Many of the steps and strategies in this guide will also assist you to take reasonable steps to ensure good handling of other types of information, such as commercially confidential information.

The information lifecycle

If you handle personal information, you should consider how you will protect personal information during the stages of its lifecycle.

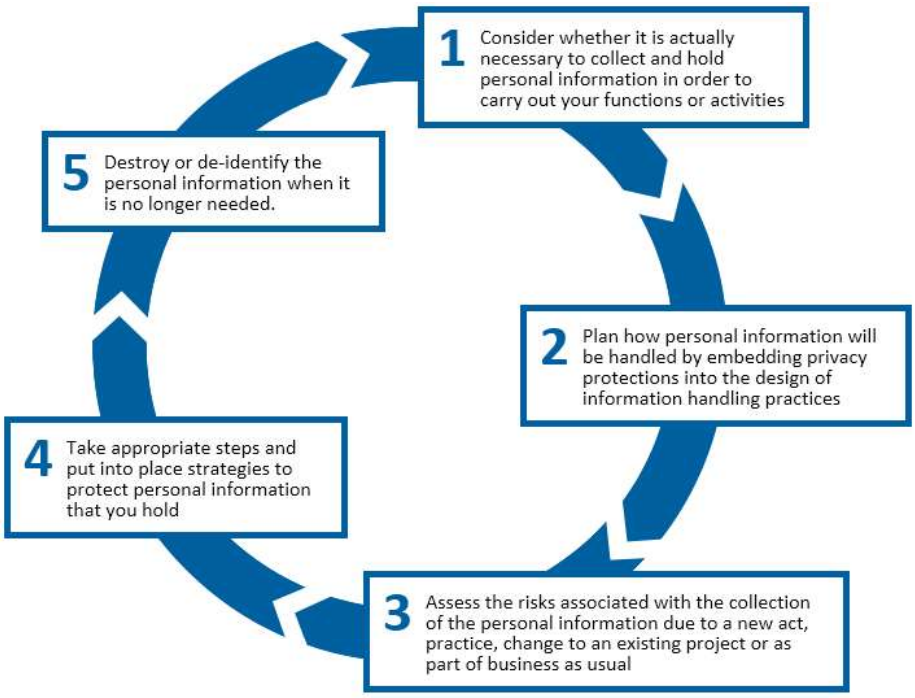
Personal information security throughout the lifecycle involves:

1. considering whether it is actually necessary to collect and hold personal information in order to carry out your functions or activities
2. planning how personal information will be handled by embedding privacy protections into the design of information handling practices
3. assessing the risks associated with the collection of the personal information due to a new act, practice, change to an existing project or as part of business as usual
4. taking appropriate steps and putting into place strategies to protect personal information that you hold
5. destruction or de-identification of the personal information when it is no longer needed.

To effectively protect personal information throughout its lifecycle, you will need to be aware of when and how you are collecting it and when and how you hold it. As noted above, your personal information holdings can be dynamic and change without any necessarily conscious or deliberate action.

Additionally, the lifecycle may include the passing of personal information to a third party for storage, processing or destruction.

The information lifecycle



1. Consider whether to collect personal information

Under APP 3, you should only collect personal information that is reasonably necessary (and for agencies, directly related) to carry out your functions or activities. Over-collection can increase risks for the security of personal information.

Therefore, the first step in managing the security of personal information is to ask whether the collection of personal information is reasonably necessary to carry out your functions or activities.[20] If it is, you should then consider, even if you can collect it, should it be collected? That is, do you really need to collect the personal information or can the collection be minimised?

Personal information that is not collected or is not stored cannot be mishandled.

2. Privacy by design

APP 1 outlines the requirements for APP entities to manage personal information in an open and transparent way. This includes taking reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs. The OAIC refers to

[20] For agencies it can also be collected if it is 'directly related' to its functions or activities.

this as 'privacy by design'.[21] Privacy should be incorporated into your business planning, staff training, priorities, project objectives and design processes, in line with APP1.

You should design your personal information security measures with the aim to:

- prevent the misuse, interference, loss or unauthorised accessing, modification or disclosure of personal information
- detect privacy breaches promptly
- be ready to respond to potential privacy breaches in a timely and appropriate manner.

You will be better placed to meet your personal information security obligations if you embed them early, including by choosing the appropriate technology and by incorporating measures that are able to evolve to support the changing technology landscape over time. You also need to take into account the rapid development of new and existing technologies and platforms when designing your information security policies and systems.

An important element of 'privacy by design' is to integrate privacy into your risk management strategies (see 'Assessing the risks' below). Robust internal personal information-handling practices, procedures and systems can assist you to embed good personal information handling practices and to respond effectively in the event a privacy breach occurs.

