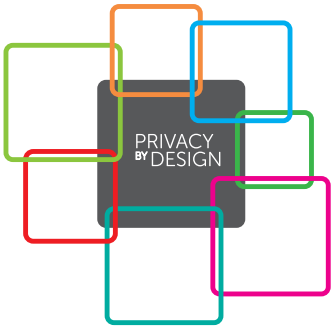

Privacy by Design

The importance of a lifecycle approach involving people and programs.

1 PROACTIVE NOT REACTIVE; PREVENTATIVE NOT REMEDIAL

Establish and monitor governance mechanisms for privacy responsibility.

Promote an organisation-wide 'privacy-culture' to ensure that privacy is integrated into your policies and programs.

'Operationalise' privacy by establishing and implementing privacy policies, conducting privacy awareness training, and developing data breach response protocols in the event that a breach does occur.

Audit and monitor your organisation's information handling processes.

2 PRIVACY AS THE DEFAULT SETTING

Ensure that the necessary privacy controls are built into new systems during the design and procurement phases.

Undertake privacy impact assessments for all projects and programs that involve personal information.

3 PRIVACY EMBEDDED INTO DESIGN

Ensure that a program's overall risk assessment includes an obligation to consider potential privacy risks.

Ensure that programs are signed off with appropriate privacy protections in place prior to a project's commencement.

4 FULL FUNCTIONALITY: POSITIVE-SUM NOT ZERO-SUM

Commit to finding workable solutions to achieve multiple objectives, rather than compromising any interests that seem to be in competition.

5 END-TO-END SECURITY: FULL LIFECYCLE PROTECTION

Ensure that your employees understand – and are able to adhere to – their privacy responsibilities at all times.

Ensure that contractual agreements with third parties and vendors clearly set out obligations and responsibilities, from the commencement of a program through to the point of data destruction.

Map a program's data flows and ensure that security measures are in place at each stage, including user authentication, encryption and destruction of data.

6 VISIBILITY AND TRANSPARENCY: KEEP IT OPEN

Commit to keeping the organisation's practices transparent to the extent possible, without inviting risk.

Seek independent verification for programs and procedures to ensure compliance with privacy obligations.

7 RESPECT FOR USER PRIVACY: KEEP IT USER-CENTRIC

Support an approach to designing programs that considers privacy from a user's point of view.

THE UNIVERSITY OF MELBOURNE

Privacy impact assessment contact- pia-review@unimelb.edu.au
Privacy Coordinator - privacy-officer@unimelb.edu.au
http://www.unimelb.edu.au/governance/compliance/privacy

Commissioner for Privacy and Data Protection

Commissioner for Privacy and Data Protection

Information sheet

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.