearly stated and must be more specific than a general reference to some broad power.

If secondary purposes are known in advance, they too should be explained to the subject.

IPP 1.3(d): Usual recipients of the information

IPP 1.3(d) requires the organisation to ensure individuals are aware of the individual or organisation, or the types of individuals or organisations, to whom the information is usually disclosed.

When you collect personal information with the intention of publishing it or disseminating it (eg, online), you should make this intention clear at the time of collection. Where lawful and practicable, consider offering individuals an opportunity to restrict the publication of their details, such as where they are concerned that disclosure may pose a risk to their personal safety.

IPP 1.3(e): Compulsory collection

Where government has the power compulsorily to obtain information, that should be made clear to the person. The notice statement should specify which law is being invoked as a basis for collection.

IPP 1.3(f): Consequences for individuals who do not provide their information

IPP 1.3(f) requires organisations to give notice of the main consequences (if any) for the individual if they do not provide all or part of the information being collected. Organisations should be careful not to overstate the consequences for individuals who do not provide all or part of the requested information

IPP 1.4: Direct collection

IPP 1.4 requires organisations to obtain information about an individual only from the individual, where it is lawful and practicable to do so.

Nevertheless, there will be many circumstances where it would not be practicable to collect information directly from the individual. As a result of indirect collection, organisations may end up collecting a considerable amount of information about individuals without those individuals' knowledge.

In many circumstances, particularly where the information can be used to affect their interests, these third parties should be given notice that their information has been collected, that they can find out what is known about them, and that they can be informed about where their information will flow. That is what IPP 1.5 requires.

IPP 1.5: Notice of indirect collection

IPP 1.5 requires organisations to take reasonable steps to make an individual aware of the matters in IPP 1.3 if they collect personal information from someone else, unless to do so would pose a serious risk to the life or health of any individual.

The Guidelines also discuss:

- Timing for giving notice
- Form of notice
- Multi-layered (or “short”) notices
- Distinguishing notice statements from privacy policies
- Optional information
- Consequences for individuals who do not provide their information
- “Reasonable steps” for giving notice (including where information is unsolicited or indirectly collected)
- Automated collection

Principle 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 use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual –
 - (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
 - (ii) in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the information; or
 - (d) 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, safety or welfare; or
 - (ii) a serious threat to public health, public safety, or public welfare; or
 - (e) 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
 - (f) the use or disclosure is required or authorised by or under law; or
 - (g) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency –
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;
 - (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;
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
 - (h) the Australian Security Intelligence Organization (ASIO) or the Australian Secret Intelligence Service (ASIS), in connection with its functions, has requested the organisation to disclose the personal information and –
 - (i) the disclosure is made to an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) to receive the disclosure; and

- (ii) an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) for the purposes of this paragraph has certified that the disclosure would be connected with the performance by ASIO or ASIS (as the case requires) of its functions.

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

The basic rule of IPP 2.1 is relatively straightforward: Use and disclose personal information only for the primary purpose. But there are eight other instances where uses or disclosures might be permitted beyond the primary purpose. These are contained in IPPs 2.1(a)-(h).

Distinguishing “use” from “disclosure”

The word “use” is to be interpreted broadly in relation to personal information, especially in light of technological developments. To “disclose” is to reveal.

Oral disclosure of recorded information

The IP Act will apply to oral disclosures of personal information as long as the information in question exists or existed at one time in a recorded format, including but not limited to visual formats.

Disclosure by allowing others to view information

Personal information can be disclosed even though it remains in the possession or control of its original collector. It is possible to disclose information by permitting a person to read the material displayed on a computer screen.

Intra-organisation uses and disclosures

Entities within the Victorian public sector should not assume that, because one part of the organisation collected some personal information, the collecting part can disclose to any of the other parts and the recipient parts can use, without regard for IPP 2.

In the case of large public sector agencies consisting of specialised units, the exchange of personal information between units may constitute disclosure.

Every disclosure by one body will constitute a collection by the recipient body. Organisations, and entities within a departmental portfolio, should ensure that they comply with both IPPs 1 and 2 when sharing information.

IPP 2.1: Primary purpose

Primary purpose governs primary use and primary disclosure.

In general, information should only be used in accordance with the primary purpose for which it was collected, or otherwise by consent. Information may also be used or disclosed for related secondary purposes that are reasonably expected, and for purposes for which a sufficiently strong public interest exists.

Using compulsorily acquired information – the general principle

In general, where an organisation has statutory powers to compel the provision of information to it, it should not disclose that information except for the purposes for which the powers were conferred or where otherwise required by law.

Where the statute or regulations conferring the compulsory powers provides clear authority for certain uses or disclosures, then the IP Act permits them.

IPP 2.1(a): Reasonably expected related secondary purposes

Personal information can be used and disclosed for purposes secondary to the primary purpose and related to it. Secondary purposes for use and disclosure must be related (or, in the case of sensitive information, directly related) to the primary purpose of collection and consistent with what an individual would reasonably expect.

Related secondary purposes

The secondary purpose for which the information is used or disclosed has to be connected to or associated with the primary purpose. It must relate to the primary purpose for which it was collected. If sensitive information is involved, the secondary purpose has to be directly related to the primary.

Reasonably expected

The test used for interpreting reasonable expectation is an objective one. It is the reasonable expectation of an ordinary person, who is not necessarily expert in the workings of government, that is to be considered in the particular circumstances

A secondary use or disclosure might be reasonably expected where that use or disclosure is “inextricably linked” to the primary purpose of collection.

Limiting disclosure to what is sufficient

When disclosing under IPP 2.1(a), the amount of information disclosed should not exceed what is sufficient to satisfy the related secondary purpose. Excessive disclosure is not reasonably expected.

Using notices to build an expectation

Notice statements outlining the secondary purposes for which the information is to be used or disclosed, given at or prior to the time of collection (under IPP 1.3), can assist in creating an expectation that information is to be used for related secondary purposes. However, more may be required to establish that the secondary use is “reasonably” expected. Notice cannot be used to override other existing legal obligations (such as a duty of confidentiality). Reasonableness requires that the related secondary use or disclosure is also proper and fair, and generally not incompatible with the primary purpose of collection

IPP 2.1(b): Consent

Consent is one of the exceptions to the basic rule that primary purpose governs use and disclosure. Where an individual has consented to other uses or disclosures, including unrelated or even incompatible ones, an organisation may use or disclose the personal information accordingly.

Distinguishing consent from notice

Organisations must distinguish consent from notice. When the individual signs a form it may be regarded as an acknowledgement that he or she has received notice and not “consent” in the proper sense of the word.

Opting in versus opting out

If organisations want to use existing stores of personal information in ways that do not fall within either the primary or related secondary purposes, it is open to them to seek consent from the individuals concerned. An opt-in model is appropriate.

IPP 2.1(c): Research or statistics where impracticable to seek consent

The IP Act applies in the research and statistics context where a Victorian government organisation uses or discloses identifiable information obtained directly from the individuals concerned (that is, the research subjects), or where the information is obtained from other sources (such as records held by a public or private sector organisation).

The IP Act facilitates the conduct of research in a number of ways, not limited to the use/disclosure ground in IPP 2.1(c). For instance, using unidentifiable data, or relying on consent, are alternative ways that research can be carried out in compliance with the IP Act.

Research using sensitive information

If a researcher wishes to use sensitive information (eg ethnic origin and criminal record), IPP 10 may be relevant. IPP 10 authorises collection of such information in limited circumstances, such as by consent or, in some situations, without consent where the research is relevant to government funded targeted welfare and educational services.

