



# Checklist

## Privacy considerations when using commercially available AI products

### Who is this guidance for?

This guidance is targeted at organisations that are deploying AI systems that were built with, collect, store, use or disclose personal information. A ‘deployer’ is any individual or organisation that supplies or uses an AI system to provide a product or service.

This guidance is intended to assist organisations to comply with their privacy obligations when using commercially available AI products.

### Privacy issue

Are you **using or disclosing personal information** in the context of an AI system?

#### Considerations

To assess whether you will be compliant with your entity’s obligations under APP 6, consider:

- Is the purpose for which you intend to use or disclose the personal information the same as the purpose for which you originally collected it?
- If it is a secondary use or disclosure, would the individual reasonably expect you to use or disclose it for the secondary purpose?
- If it is a secondary use or disclosure, is it related to the primary purpose of collection (or if the information is sensitive information, is it directly related to the primary purpose?)

### Privacy issue

Are you **collecting, generating or inferring personal information** using an AI system?

#### Considerations

To assess whether you will be compliant with your entity’s obligations under APP 3, consider:

- Is the collection or generation reasonably necessary for your entity’s functions or activities?
- Are you collecting or generating personal information using AI only by lawful and fair means?
- Would it be unreasonable or impracticable to collect the personal information directly from the individual?
- If you’re collecting or generating sensitive information using AI, do you have the individual’s consent?



## Privacy issue

Have you taken **reasonable steps to ensure the accuracy** of personal information in relation to the AI system?

### Considerations

To comply with your APP 10 obligations, your organisation should consider:

- Is the personal information being input into the product accurate and of a high quality?
- Do your records clearly indicate where information is the product of an AI output and therefore a probabilistic assessment rather than fact?
- Do you have processes in place to ensure appropriate human oversight of AI outputs, with a human user responsible for verifying the accuracy of any personal information obtained through AI?
- Does your organisation ensure that individuals are made aware of when AI is used in ways that may materially affect them?



**Examples of personal information include a person's name, email address and images or videos where a person is identifiable.**

### Learn more

The OAIC's guidance on [Privacy and the use of commercially available AI products](#) includes practices that organisations that are APP entities must follow to comply with their obligations under the Privacy Act as well as good privacy practice when using commercially available AI products.

## Privacy issue

Has your organisation **put in place appropriate transparency and accountability** measures?

### Considerations

To comply with your organisation's obligations under APP 1 and APP 5, you should consider:

- Have you informed individuals about how their personal information is used in connection with AI, including at the time you collect their information and in your organisation's Privacy Policy?
- Does your organisation have in place procedures and resources to be able to understand and explain the AI systems you are using, and particularly how they use, disclose and generate personal information?

## Privacy issue

What **ongoing assurance processes** need to be put in place?

### Considerations

Your organisation will need to ensure it has established appropriate processes and systems to ensure it complies with its APP obligations throughout the lifecycle of the AI system. Consider:

- Do you have policies in place that outline the permitted and prohibited uses of the system?
- Have you provided appropriate training of staff about the operation of the AI system and the potential privacy and security risks?
- Do you have processes in place to provide ongoing monitoring of AI systems to ensure they are operating as intended? Have you provided for regular audits or reviews?