Privacy - Management of information

Information Act Guideline

IPPs 3 and 4 require each organisation to take reasonable steps to —

- ensure that personal information is accurate, complete and up to date;
- protect personal information from misuse and loss and from unauthorised access, modification or disclosure;
- destroy or permanently de-identify personal information if it is no longer needed for any purpose.

Accurate, complete and up to date

IPP 3 puts a positive obligation on organisations to take reasonable steps to ensure that the personal information they hold is accurate, complete and up to date.

This requirement can be compared to IPP 6.3 which allows a person to seek correction of personal information that is inaccurate, incomplete or out of date.

Personal information extends to opinions about a person (whether valid or not) as well as factual matter.

Compliance with this principle will be most important when an organisation is about to use or disclose the information, although the requirement is not expressly limited to such occasions.

Whether information is 'complete' and 'up to date' will be judged according to the purpose or purposes for which the information is kept or is to be used or disclosed.

The requirement is not absolute. The organisation is required to take 'reasonable steps'. What this requires will depend on the individual circumstances of the case. These may include factors like —

- how sensitive the information is
- how recently it was collected
- how quickly the type of information is likely to go out of date
- what the organisation uses the information for
- who the organisation discloses the information to
- how the information will be used by the recipient.

For example, what is required of an organisation to act to ensure accuracy may be greater if the information comprises a record of serious criminal conduct than if it relates to a person's eye colour. And, it is likely to be greater if the organisation is about to make a decision to the detriment of the person based on the information in question, than if it is merely historical information that remains on a closed file.

Protection from misuse, loss, unauthorised access, modification and disclosure

Organisations hold information as trustees for the community. Members of the community have the right to expect that personal information about them will be protected by appropriate records management processes. There is no point putting in place limits on use and disclosure of information if those limits are defeated by poor care of the information they are designed to protect.

Organisations must take reasonable steps to ensure that the personal information they hold is appropriately protected in terms of good records management procedures, good internal security and good external security.

Good records management is important in that appropriate systems protect against misuse or loss of personal information.

Information security is essential to the operations of most organisations for a variety of reasons, including maintaining information privacy. Clear policies and procedures need to be developed and kept under regular review to ensure that security and information privacy requirements are met.

While the focus is frequently on external security, failure to develop good internal security measures can just as easily give rise to inappropriate use and disclosure of personal information.

Complying with IPP 3 is the responsibility not only of the organisation as a whole but also of individual staff members. Organisations should make all staff aware of their responsibilities. Measures staff members may take include taking steps to ensure that—

- computer documents containing personal information are stored in folders with appropriate levels of security;
- personal information is not discussed with other staff, except when there is a legitimate need to do so for the purposes of the organisation;
- computer screens that display personal information are not visible to members of the public, or to staff who have no need to see them;
- conversations that involve personal information are carried out in a place and manner that limits scope for disclosure to other staff and members of the public.

It should be remembered that the requirement is to take reasonable steps. What is reasonable will depend on the individual circumstances, which may include the nature of the information, the costs of the measure, the resources available to the organisation and physical limitations.

Destruction/De-identification

The requirement is to destroy or de-identify personal information when it is no longer needed 'for any purpose'. It is a requirement to take 'reasonable steps'.

A significant limit on this principle is the requirement on public sector organisations to hold records in accordance with approved disposal schedules. Penalties apply for unauthorised disposal of records. Arguably, a record which is not yet available for disposal in accordance with a disposal schedule, cannot be said to be no longer needed for any purpose. So, much personal information will be retained for the purpose of complying with disposal schedules.

Another purpose for retaining personal information beyond day-to-day operational needs will be to ensure that sufficient information is available for the organisation to appropriately record its past activities and to be accountable for its actions and decisions. This may require the retention of some personal information for extended periods. In such cases, it is incumbent on organisations to assess whether the necessary information can be retained in a way that does not identify the person.

.

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