Research in the public interest, where impracticable to seek consent

An organisation seeking to rely on IPP 2.1(c) should firstly consider the following questions:

- a Is the use or disclosure of identifiable information necessary for research or statistical work, by the organisation itself or by the proposed recipient of the information? Can the same research objectives be achieved with alternative sources of data, or data that has been de-identified or is anonymous?
- b Will the research or statistical analysis/compilation result in publication of the information in a form that identifies any particular individual? If the data is to be de-identified prior to publication, how effective will that be? Consider, for instance, whether research subjects' identity can be reasonably ascertained where data is drawn from small communities.
- c Does the organisation reasonably believe that the recipient of the personal information will not disclose the information? Have undertakings of confidentiality been sought? Where the disclosure is outside of Victoria, have appropriate privacy protection measures been attended to, in accordance with obligations under the Transborder Data Flow Principle (see especially para 9:4 and the general discussion under IPP 9).
- d If it is necessary to use identifiable data, can the research subjects' consent be sought? Or is it impracticable to seek the subjects' consent before their personal information is used or disclosed?
- e Is the work in the public interest?

“Impracticable” to seek consent

Impracticability must be assessed in context, but generally it means more than mere inconvenience or some cost and effort for a public sector organisation.

Moreover, the *impracticability* of seeking consent should not be confused with the undesirability of seeking consent. IPP 2.1(c) does not permit consent to be waived where, for example, consent can be readily sought but organisations would prefer not to do so (for instance, out of a desire for a high or 100% rate of participation).

Research “in the public interest”

Research and statistics “in the public interest” may involve “matters which affect society’s essential interests and in which the state has responsibilities” such as containing epidemics, combating drug taking, investigating the scale and pattern of sexual assaults on minors, or developing aid to social groups in difficulty.

In assessing whether research or the compilation or analysis of statistics is “in the public interest”, organisations should consider questions such as:

- a Is the organisation conceiving of the public interest as being wider than its own needs?
- b How is the wider community expected to benefit from the research or statistical analysis/compilation?
- c Are there any countervailing considerations or interests that should be taken into account in balancing the public interests in privacy and the conduct of the research?
- d Will the research or statistical work lead to any particular benefit – or pose any particular risk – to participants from specific groups who may, for instance, be in a relationship of dependency or inequality or may otherwise be vulnerable?

IPP 2.1(d): Necessary to lessen or prevent serious threats to health or safety

IPP 2.1(d) allows use or disclosure to occur where the organisation reasonably believes it is necessary to lessen or prevent:

- a a serious and imminent threat to an individual’s life, health, safety or welfare; or
- b a serious threat to public health, public safety or public welfare.

Imminent

The meaning of “imminent” has been accepted as being “likely to occur at any moment; impending”.

In IPP 2.1(d)(i), note that the threat to public health/safety/welfare must be serious, but not necessarily imminent. This is in contrast to a threat to an individual's life/health/safety/welfare, which must be both serious and imminent.

Disclosures in relation to non-imminent threats to individual life/health/safety/welfare may be dealt with by way of consent. In contrast, threats to public health or safety may be serious enough to warrant extraordinary disclosures of personal information but may not be imminent in terms of time. It may be certain that, unless addressed, the threat will do serious harm to public health or safety but not certain when that harm will actually be done.

Use/disclosure is necessary

It is not enough for an organisation to form a reasonable belief that there is a serious (and, in the case of an individual, imminent) threat. IPP 2.1(d) also requires that the organisation believe that it is necessary to disclose information in order to lessen or prevent the threat. In determining whether a use or disclosure might be regarded as necessary, consider the following:

- a Is the use or disclosure motivated by an intention to lessen or prevent the threatened harm?
- b Is the information being used or disclosed relevant to managing that threat?
- c Where information is disclosed, is the recipient in a position to act on the information to lessen or prevent the harm from eventuating?

In most cases, the recipient would need to be an appropriate agency that is in a position to lessen or prevent the particular threat.

IPP 2.1(e): Investigating suspected unlawful activity

Where an organisation has reason to suspect that unlawful activity has been, is being, or may be, engaged in, IPP 2.1(e) allows personal information to be used or disclosed:

- a as a necessary part of the organisation's investigation of the matter; or
- b in reporting the organisation's concerns to relevant persons or authorities.

Unlawful activity

The activity being investigated must be unlawful, not simply unethical or objectionable. Clearly, suspected breaches of the criminal law fall within the meaning of "unlawful activity".

Disclosure to relevant persons and authorities

When an organisation decides to report suspected unlawful activity, such use or disclosure should be limited to the persons or authorities with a need to know the information because they have relevant duties to perform in the circumstances.

IPP 2.1(e): Investigating suspected unlawful activity

Where an organisation has reason to suspect that unlawful activity has been, is being, or may be, engaged in, IPP 2.1(e) allows personal information to be used or disclosed:

- a as a necessary part of the organisation's investigation of the matter; or
- b in reporting the organisation's concerns to relevant persons or authorities.

Unlawful activity

The activity being investigated must be unlawful, not simply unethical or objectionable. Clearly, suspected breaches of the criminal law would fall within the meaning of "unlawful activity".

Misconduct by public sector officials may be considered unlawful if it contravenes a statutory secrecy or confidentiality obligation.

Investigation by the organisation

When an organisation proposes to use or disclose personal information in order to investigate the matter itself:

- a any suspicion of wrongdoing should be based on reasonable grounds, not just unsubstantiated gossip or rumour;

- b the use or disclosure must be considered necessary after due consideration of alternatives;
- c the use or disclosure should be as confined as possible throughout the organisation's investigation, both in terms of the number of individuals whose information is involved and the number of people who are given access to the information.

Disclosure to relevant persons and authorities

When an organisation decides to report suspected unlawful activity, such use or disclosure should be limited to the persons or authorities with a need to know the information because they have relevant duties to perform in the circumstances.

IPP 2.1(f): Required or authorised by law

IPP 2.1(f) allows personal information to be used or disclosed otherwise than for the primary purpose if such use or disclosure is required or authorised by or under law. This principle is consistent with section 6 of the IP Act in that other more specific laws dealing with use and disclosure will prevail.

Required by law

"Required by law" means there is a legal obligation to use or disclose personal information in a particular way. Words such as "must" or "shall" will indicate a requirement, and may be accompanied by the presence of a sanction for non-compliance.

Authorised by law

"Authorised by law" means that while the law permits the use or disclosure, it does not make either compulsory. Words such as "may" are indicative of this, and discretionary powers may be involved.

IPP 2.1(g): Reasonably necessary assistance for law enforcement and protection of public revenue

IPP 2.1(g) allows an organisation to use or disclose personal information where the organisation reasonably believes that the use or disclosure is reasonably necessary for any of five specified purposes undertaken by or on behalf of a law enforcement agency:

- a the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;
- b the enforcement of laws relating to the confiscation of the proceeds of crime;
- c the protection of the public revenue;
- d the prevention, detection, investigation or remedying or seriously improper conduct;
- e the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

If an organisation uses or discloses personal information to assist law enforcement agencies for any of the above purposes, IPP 2.2 requires the organisation to make a written record of that use or disclosure.

