Australian Government
Office of the Australian Information Commissioner

# Top five takeaways

## Privacy considerations when using commercially available AI products

**1** **Privacy obligations will apply to any personal information input into an AI system, as well as the output data generated by AI (where it contains personal information).** When looking to adopt a commercially available product, organisations should conduct due diligence to ensure the product is suitable to its intended uses. This should include considering whether the product has been tested for such uses, how human oversight can be embedded into processes, the potential privacy and security risks, as well as who will have access to personal information input or generated by the entity when using the product.

**2** **Businesses should update their privacy policies and notifications with clear and transparent information about their use of AI,** including ensuring that any public facing AI tools (such as chatbots) are clearly identified as such to external users such as customers. They should establish policies and procedures for the use of AI systems to facilitate transparency and ensure good privacy governance.


**3** **If AI systems are used to generate or infer personal information, including images, this is a collection of personal information and must comply with APP 3**. Entities must ensure that the generation of personal information by AI is reasonably necessary for their functions or activities and is only done by lawful and fair means. Inferred, incorrect or artificially generated information produced by AI models (such as hallucinations and deepfakes), where it is about an identified or reasonably identifiable individual, constitutes personal information and must be handled in accordance with the APPs.

**4** **If personal information is being input into an AI system, APP 6 requires entities to only use or disclose the information for the primary purpose for which it was collected**, unless they have consent or can establish the secondary use would be reasonably expected by the individual, and is related (or directly related, for sensitive information) to the primary purpose. A secondary use may be within an individual's reasonable expectations if it was expressly outlined in a notice at the time of collection and in your business's privacy policy.

**5** **As a matter of best practice, the OAIC recommends that organisations do not enter personal information, and particularly sensitive information, into publicly available generative AI tools**, due to the significant and complex privacy risks involved.

*This document is a summary only and should be considered together with the OAIC's Guidance on privacy and the use of commercially available AI products.*

OAIC