3. Assessing the risks

Assessing the security risks to personal information is also an important element of 'privacy by design'. You can assess your personal information security risks by conducting a privacy impact assessment (PIA), an information security risk assessment and regular reviews of your personal information security controls. You should use PIAs and information security risk assessments along with regular reviews so that you are aware of the variety of security risks you face, including threats and vulnerabilities, along with the possible impacts before designing and implementing your personal information security framework. They will also assist you in integrating privacy into your risk management strategies.

PIAs

A PIA is a written assessment that identifies the privacy impacts of a proposal and sets out recommendations for managing, minimising or eliminating those impacts. Generally, a PIA should:

- describe the personal information flows in a proposal
- analyse the possible privacy impacts of those flows

[21] Privacy-by-design was first developed in the 1990s by Dr Ann Cavoukian, former Privacy and Information Commissioner of Ontario, Canada. Since then, it has been adopted by both private and public sector bodies internationally. For further information, see *Privacy by Design* [PDF].

- assess the impact the project as a whole may have on the privacy of individuals
- explain how those impacts will be eliminated or minimised.

A PIA, especially one conducted at the early stage of a proposal's development, can assist you to identify any personal information security risks and the reasonable steps that you could take to protect personal information. A PIA can also be seen as an iterative process during the life of any proposal, being updated to take account of changes to the proposal as it evolves.

A detailed guide to conducting PIAs is available from the OAIC website. The OAIC encourages entities to undertake a PIA for any new proposals across all business activities that involve the handling of personal information.[22] The PIA guide includes a threshold assessment to assist you in determining whether it is appropriate for you to undertake a PIA. It will depend on a proposal's size, complexity and scope and the extent to which it involves personal information. The OAIC also has a PIA eLearning course that aims to help entities to conduct an in-house PIA.

While the PIA guide focuses on undertaking PIAs for new projects, you should also consider applying the same principles across your business generally, including existing business operations, to give a greater understanding of the privacy risks that exist currently. Entities should also consider building the use of PIAs into their risk management processes and plans.

Information security risk assessments

You may also need to conduct an information security risk assessment (also known as a threat risk assessment) in conjunction with a PIA. An information security risk assessment is generally more specific than a PIA because it involves the identification and evaluation of security risks, including threats and vulnerabilities, and the potential impacts of these risks to information (including personal information) handled by an entity. As with a PIA, an information security risk assessment can be seen as an iterative process and may be undertaken across your business generally.

The findings of a PIA and information security risk assessment should inform the development of your risk management and information security policies, plans and procedures.

Once the risks have been identified, you should then review your information security controls (virtual and physical) to determine if they are adequate in mitigating the risks. Given that processes, information, personnel, applications and infrastructure change regularly, and given the constantly evolving technology and security risk landscape, regular review and monitoring of personal information security controls is crucial.

[22] Under s 33D of the Privacy Act, if an agency proposes to engage in an activity or function involving the handling of personal information and if the OAIC considers that the activity or function might have a significant impact on the privacy of individuals, the OAIC may direct the agency to give the OAIC, within a specified period, a PIA about the activity or function.

Risk of human error

Threats to personal information can be internal or external as well as malicious or unintentional. Privacy breaches can arise as a result of human activity or events such as natural disasters. Human error is regularly claimed as the cause of privacy incidents; however entities should assume that human error will occur and design for it.[23] Research has shown that human error can be seen as a trigger rather than a cause of an incident.[24] PIAs, information security risk assessments and regular reviews will enable you to design practices, procedures and systems to deal with the foreseeable risk of human error and minimise its effect.

4. Taking appropriate steps and putting into place strategies to protect personal information

Once your entity has collected and holds personal information, you need to consider what appropriate security measures are required to protect the personal information. This will need to be considered in regards to all of your entity's acts and practices. Part B of this guide sets out examples of key steps and strategies you should consider taking in order to protect the personal information you hold to satisfy your security obligations under the Privacy Act.

5. Destroy or de-identify personal information

Under APP 11.2, APP entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs.[25] This requirement does not apply where the personal information is contained in a 'Commonwealth record' or where the entity is required by law or a court/tribunal order to retain the personal information.

Destroying or permanently de-identifying personal information that you no longer need is an important risk mitigation strategy and is discussed in Part B.

[23] See the Own motion investigation report AICmrCN 5. This case illustrates how the failure to put in place adequate policies, procedures and systems to mitigate the risk of human error can result in a data breach. Failures at a number of levels aligned to create circumstances that enabled a breach to occur.

[24] This approach is based on the 'Swiss cheese' or 'cumulative act effect' model of accident causation which is an illustration of how organisational failures at a number of levels can combine to create a situation in which human error can trigger a data breach. This is a model used in risk analysis and risk management originally propounded by Dante Orlandella and James T. Reason in 1990.

[25] APP 4.3 also requires the destruction or de-identification of unsolicited personal information received by an organisation in certain circumstances.