Reasonably believe that disclosure is reasonably necessary

Organisations are not prevented by the IP Act from continuing, as they did before the IP Act came into force, to cooperate with police and other law enforcement agencies in their investigation of criminal activities. IPP 2.1(g) expressly authorises organisations to assist police and a range of other law enforcement agencies by providing information relevant to a number of broadly-worded law enforcement functions. IPP 2.1(g) requires, however, that organisations consider the reasonableness of their actions before handing over personal information. Tests of reasonable belief and reasonable necessity must be satisfied.

In some cases, organisations may determine that it would not be appropriate to release the information under IPP 2.1(g). This may be because they have not been persuaded that the information is necessary for one of the authorised purposes. Or the organisation may determine that, due to the sensitivity or volume of information requested, it would be more appropriate to withhold the information until and unless a warrant or other legal authority is produced.

IPP 2.1(h): Commonwealth security agencies

Under a number of specified conditions IPP 2.1(h) allows an organisation to disclose information to officers of the Australian Security Intelligence Organisation (ASIO) and the Australian Secret Intelligence Service (ASIS).

IPP 2.1(h) allows an organisation to disclose information to officers of the Australian Security Intelligence Organisation (ASIO) and the Australian Secret Intelligence Service (ASIS) where the agency has requested the information in connection with its functions and:

- a the disclosure is made to an ASIO or ASIS officer or employee who is authorised in writing by the Director-General of ASIO or ASIS to receive the information; and
- b the Director-General of ASIO or ASIS has also certified in writing that the disclosure would be connected with the performance by ASIO or ASIS of its functions.

Organisations need to be satisfied that a request for information is legitimate and appropriately documented.

IPP 2.2: Written notes of uses/disclosures under IPP 2.1(g) to law enforcement agencies

A written note must be made of any disclosure to a law enforcement agency under IPP 2.1(g). The note should specify at least the following information:

- a the personal information used or disclosed, with a copy of any material supplied;
- b the law enforcement agency or agencies and their representatives' names;
- c the basis of the reasonable belief that the use or disclosure was reasonably necessary, taking care not to prejudice any investigation or proceeding; and
- d the name and title of the decision-maker.

The Guidelines also discuss:

- Research using unidentified data
- Research with consent
- Non-consensual research under other IPP 2 grounds
- Making first contact with prospective participants
- Research using data matching or data linkage
- Role of research ethics committees
- Public officials acting on information obtained in their private capacity
- Anticipating the need to provide information during an emergency
- Using or disclosing during emergency relief efforts
- Administrative release of information under s. 16(2), FoI Act
- Obligations to make documents available for inspection
- Disclosing only to the extent required or authorised
- Relevance of the *Charter of Human Rights and Responsibilities*
- Disclosure to law enforcement agencies
- Specified law enforcement purposes (IPP 2.1(g)(i)-(v))
- Exemptions contained in IPP 2.1(g)(i)-(v)
- Reasonably believe that disclosure is reasonably necessary
- Exercising discretion to disclose under IPP 2.1(f)-(g)
- Verifying the authority underpinning requests for information under IPP 2.1(f)-(h)

Principle 3: Data Quality

- 3.1 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.

In the Guidelines, the word “quality” is used to refer collectively to the states of being accurate, complete and up-to-date.

Old records and archives

Organisations do not have to monitor data quality when information is dormant. Personal information collected and used for a particular purpose and then archived does not need to be constantly checked for accuracy.

Data quality should be assessed at some key points, including at the time of collection, when the information is used or re-used, and when it is disclosed to another organisation. Where use is regular or constant, the frequency of monitoring the quality of data will depend in part on the potential for that type of information to lose quality over time.

“Reasonable steps”

Quality is a relative term – it will depend on the circumstances. IPP 3 does not require organisations to take every possible step to ensure quality, but rather, to take “reasonable steps”. Thus the steps that are reasonable in this context will differ with the particular circumstances.

The reasonable steps required to ensure data quality in particular circumstances will depend on several factors, including:

- a the nature of the information;
- b how recently the information was collected;
- c how quickly the information can go out of date;
- d who provided the information;
- e the purpose for which the organisation uses the information;
- f to whom the organisation discloses the information;
- g how, and for what purpose, the information will be used by the recipient; and
- h the consequences for the individuals concerned if the data is not sufficiently accurate, complete and up to date.

The nature or type of personal information, and the consequences that may flow from poor data quality, is particularly important. Certain categories of information may seriously disadvantage or humiliate an individual if the information is of poor quality. Where information can have adverse consequences for an individual, it will require much greater care to ensure high quality and meet the requirements of IPP 3.

Organisations should take reasonable steps to ensure that data remains intact during all phases of its handling – from collection, recording and transcription through to its storage and any dissemination.

“Accurate” and “complete”

Accurate means “careful, precise; lacking errors” or “conforming exactly with the truth or with a given standard”. Inaccurate information covers assertions that are factually erroneous as well as opinions based on erroneous facts.

Complete means “having all its parts or elements; entire”. The application of the word “complete” will depend on the specific information, context and purpose.

“Up to date”

Up to date means “meeting or according to the latest requirements, knowledge”. The requirement to keep information up to date is intended to deal with situations in which subsequent information would make the existing record inaccurate or obsolete if it were not added.

The Guidelines also discuss:

- Relationship between data quality and other information handling obligations
- Reciprocal obligations when disclosing to other organisations
- Public register and other online information
- Data cleansing
- Contracted service providers

Principle 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.

IPP 4 contains two distinct obligations, the first dealing with data security and the second dealing with the disposal of data.

Security and retention as part of “life cycle” of personal data

Personal information can take many forms and will need to be secured at various stages throughout its “life” – from the time of creation (when the data is first recorded), through any transformation (such as from paper to electronic form), during its transmission (whether physically carried or sent digitally through a computer network), and while it is held (for example, text messages stored in a mobile phone).

Your obligations to secure personal information under IPP 4.1 will continue for as long as you hold the data – that is, until the time of appropriate disposal under IPP 4.2 (and any other relevant laws, such as the *Public Records Act 1973* (Vic)).

IPP 4.1: Security of data

IPP 4.1 is concerned with an organisation’s obligation to take reasonable steps to protect personal information it holds from misuse, loss, unauthorised access, unauthorised modification and unauthorised disclosure.

Since the 1980s, there has been a significant amount of work done in the area of data and information security. Organisations can draw on a wealth of resources and expertise for guidance on managing data security risks. Many publications are particularly thorough and, if followed, will provide robust security across various areas of potential risk. The advice of security experts can also be sought.

Regardless of where advice is obtained, organisations may still need to identify and assess the risks associated with its particular holdings and its methods of handling personal information. An assessment of data security risks could be incorporated into an organisation’s broader approach to risk management. A Privacy Impact Assessment (PIA) may assist organisations in identifying and mitigating possible security and privacy risks.

“Reasonable steps” to secure information

Consistent with the taking of “reasonable steps” under other IPPs (notably IPP 3), taking reasonable steps under IPP 4.1 to protect personal information will depend on the particular circumstances.

Security measures should be proportionate and appropriate to the likely risk of a security breach and the gravity of harm that may result

In deciding what “reasonable steps” to take, organisations should consider factors such as:

- a the nature or sensitivity of the personal information concerned;
- b the likelihood of a security breach occurring; and
- c the gravity of any harm to an individual if a security breach occurs.

While it is recognised that organisations do not have unlimited resources to use in designing and adapting security safeguards to protect personal information, organisations would be expected to implement safeguards that are appropriate and proportionate in the circumstances. This will inevitably involve a balancing of a number of factors, including risks to personal privacy and costs of implementation.

