



Privacy - Use and disclosure

Information Act Guideline

IPPs 2, 7 and 9 control the use and disclosure of personal information.

General limits on use and disclosure

Under IPP 2, use and disclosure is limited to the primary purpose for collection unless —

- it is required or authorised by law;
- the person consents;
- it is related to the primary purpose (or directly related, for sensitive information) and the person would reasonably expect the use or disclosure;
- it is necessary for some law enforcement or health and safety purposes.

This limit applies to use and disclosure within the organisation as well as disclosure outside the organisation. Personal information collected by one business unit of an organisation for a particular purpose is not automatically available for all functions of the organisation.

In each case, an organisation must judge whether use or disclosure for the particular secondary purpose is allowed by the person or otherwise under the Act.

Primary purpose for collection

The primary purpose for collection is the reason why the information was collected.

For information collected after 1 July 2003, this should have been identified in the process of confirming that collection was necessary for the functions or activities of the organisation, and notifying the person of the purpose for collection.

Information that can help in establishing the primary purpose may include —

- the particular law or policy under which the information was collected;
- information that was provided to the person about the reason for collection.

The primary purpose should not be described too broadly. For example, describing the primary purpose as collection for the purpose of “administering the functions of the agency” or for the purpose of administering a particular Act, are likely to be too broad.

It appears that it is possible for there to have been more than one primary purpose for collection of information.

When is something required or authorised by law?

An organisation can use or disclose personal information if it is required or authorised by law.

Something will be **required by law** when there is a specific provision that places a duty on the organisation or staff member to use or disclose the information, or the law requires action to be taken which cannot be taken without the information being used or disclosed in that way.

A finding that use or disclosure is required by law is not likely to be based on a general description of a function in an Act. It will usually be linked to a specific requirement for use or disclosure in a law or a specific requirement that necessitates use or disclosure.

Use or disclosure will be **authorised by law** when it is allowed or permitted by the law even if it is not required.

Privacy - Use and disclosure

Again, a finding that use or disclosure is authorised by law is not likely to be based on a general description of a function in an Act. It will usually be linked to a specific authorisation for use or disclosure.

What is required for consent from the person?

Consent by the person should be relied on when the organisation is satisfied that the consent is informed and voluntary.

Consent can be expressly given by the person or it can be implied from the circumstances. If it is reasonable and practicable, it is preferable to obtain express consent.

Use or disclosure for a related purpose

Use or disclosure for a secondary purpose is allowed if—

- it is related to the primary purpose for collection (or directly related, for sensitive information); and
- the person would reasonably expect the organisation to use or disclose it for the secondary purpose.

For this exception to apply, there should be a relatively close relationship between the primary purpose and the secondary purpose. A remote or tenuous relationship would not be sufficient.

For sensitive information, the requirement that the secondary purpose be directly related requires a substantially closer relationship.

The test for reasonable expectation is an objective one based on the circumstances of the case. The test does not involve deciding on the particular expectations of an individual. But it is open to argument that the particular circumstances of the class of people involved may be relevant.

Law enforcement and health and safety exceptions

IPP 2 recognises that there are cases in which the interests of health, safety and security can justify use or disclosure. They relate to:

- serious and imminent threats to life, health or safety;
- serious threats to public health or public safety;
- investigation and reporting of suspected unlawful activity;
- use or disclosure that is reasonably necessary for specific functions of a law enforcement agency;
- certified requests for information from ASIO or ASIS.

Section 70 of the *Information Act* also allows non-compliance with the IPPs by law enforcement agencies if it is necessary for specified functions.

Limits on unique identifiers

A 'unique identifier' is a code that is assigned by a public sector organisation to identify a person for the purposes of the operations of the organisation. It includes things like a driver's licence number.

IPP 7 is designed to address concerns about people being reduced to a number in the system, and concerns about collection and cross-checking of information about an individual from different sources. It limits when an organisation can —

- assign a unique identifier,
- adopt a unique identifier that has been assigned by another organisation,
- use or disclose a unique identifier assigned by another organisation;
- require an individual to provide a unique identifier.

An organisation can only **assign** a unique identifier to a person if it is necessary to enable the organisation to perform its functions efficiently.

Privacy - Use and disclosure

An organisation can **adopt** a unique identifier that has been assigned by another organisation if:

- it is necessary to enable the organisation to perform its functions efficiently;
- the person consents; or
- it is an outsourcing organisation adopting an identifier created by a contract service provider in the performance of its obligations to the organisation under a service contract.

An organisation can **use or disclose** a unique identifier assigned by another organisation if:

- it is required or authorised by law;
- the person consents;
- it is necessary to enable the organisation to fulfil its obligations to the organisation that assigned the unique identifier;
- the use or disclosure is allowed in IPP 2 under the exceptions dealing with —
- serious and imminent threats to life, health or safety
- serious threats to public health or public safety
- investigation and reporting of suspected unlawful activity
- use or disclosure that is reasonably necessary for specific functions of a law enforcement agency.

IPP 7 does not spell out the relationship between the 'adoption' restriction and the 'use or disclosure' restriction. It appears that IPP 7.2 and 7.3 operate independently so that, even in a case where a unique identifier has been lawfully adopted by an organisation, its use or disclosure by the adopting organisation is only allowed in the situations set out in IPP 7.3.

If that is the correct interpretation, use or disclosure of the adopted identifier would not be justified on the grounds that it is necessary

to enable the organisation to perform its functions efficiently. Something more would be required, whether that be authorisation by a law, consent by the person, or another exception in IPP 7.3.

Limits on transfer outside the Territory

Under IPP 9, an organisation cannot transfer personal information outside the Territory unless one of the following exceptions applies.

- **Required or authorised by a law of the Territory or the Commonwealth.**
- **Person consents.**
- **Recipient bound by privacy principles**
 - Organisation reasonably believes the person receiving the information is subject to a law or legally binding arrangement to comply with principles substantially similar to the NT IPPs; or
 - Organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed in a way inconsistent with the NT IPPs.
- **Contracts with the person or that benefit the person**
 - Necessary for performance of a contract between the organisation and the person or for pre-contractual measures taken in response to the person's request; or
 - Necessary for performance or completion of a contract between the organisation and a third party, the performance or completion of which benefits the person.
- **For benefit of the person**, it is impracticable to obtain their consent and it is likely that they would consent.

1800 005 610 — infocomm.nt.gov.au — infocomm@nt.gov.au

This guideline is produced by the Information Commissioner to promote awareness and understanding about the *Information Act*. It is **not a substitute for the Act**. You should read the relevant provisions of the Act to see how it applies in any particular case. Any views expressed in this guideline about how the Act works are **preliminary** only. In every case, the Commissioner is open to argument by a member of the public or a public sector organisation that a different view should be taken.