Australian Government
Office of the Australian Information Commissioner

Checklist

Privacy considerations when selecting a commercially available AI product

Privacy issue

Is the AI system **appropriate and reliable** for your entity's intended uses?

Considerations

To assist with meeting your organisation's privacy obligations, particularly regarding accuracy under APP 10, consider:

- Has the system been tested and proven for your entity's intended uses?
- Do you understand the limitations of the product and whether there are mitigations or safeguards in place?
- Is the intended use of the AI system likely to be a high privacy risk activity, such as making decisions that may have a legal or similarly significant effect on an individual's rights?
- If there is a high privacy risk, will the product be appropriate and produce accurate outputs? Will your organisation be able to understand and explain these outputs and how the system works?

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

Can you **clearly identify the data** that the system has been trained on, to ensure that its output will be accurate?

Considerations

To help assess whether your use of the AI system will be compliant with your APP 10 obligations:

- Do you understand where and how the system has been trained?
- Are the training datasets appropriate and relevant to your entity's purposes and functions?
- Has your organisation carried out testing to identify the risk of inaccurate responses?

Privacy issue

What are the **potential security risks** associated with the system?

Considerations

It is important to consider your entity's security obligations under APP 11 when selecting an AI product. Consider:

- Can you find information about any past security incidents for the system?
- What security measures have been put in place by the developer to detect and protect against threats and attacks?

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

What is the **intended operating environment** for the AI system?

Considerations

As part of assessing your APP 11 obligations, consider:

- Will the AI system will be integrated into your entity's systems and have access to its documents?
- Will the product be hosted through the cloud? If so, what are the privacy and security risks in relation to this?

Privacy issue

Will your **inputs be accessible** by the system developer?

Considerations

Your use of the AI system must be compliant with your APP 6 obligations regarding the disclosure of personal information. Ensure you understand:

- Do the system's terms of use allow the developer access to personal information input into, or generated by, the system?
- If so, can your organisation opt-out or place controls around the use of the system?