Some key areas to consider

Information security standards usefully focus on a number of areas where data security risks could be managed, such as physical security (that is, securing a building or equipment where information is housed), logical security (that is, controlling access to data), and communication security (that is, protecting data during transmission).

The following examples of steps organisations may consider to be reasonable when securing personal information are discussed in greater detail in the Guidelines:

- Limiting access to those with a “need to know”
- Using audit logs to deter and detect security breaches
- Securing the places where information is physically stored
- Securing data during, and after, its transmission (eg, facsimiles, emails and online information)

“Information it holds”

IPP 4.1 requires organisations to take reasonable steps to protect the “information it holds”. Section 4(1) of the IP Act states that an organisation “holds” personal information if it is the possession or control of the organisation, whether alone or jointly with other persons or bodies, irrespective of where the information is situated, whether in or outside of Victoria.

Data security obligations do not cease, therefore, if the information leaves Victoria. Reasonable steps must be taken to secure information that travels interstate or overseas, or in cyberspace. Transborder dataflow obligations (IPP 9) will be relevant. Where custody or control over information is shared, which may often happen in an outsourcing context, each organisation has an obligation to secure the data. Organisations cannot contract out of their security (or other privacy) obligations.

“Misuse”

“Misuse” of personal information is use that is improper or unlawful. Generally speaking, proper uses are those that conform to the IP Act and IPPs (principally, IPP 2), to other relevant laws, and to the policies and standards organisations adopt themselves. The law, policies and standards that are relevant will depend on the information, the organisation and the particular circumstances.

Unlawful uses include those that are expressly prohibited by the Crimes Act 1958 (Vic) and other relevant laws.

Use of personal information by a public sector official may be unlawful or improper if the use contravenes statutory or common law obligations of secrecy or confidentiality. Misuse of information will also include uses of information by public sector officials otherwise than in carrying out official duties, or for personal or financial gain.

“Loss”

Information can be lost in the sense that its whereabouts are unknown and in the sense that there has been a failure to preserve or maintain it. Loss includes intentional or inadvertent destruction. Loss can be temporary or permanent, partial or total.

“Unauthorised access, modification or disclosure”

Access will include viewing information on a computer screen or reading a document on a file. Modification includes changing, removing or adding information. The meaning of “disclosure” essentially means opening up something to view or revealing

Access, modification or disclosure of personal information may be regarded as “unauthorised” where the person:

- a has *no* authority to access, modify or disclose the information;
- b *exceeds* their authority; or
- c *misuses* their authority.

IPP 4.2: Disposal of data

IPP 4.2 requires organisations to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

“Reasonable steps to destroy or permanently de-identify”

Organisations should already have records management processes in place for disposing of records under the *Public Records Act 1973* (Vic) (the PR Act). Where an organisation is not bound by the PR Act, because it falls outside of the meaning of “public office” and is otherwise not covered by the PR Act, then a records management plan should be progressively developed to deal with current, archived and new collections of personal information.

Reasonableness of destruction or de-identification will be assessed in the context of each particular case. The sensitivity and extent of information should be considered with particular care, not only during risk assessment and setting access control, but also when assessing the timing and method of disposal.

Organisations may decide that the disposal obligations applying to particular types of information holdings may warrant greater clarity or specificity than might already apply under an existing Disposal Authority issued by PROV. Advice from PROV should be sought.

Reasonableness will also involve a consideration of the medium in which personal information is stored. Data media differences have a major bearing on the interpretation of destruction or de-identification. Hard copy documents are relatively straightforward. When data is held electronically, more complex issues arise.

An organisation may decide to dispose of information by de-identifying it, rather than through destruction. In that case, IPP 4.2 requires the de-identification to be “permanent”. Permanent means irrevocable or irretrievable.

“No longer needed for any purpose”

IPP 4.2 allows organisations to retain information for the original purpose for which it was collected, or “for any purpose”. The purpose can be either the primary purpose for which the information was collected, or it can be some other legitimate purpose such as those specified in IPP 2.1.

The *Public Records Act 1973* (Vic) is particularly relevant, as discussed earlier. Other statutory obligations may require or authorise records to be retained, or may compel their destruction, in particular circumstances. These statutes will prevail over the disposal obligation in IPP 4.1, to the extent of any inconsistency.

Information will often have great statistical and research value and can inform and guide public policy decisions. IPP 4.2 does not require this information to be destroyed. Nor does it authorise routine retention in identifiable form.

The purpose for retaining personal information should be specific and identifiable, rather than undefined and hypothetical. IPP 4.2 does not authorise retention of information “just in case” it is needed for some future use by the organisation or by a third party.

The Guidelines also discuss:

- Records management and other relevant personnel within the organisation can provide valuable assistance
- Distinguishing data security from information privacy
- Relationship between unauthorised disclosures and security breaches
- Balancing convenience and efficiency with privacy and security
- Notification of a security breach
- Relationship between the disposal principle and other IPPs
- Relevance of the *Public Records Act*

Principle 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.

The Openness Principle promotes a greater awareness and understanding of the way in which personal information is handled.

Relationship of IPP 5 with other information handling obligations

Information handling policies (or privacy policies) kept for the purposes of IPP 5 will often be useful in notifying individuals of some of the matters contained in IPPs 1.3 and 1.5.

The Openness Principle has been regarded as a prerequisite for the Access Principle (IPP 6, FoI Act) for it must be possible to know what type of information is generally held by an organisation in order to effectively make a more specific request to access one's personal information.

IPP 5.1: Written policy on management of personal information

Victorian public sector organisations and their contractors bound by the IP Act should already have privacy policies in place. Organisations may wish to periodically review their policies, especially where they have been given new functions or have undergone a restructure. It is good practice (and consistent with Public Records Act obligations to keep full and accurate records) to include a date and version reference on privacy policies.

In privacy policy work, there is no "one size fits all". It is usually risky and short-sighted to just copy another organisation's policy and presume it will work for your organisation. By all means, consult the work of others and take the best from good privacy policies. But be sure to ask yourself, "Does that apply to us in what we do here? Will that work here?"

Every organisation should appropriately tailor its own policy. The policy should not simply be a reproduction of the IPPs.

Large organisations should consider whether they want to have more than one privacy policy to cover, for example, the activities of individual business units which have quite distinct and varied functions. Organisations may wish to have a suite of policies to cover different types of information or information handling practices.

While there is no specific requirement to publish the IPP 5.1 policies – only to make them available on request to anyone who asks – most organisations will find it convenient and cost effective to publish them, in hardcopy form and on a website. Other options include:

- a sending the privacy policy with any written correspondence to individuals when they first transact with, or become a client of, the organisation;
- b sending the privacy policy with annual notices such as re-registration forms; and/or
- c having a copy of the privacy policy at the enquiries desk or counter.

Organisations may decide to take a “layered” approach to complying with IPP 5 (and, where appropriate, the notice obligations under IPP 1). A brief outline of information handling obligations can be provided on a form or poster, with additional layers of information readily available in brochures or online via the organisation’s website.

Privacy policies should be readily available to staff within an organisation to enable a prompt response to a request from a member of the public.

IPP 5.2: Responding to requests about the sort of information held and how it is used

Unlike IPP 5.1, IPP 5.2 does not expressly require organisations to document the sorts of personal information it collects and handles – only to take reasonable steps, when asked, to let people know generally what kind of personal information it collects and how it uses it.

