

Short guide to the Information Privacy Principles

The ten Information Privacy Principles (IPPs) are contained in Schedule 1 to the *Privacy and Data Protection Act 2014* (PDPA). With limited exemptions, all Victorian Government organisations, contracted service providers and local councils must comply with these principles. This is a short summary of the IPPs. It is intended to provide a high level guide only. For any detailed privacy analysis, please refer to the full text of the IPPs in Schedule 1 of the PDPA.

- 1 Collection** An organisation can only collect your personal information if it is necessary to fulfill its functions. It must collect information only by lawful and fair means and not in an unreasonably intrusive way. It must provide you notice of the collection, including such things as the purpose of collection and how you can access the information. This is usually done through provision of a Collection Notice that is consistent with an organisation's Privacy Policy. More information on these two documents is available on www.cpdp.vic.gov.au.
- 2 Use and Disclosure** Your personal information can only be used and disclosed for the primary purpose for which it was collected, for a secondary purpose that you would reasonably expect or in other limited circumstances. It is best that the organisation gets your consent, but the law allows some uses without consent, such as law enforcement purposes and to protect safety.
- 3 Data Quality** Organisations must keep your personal information accurate, complete and up to date.
- 4 Data Security** Your personal information must be protected from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify your personal information when it is no longer needed.
- 5 Openness** Organisations must have clearly expressed policies on the way they manage personal information. You can ask to view an organisation's Privacy Policy.
- 6 Access and Correction** You have a right to seek access to your own personal information and to make corrections if necessary. An organisation may only refuse in limited circumstances that are detailed in the PDPA, for example where disclosure might threaten someone's safety.
- 7 Unique Identifiers** Unique identifiers, usually a number, can facilitate data matching. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently by organisations. There are also restrictions that are detailed in the PDPA, on how organisations use unique identifiers assigned by other organisations.
- 8 Anonymity** Where lawful and feasible, you should have the option of transacting with an organisation without identifying yourself.
- 9 Transborder Data Flows** If your personal information travels outside Victoria, your privacy protection should travel with it.
- 10 Sensitive Information** This includes your racial or ethnic origin, political opinions and membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record. The law puts special restrictions on its collection.

Please note that the contents of this information sheet are for general information purposes only, and should not be relied upon as legal advice. CPDP does not guarantee or accept legal liability whatsoever arising from, or connected to the accuracy and reliability of the contents of this document. We encourage your organisation to obtain independent legal advice as necessary.