IPP 5.2 does not require organisations to inform individuals about what information is specifically held about them – requests for specific access to personal information is governed by IPP 6 and the FoI Act. For IPP 5.2 purposes, it is sufficient to give generic information about the sort of information that is held, its purposes, how it is collected, held, used and disclosed.

Organisations may find it more efficient, however, to meet the requirements of IPP 5.1 and anticipate common queries under IPP 5.2 in the same document, or by using the multi-layered approach discussed earlier. However, where a generic document does not cover a person’s more specific request, the organisation is required to take reasonable steps to give a specific response.

The Guidelines also discuss:

- Relationship of IPP 5 with other information handling obligations

Principle 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) providing access would pose a serious and imminent threat to the life or health of any individual; or
 - (b) providing access would have an unreasonable impact on the privacy of other individuals; or
 - (c) the request for access is frivolous or vexatious; or
 - (d) the information relates to existing legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or
 - (e) 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
 - (f) providing access would be unlawful; or
 - (g) denying access is required or authorised by or under law; or
 - (h) providing access would be likely to prejudice an investigation of possible unlawful activity; or
 - (i) providing access would be likely to prejudice –
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (iii) the protection of public revenue; or
 - (iv) the prevention, detection, investigation or remedying of seriously improper 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 a law enforcement agency; or
- (j) ASIO, ASIS or a law enforcement agency 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.
- 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 (j) (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, the organisation –
- (a) must advise an individual who requests access to personal information that the organisation will provide access on the payment of the prescribed fee; and
 - (b) may refuse access to the personal information until the fee is paid.
- 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.
- 6.8 If an individual requests access to, or the correction of, personal information held by an organisation, the organisation must –
- (a) provide access, or reasons for the denial of access; or
 - (b) correct the personal information, or provide reasons for the refusal to correct the personal information; or
 - (c) provide reasons for the delay in responding to the request for access to or for the correction of personal information--
- as soon as practicable, but no later than 45 days after receiving the request.

IPP 6 provides individuals with a right to access and correct their own personal information. While the formal mechanism for access and correction is through the Freedom of Information Act (Fol Act), organisations are encouraged to permit access and correction through less formal means if practicable.

Interaction of IPP 6 with the Freedom of Information Act

The interaction of the IP Act and the Fol Act is most directly described in the IP Act in sections 6(2) and 12:

- a section 6(2) provides that nothing in the IP Act affects the operation of the Fol Act or any right, privilege, obligation or liability conferred or imposed under the Fol Act or any exemption arising under the Fol Act; and
- b section 12 provides that nothing in IPP 6 or any applicable code of practice applies to documents that are regulated by the Fol Act, and access to and correction of these documents can only be granted in accordance with the Fol Act.

Other sections in the IP Act preserve the exemptions under Fol for documents that can be required during the handling of complaints or during compliance investigations.

Fol will be the usual procedure for access and correction

If an organisation is subject to the Fol Act, then the procedures in that Act will apply. If an organisation is not subject to Fol but is bound by the IP Act, then access and correction must be handled in accordance with IPP 6.

As far as is lawful and practicable, access and correction under IPP 6 should mirror the procedures, use the knowledge and build on the analogous Fol case law built up over two decades of Fol. But analogies with the Fol Act are not exact. Care must be taken in the particular circumstances and with the particular information involved to apply the provisions of IPP 6 when it is the governing law and not the Fol Act, which may be analogous but which is also much older law than the IP Act.

Contractors and other organisations not subject to the FoI Act

IPP 6 will apply to those organisations that are bound to comply with the IP Act but are not covered by the FoI Act. “[T]he access provisions in principle 6 have a limited operation to contracted service providers, which are not always subject to freedom of information legislation, and certain other bodies.”

Contracted service providers

A government agency that engages a contractor service provider and binds them to the IP Act will need to consider how to manage access requests for personal information. Individuals may, for instance, be able to seek access directly from the contracted service provider or indirectly through the outsourcing government organisation where that organisation retains possession or control over the documents.

Where a contracted service provider has not been contractually bound to comply with the IP Act, the outsourcing government agency will need to give thought to how it will ensure that it can get hold of personal information in the possession of the service provider for the purposes of the contract so that the outsourcing organisation can meet its own access and correction obligations.

Other organisations not subject to FoI

IPP 6 will also be the mechanism for dealing with access and correction requests where the organisation is not bound by the FoI Act but is nevertheless subject to the IP Act. This will include those organisations that fall within section 9 of the IP Act but fall outside of the definition of “agency” in section 5 of the FoI Act.

Bodies excluded by ss 5(3) and 6, FoI Act

Some organisations are expressly excluded from having to comply with the FoI Act by virtue of sections 5(3) and 6 of the FoI Act. Section 5(3) excludes offices such as those of the Electoral Commissioner, Ombudsman and Director of Public Prosecutions from having to comply with the FoI Act, while section 6 similarly excludes courts acting in their judicial function.

While these bodies are bound by the IP Act and must comply with the other IPPs (subject to any applicable exemption¹), section 12(b) of the IP Act expressly states that bodies excluded by virtue of these sections 5(3) or 6 in the FoI Act are not required to comply with IPP 6.

These excluded organisations can, of course, decide to voluntarily comply with IPP 6.

Other bodies not bound by the FoI Act

IPP 6 may apply to those bodies bound by the IP Act but excluded or not covered by the FoI Act otherwise than by virtue of sections 5(3) and 6 of the FoI Act.

Similarly, IPP 6 obligations may apply to those bodies that have been held by a tribunal or court decision to fall outside of the operation of the FoI Act.

IPP 6.1: Right of access

Like FoI, IPP 6 starts with a presumption of access:

- 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 [one of the exceptions in IPP 6.1(a)-(j) applies].

The exceptions are discussed further overleaf.

¹ Notably, organisations that investigate or prosecute criminal offences and breaches of other laws that carry a sanction or penalty may not be required to comply with IPP 6 where they reasonably believe non-compliance is necessary: section 13, *Information Privacy Act 2000* (Vic).

Providing partial or limited access

Organisations should endeavour to provide access to the extent they can. Where an organisation is proposing to withhold personal information because one of the exceptions in IPP 6.1(a)-(j) applies, consideration should be given to providing access to some extent or in some other way.

This may involve using mutually agreed intermediaries under IPP 6.3. Or, this may involve providing access to documents after removing (or blacking out) the material that was subject to the relevant exception in IPP 6.1(a)-(j).

IPP 6.1(a)-(j): Restricting access

The exceptions limiting the right of access under IPP 6.1 are listed in IPP 6.1(a)-(j). The Guidelines discuss these exceptions in greater detail.

IPP 6.2: Commercially sensitive decision-making

IPP 6.2 allows organisations to give individuals an explanation for a commercially sensitive decision, rather than direct access to the information underpinning that decision where that would reveal evaluative information generated in connection with the decision-making process.

IPP 6.2 cannot be used to withhold factual personal information on which a commercial decision is based – only “evaluative information”. IPP 6.2 was intended to ensure that, where individuals are adversely affected by a commercial decision, they are able to receive an explanation of the reasons for the decision.

IPP 6.3: Providing limited access through intermediaries

Where one of the exceptions in IPP 6.1(a)-(j) applies, IPP 6.3 requires organisations to, if reasonable, consider the use of mutually agreed and properly authorised intermediaries to allow sufficient access to meet the needs of both parties.

Where the organisation determines that full access to the requested information should not be granted because of a relevant exception applies, organisations should endeavour to provide more limited access through intermediaries, such as the requester’s relative, lawyer or other nominated representative agreed to by the organisation.

Organisations should consider, where reasonable, whether it would be appropriate to give full access to the agreed intermediary to enable that person to assess the content in order to explain the information to the requester or determine whether partial or conditional access should be negotiated.

IPP 6.4: Access fee

Section 69 of the IP Act allows organisations to charge a prescribed fee for providing access, and IPP 6.4 permits the organisation refuse access until the prescribed fee is paid.

To date, however, there are no prescribed fees for access under the IP Act. Organisations that are required by IPP 6 to give access are not currently entitled to charge a fee for access or to refuse access because some fee or charge has not been paid. (The Guidelines are current to 1 September 2006. Organisations should check whether regulations have been made under the IP Act after this date that authorise the charging of a fee for access under IPP 6.)

IPPs 6.5 & 6.6: Right of correction

If an individual establishes that the information held by an organisation about him or her is not accurate, complete or up to date, IPP 6.5 requires the organisation to take reasonable steps to correct the information.

If the organisation and the individual cannot agree about whether the information is wrong, and the individual asks the organisation to place a statement with the information claiming it is not accurate, complete or up to date, then IPP 6.6 requires the organisation to take reasonable steps to do so.

The use of the term “reasonable steps” in IPP 6.5 and 6.6 was not intended to impose an onerous obligation on organisations in respect of information that was inaccessible and never to be used. On the other hand, the term “reasonable steps” was intended to be broadly interpreted to discourage the persistence of poor quality data and to encourage organisations to respond to data quality issues that individuals bring to their attention.

Where it is difficult to determine whether information is misleading or whether it is inaccurate, incomplete or out of date, organisations are encouraged to err on the side of correcting (or placing a statement with) the information in accordance with IPPs 6.5 and 6.6.

IPP 6.7: Reasons for denial of access or refusal to correct

Where an organisation refuses a request for access or correction, IPP 6.7 requires the organisation to provide reasons.

IPP 6.8: Time limit for responding to request for access or correction

IPP 6.8 sets a time limit for organisations to respond to a request for access or correction. Organisations must respond to a request as soon as practicable, but no later than 45 days after receiving the request.

Organisations should endeavor to provide access or agree to correct, or provide reasons for a denial of access or refusal to correct, within this time limit. IPP 6.8 does not, however, demand that organisations finalise their response within 45 days, provided they notify the requester within this timeline of the reasons for any delay in responding.

The Guidelines also discuss:

- Government not the public, need the IP and FoI Acts to mesh together
- Form of access
- Who is entitled to exercise the rights of access and correction under IPP 6? (Access to and correction of one’s own information; and Accessing a child’s personal information)

Principle 7: Unique Identifiers

“**unique identifier**” means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual’s name.

- 7.1 An organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.
- 7.2 An organisation must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless –
 - (a) it is necessary to enable the organisation to carry out any of its functions efficiently; or
 - (b) it has obtained the consent of the individual to the use of the unique identifier; or
 - (c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.
- 7.3 An organisation must not use or disclose a unique identifier assigned to an individual by another organisation unless –
 - (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation;
or
 - (b) one or more of paragraphs 2.1(d) to 2.1(g) applies to the use or disclosure; or
 - (c) it has obtained the consent of the individual to the use or disclosure.
- 7.4 An organisation must not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

Meaning of “unique identifier”

An identifier can be a sequence of numbers, letters and/or characters used to identify or refer to a person. An individual’s name is not considered to be a unique identifier under the definition in the IP Act. However, an identifier that is comprised in part of a person’s name or initials may be regarded as a unique identifier.

IPP 7 will not apply to unique identifiers that fall within the meaning of “identifier” in the Victorian *Health Records Act 2001*. Instead, Health Privacy Principle 7 will apply to the assignment, adoption, use and disclosure of identifiers.

IPP 7.1: Assignment of a unique identifier

IPP 7.1 states that an organisation must not assign unique identifiers to individuals unless that is necessary to enable the organisation to carry out any of its functions efficiently.

As with IPP 1.1, you should be clear about both the need and the function. Necessity requires more than desire or convenience. Be clear and specific about which functions the assignment is in aid of, and whose functions are being carried out.

Organisations should also ask whether issuing a unique identifier is necessary in order that the organisation can carry out its functions “efficiently”, that is, with minimum waste or effort. The test of efficiency in carrying out any function will require an assessment of efficiency from the perspective of both the organisation and those with whom it deals.

IPP 7.2: Adoption of an existing unique identifier

The potential privacy risks associated with profiling and data matching grows when a unique identifier assigned by one organisation is adopted by other organisations. The risks are reduced by limiting the proliferation of any one identifier across multiple agencies.

IPP 7.3: Use or disclosure of a unique identifier

Use and disclosure of other organisations’ unique identifiers is only permitted in the three circumstances outlined in IPP 7.3(a)-(c):

- IPP 7.3(a): Necessary to fulfil obligations to the other organisation
- IPP 7.3(b): Use or disclosure in certain public interests
- IPP 7.3(c): Use or disclosure by consent

These are discussed further in the Guidelines.

IPP 7.4: Demanding identifiers be provided in order to obtain a service

IPP 7.4 states that an organisation must not require an individual to provide a unique identifier in order to obtain a service unless:

- a the provision of the unique identifier is required or authorised by law; or
- b the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

Organisations must not make service delivery contingent on individuals providing their identifier unless they have authority under law, or the identifier is relevant to the purpose for which it was assigned.

Organisations who require service users to provide their driver’s licence or other identifiers should ask whether, and if so how, the organisation’s service is connected to the reason for which the identifier was assigned.

If the identifier is neither relevant nor legally authorised, organisations should refrain from demanding identification be produced by individuals seeking to obtain a service.

The Guidelines also discuss:

- Data-matching and the IPPs
- Statistical linkage keys
- “Adopt as own” distinguished from recording identifiers
- Necessary to efficiently carry out functions (IPP 7.2(a))
- Consent (IPP 7.2(b))
- Outsourcing (IPP 7.2(c))
- Other uses are not authorised under IPP 7.3

Principle 8: Anonymity

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

IPP 8 was explicitly intended to “preserve” and “protect”, where lawful and practicable, individuals’ ability to remain anonymous in transactions with government organisations.

“Transactions”

“Transactions” should be interpreted broadly to include the interactions and dealings between the individual and the organisation, whether or not they involve an exchange in a commercial sense.

“Lawful and practicable”

An organisation may not be in a position to offer an anonymous option if that would be contrary to law. An Act or regulation may require that identifying information be collected before an individual is permitted to transact with the organisation. Registering for a profession or applying for a licence are examples where anonymity is simply not an option.

However, there will be many cases where identification is not required by law, giving organisations an opportunity to consider whether it is practicable to give individuals the option to remain anonymous.

Assessing whether it is practicable to offer an anonymous option will involve a weighing up a number of considerations. Cost is likely to be an issue, but it is not the only issue. Prudence will need to be exercised when examining the various public interests in favour of anonymity, as compared to any countervailing interests. Just as there are legitimate uses of anonymity, so too are there legitimate reasons for seeking identification or making anonymous options conditional.

Where identification is required to establish eligibility for a service or benefit, it might be sufficient just to sight a document and perhaps record that the particular document was sighted, rather than to record or copy the personal information contained on the document.

Providing an anonymous option will not always be appropriate. Determining the circumstances when anonymity will be appropriate requires a careful balancing between what can be done within existing legal and technological constraints, and what should be done to promote and protect privacy and other fundamental rights and public interests. Any restriction on the ability to transact anonymously should be limited to what is necessary and proportionate to protect the various interests at stake, while ensuring that less restrictive means are always considered.

The Guidelines also discuss:

- Relationship between anonymity and other IPPs

Principle 9: Transborder Data Flows

- 9.1 An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria 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 Information 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 that 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 Information Privacy Principles.

IPP 9 regulates the transfer of data to someone who is outside of Victoria – either interstate or overseas. In this context, the term “data” means personal information. The flow of data must be from the organisation to a person or body who is outside Victoria. IPP 9 will not restrict transfers to the individual who is the subject of the information.

IPP 9 does not apply where both the sender and the recipient are part of the same organisation, such as when an organisation communicates with or transfers information to staff who are located or travelling interstate or overseas.

The Transborder Data Flow Principle aims to ensure that, when personal information travels, privacy protection travels with it. IPP 9 is about organisations taking steps to ensure that safeguards are in place *before* the information leaves the protections of the IP Act.

Other than under other Victorian or Commonwealth laws, personal information may be transferred under any of six grounds set out in IPP 9.1(a)-(f). The six bases on which personal information may be transferred to someone outside Victoria under IPP 9.1(a)-(f) are alternatives. Only one need be met, although in practice several may be fulfilled at once.

Where possible, organisations should endeavour to ensure privacy protections accompany any transfer. Where such protections are not in place, and the organisation seeks to rely on IPP 9.1(b)-(e) for the transfer, it is expected this would only occur where the individual's interests in favour of the transfer overrides their interest in protecting

the privacy of their information, or where the privacy risk is relatively small. Examples of transborder data flows that might involve a serious risk to personal privacy include those that:

- a involve vast amounts of personal information;
- b involve information of uneven quality;
- c involve information about vulnerable persons;
- d involve sensitive information (defined in the IPPs to include personal information such as racial and ethnic origin, political opinions, sexual preferences, and criminal record);
- e utilise insecure methods of transfer;
- f carry a risk of broader dissemination to entities that are not required or otherwise committed to protecting individuals' privacy;
- g. carry a risk of identity theft or financial harm; or
- h. carry a risk of harm to a person's life, safety, liberty, reputation or livelihood.

In principle, these types of transfers should be accompanied by a similar level of privacy protection as can be found in the IPPs.

IPP 9.1(a): Recipient bound by principles substantially similar to the IPPs

IPP 9.1(a) permits organisations to transfer data where they reasonably believe the recipient is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of information that are substantially similar to the IPPs.

Organisations should check whether the proposed recipient is covered by a privacy law that is comparable to the IP Act. Note that not all Australian jurisdictions have privacy laws in force. If you have queries about the application or coverage of privacy laws operating in other jurisdictions, you are encouraged to seek independent legal advice. You may also wish to contact the relevant oversight body or responsible government agency.

Where a privacy law operates in the recipient's jurisdiction, organisations should be aware that, while there is likely to be many similarities, there may also be some significant differences that can impact on a particular data transfer.

The Victorian Privacy Commissioner has no legislative authority to deem a privacy law, scheme or contract as providing substantially similar privacy protection for the purposes of IPP 9. Nor does the Victorian Privacy Commissioner have any authority to issue a "whitelist" of persons or bodies who would be regarded as subject to adequate protections (or "safe harbours") for the handling of personal information. Each case will need to be assessed on its merits, taking into account the circumstances of the particular data transfer that is proposed or has been undertaken.

Judgments will need to be made in each case about the extent to which the recipient is subject to the relevant law, binding scheme or contract; the extent to which principles are upheld effectively under that law, binding scheme or contract; and the degree to which the relevant principles are sufficiently similar to Victoria's IPPs to merit the description "substantially similar". These elements are essentially about:

- a *Form of obligation*: what form of regulatory mechanism is used to impose fair handling obligations on the recipient – law, binding scheme or contract?
- b *Content of principles*: which privacy or data protection rights are included in the fair handling principles that the recipient is required to uphold?
- c *Enforceability*: are the fair handling principles binding on the recipient and capable of being effectively upheld; that is, are they enforceable?

These elements are discussed in greater detail in the Guidelines.

IPP 9.1(b): Individual gives consent

IPP 9.1(b) allows organisations to transfer information interstate or overseas where they have an individual's consent.

IPP 9.1(b) would allow an organisation to obtain consent from an individual to a transfer of their information to an interstate or overseas recipient who is not subject to substantially similar privacy protections. As this creates a potential reduction in privacy protection of the information after it is transferred, organisations should ensure that individuals are properly informed of any reasonably foreseeable privacy risks associated with the transfer prior to obtaining the individual's consent.

IPP 9.1(c): Necessary to perform a contract with the individual or for implementation of pre-contractual measures at the individual's request

IPP 9.1(c) allows organisations to transfer information outside of Victoria where the transfer is necessary for:

- a the performance of a contract between the individual and the organisation; or
- b for the implementation of pre-contractual measures taken in response to the individual's request.

The use of the criterion of "necessity" constrains what might otherwise be a potentially very broad authority for transferring data. The "necessity test" in this context "requires a close and substantial connection between the data subject and the purposes of the contract."

IPP 9.1(c) cannot be used for transfers of additional, non-essential information. Nor can IPP 9.1(c) be used to authorise transfers of information for a purpose unrelated to the performance of the contract or pre-contractual measures. Transfers of information carried out to implement pre-contractual measures must be initiated by the individual, not by the organisation or recipient.

IPP 9.1(d): Necessary to perform a contract with a third party in the individual's interest

Under IPP 9.1(d), an organisation may transfer information outside of Victoria to conclude or perform a contract concluded with a third party in the interest of the individual who is the subject of the information being transferred.

IPP 9.1(d) contemplates transfers that are beneficial to the interests of the individual (that is, "in the interest of the individual"), not adverse or prejudicial to the individual's interests. The individual's interest in protecting their privacy is one among many other interests.

IPP 9.1(e): For the individual's benefit where impracticable to obtain consent or consent likely to be given

IPP 9.1(e) allows for transborder data flows where it is for the benefit of the data subject and it is impracticable to obtain consent, but that the organisation reasonably believes that the data subject would give consent.

The transfer must be for the particular individual's benefit.

While such transfers for the benefit of the individual might ordinarily occur by consent, IPP 9.1(e) allows the transfer to proceed without consent if it is impracticable to obtain that consent and, if sought, the individual would likely give consent.

IPP 9.1(f): Reasonable steps taken to ensure data will not be handled inconsistently with the IPPs

Generally speaking, the steps required to satisfy IPP 9.1(a) will amount, in practice, to what is required by IPP 9.1(f).

However, IPP 9.1(f) also allows transfers where the recipient is not bound by a law, binding scheme or contract that requires it to effectively uphold fair handling principles that are substantially similar to the IPPs. The primary focus of IPP 9.1(f) is on the reasonable steps taken by the organisation, rather on the more formal and substantive privacy obligations binding the recipient.

Various methods might be used (often in conjunction) to satisfy IPP 9.1(f), including law, technology and administrative practices.

Principle 10: Sensitive Information

“sensitive information” means information or an opinion about an individual’s –

- (i) racial or ethnic origin; or
- (ii) political opinions; or
- (iii) membership of a political association; or
- (iv) religious beliefs or affiliations; or
- (v) philosophical beliefs; or
- (vi) membership of a professional or trade association; or
- (vii) membership of a trade union; or
- (viii) sexual preferences or practices; or
- (ix) criminal record –

that is also personal information;

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

- (a) the individual has consented; or
- (b) the collection is required under 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) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite IPP 10.1, an organisation may collect sensitive information about an individual if –

- (a) the collection –
 - (i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
 - (ii) is of information relating to an individual’s racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and
- (b) there is no reasonably practicable alternative to collecting the information for that purpose; and
- (c) it is impracticable for the organisation to seek the individual’s consent to the collection.

Meaning of sensitive information

Sensitive information must also be personal information. IPP 10, like the remainder of the IP Act, will not operate where the information an organisation collects or handles is not about a person whose identity is apparent or is reasonably ascertainable.

Racial or ethnic origin

The term “ethnic origin” has been regarded by the courts as having a wider meaning than strictly “racial”.

Citizenship has not been regarded as an element of “race”.

It has also been suggested that, “The fact that a person has a particular surname would not usually be regarded as personal information revealing his or her ethnic background.”

Membership of a political association

“Political” is not defined in the IP Act but has been interpreted in anti-discrimination cases as being a matter or activity which has a bearing on government.

Religious beliefs or affiliations

“Religious belief” may include the holding, or not holding, of a religious belief.

In Victoria, the *Equal Opportunity Act 1995* expressly defines “religious belief or activity” to mean holding or not holding a lawful religious belief or view; or engaging or not engaging in a lawful religious activity.

The Federal Court of Australia has accepted that information collected from employees during a telephone poll carried out by a call centre on behalf of a union included sensitive information.

Criminal record

“Criminal record” should be broadly interpreted to mean “any information associating an identifiable individual with criminal behaviour, whether or not charged, convicted, or found guilty.”

Photographs taken by police of individuals while in custody have been regarded as forming part of an individual’s criminal record.

Limiting the collection of sensitive information

IPP 10 states that sensitive information must not be collected unless one of the grounds in IPP 10.1(a)-(d) or IPP 10.2 apply. IPP 10 should be read in conjunction with IPP 1. A breach of IPP 1 may taint a collection under IPP 10.

IPP 10.1(a): Individual gives consent

Organisations can collect sensitive information under IPP 10.1(a) where the individual gives his or her consent. Consent must be informed, current, specific and made with legal capacity. It must also be voluntarily given. If an individual has no real choice but to consent to the collection of sensitive information, then that consent may not be regarded as voluntary.

Consent is expected to be one of the principal ways in which organisations collect sensitive information from identifiable individuals. Reliance on consent ensures individuals know who is collecting sensitive details about their racial or ethnic origin, criminal records, sexual preferences or practices, religious beliefs or affiliations, political views and the like. Where consent cannot be sought, or where consent cannot be validly given, then organisations should consider whether they are permitted to collect sensitive information under one of the other grounds set out in IPPs 10.1 or 10.2. Relevant exemptions may also apply.

IPP 10.1(b): Required by law

IPP 10.1(b) recognises organisations can collect sensitive information where collection is required under law.

Unlike IPP 2.1(f) which allows information to be used or disclosed where “required or authorised by or under law”, IPP 10.1(b) limits the authority for collection of sensitive information to when it is “required under law” – not when such collection is simply “authorised”. The requirement to collect sensitive information must be mandatory, and not simply permissive or discretionary.

In the absence of a legislative mandate, organisations seeking to collect sensitive information obtain the individual’s consent or look to one of the other grounds specified under IPPs 10.1 or 10.2.

IPP 10.1(c): Necessary to lessen or prevent serious and imminent threats to the life or health of any individual

IPP 10.1(c) allows sensitive information to be collected where this is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where consent cannot be obtained from the individual whom the information is about because that person is either physically or legally incapable of consenting, or that person cannot physically communicate his or her consent.

This ground is similar to the authority for use and disclosure under IPP 2.1(d). However, unlike IPP 2.1(d), the threat under IPP 10.1(c) must be to an individual, not just in respect of the public at large. And, like IPP 2.1(d)(i), the threat to the individual must be both serious and imminent.

IPP 10.1(d): Necessary for legal or equitable claims

Organisations may collect sensitive information where the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

IPP 10.1(d) may be relevant to situations where, for example, an organisation is defending itself against a claim of unlawful discrimination or unfair dismissal.

Establishment, exercise or defence of legal or equitable claims would encompass situations where it is necessary to collect sensitive information for the purpose of obtaining legal advice in connection with an existing or potential legal proceeding in a court or tribunal. There should either be a legal proceeding on foot or a real possibility that the organisation will need to exercise or defend its legal or equitable rights at a future date. In other words, don’t collect sensitive information “just in case”.

IPP 10.2: Research or statistics about, or delivery of, government services

Sensitive information may be collected without consent, without a legislative mandate, outside of serious threats to individuals, and apart from the conduct of legal proceedings where the collection meets the following conditions:

- (a) the collection—
 - (i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services;
 - or
 - (ii) is of information relating to an individual’s racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and
- (b) there is no reasonably practicable alternative to collecting the information for that purpose; and
- (c) it is impracticable for the organisation to seek the individual’s consent to the collection.

“Government funded targeted welfare or educational services”

The authority in IPP 10.2 is limited to particular types of services (“welfare or educational services”) that are “funded” by government and which are “targeted”.

“Welfare or educational services” are likely to include the provision of schooling and educational support services, and programs aimed at promoting physical and social well-being – especially for those in financial or social need.

The funded service must be “targeted”. This may mean that the service is aimed at a particular person or group of persons, or that the service is being carried out with a particular objective or result in mind.

“Government funded” services can include services that are funded by any combination of local, state and/or federal governments.

IPP 10.2(a)(i): Sensitive information necessary for research or statistics about government services

IPP 10.2(a)(i) equips Victorian government agencies (and, where relevant, their contracted service providers) with information necessary to carry out research or compile and analyse statistics about the services the government funds. This has the obvious benefit of enabling government to assess whether public monies are being effectively spent.

IPP 10.2(a)(ii): Information about racial or ethnic origin to deliver government services

IPP 10.2(a)(ii) authorise the collection of information about individuals’ racial or ethnic origin where this is collected for the purpose of providing a government funded targeted welfare or educational service. It does not, however, authorise the collection of other types of sensitive information for the purpose of service delivery.

The non-consensual collection of information about racial and ethnic origin was only intended to occur in “very limited circumstances...where necessary for the effective delivery of government welfare programs.”

IPP 10.2(b): No reasonably practicable alternative to proposed collection

IPP 10.2(b) emphasises the need to keep non-consensual collection of sensitive information to a minimum by directing organisations to consider all practicable alternatives.

IPP 10.2(c): Impracticable to seek consent

As stated in these earlier sections, impracticability should not be confused with undesirability. That is, IPP 10.2(c) does not permit consent to be waived where consent can readily be sought but the organisation would prefer not to do so (for instance, because a high rate of participation is desired and the organisation fears individuals would refuse their consent, if asked).

The Guidelines also discuss:

- Use of sensitive information in research
- Sensitive information necessary for research or statistics about government services
- Information about racial or ethnic origin to deliver government services
- No reasonably practicable alternative to proposed collection
- Impracticable to seek consent
- IPP 10.2: Research or statistics about, or delivery of, government services