QUAY INSIGHTS   February 2025

The Privacy Commissioner's guidance on generative AI: Part II – Guidance for AI Deployers

The Privacy Commissioner has published two sets of guidelines relevant to generative AI models: *Guidance on privacy and the use of commercially available AI products (**Guidance for AI Deployers**)*, targeted at the deployers and users of AI, and *Guidance on privacy and developing and training generative AI models (**Guidance for AI Developers**)*, targeted at developers of AI products. Each guide details how the Australian Privacy Principles (**APPs**) in the Privacy Act apply to the contexts that arise when using AI and when developing AI models and systems.

This Quay Insight summarises the Privacy Commissioner's Top 5 Takeaways in the Guidance for **AI Deployers** that are APP entities under the Privacy Act.

Top 5 privacy takeaways for AI Deployers

The Privacy Commissioner presents 5 top takeaways to AI deployers in meeting their privacy obligations:

1.   **Privacy by design** – Privacy obligations apply to any personal information input into an AI system as well as personal information generated by AI. When choosing an AI product, entities should consider whether it has been tested for the relevant uses, how human oversight can be embedded into processes, the potential privacy and security risks, and access controls over the input or output containing personal information.

     This points out that entering personal information into AI is a use or disclosure of personal information under the Privacy Act, and receiving personal information from AI is a collection of personal information. As such, entities should apply privacy by design practices when commissioning a new AI system, map the data flows and instil privacy positive practices at each point in the data cycle.

2.   **Transparency** – Entities should update their privacy policies and notifications with clear and transparent information about their use of AI. Any public facing AI tools should be clearly identified to users and the entity should have policies and procedures for how AI systems are used.

This takeaway touches on an entity's obligations in APP 1 to manage personal information in an open and transparent manner, including by having a clearly expressed and up-to-date privacy policy and by implementing practices, procedures and systems to ensure compliance with the APPs. It also highlights the obligation in APP 5 to take reasonable steps to notify individuals of a range of matters about the collection of their personal information.

3. **Collection compliance** – This takeaway reiterates that the generation of personal information from AI outputs, including images, amounts to a collection of personal information which must comply with APP 3. That means deployers must ensure the personal information generated is reasonably necessary for their functions or activities and is only done by lawful and fair means.

   Note in particular, collection may be found to be unfair if it is unreasonably intrusive or involves intimidation or deception. The Privacy Commissioner expressly mentions in the Guidance for Deployers that covert collection, that is, without the knowledge of the individual, would usually amount to unfair collection.

4. **Privacy purpose or reasonably expected secondary purpose** – AI deployers entering personal information into AI systems must only do so for the primary purpose for which the information was collected, unless they have consent or can establish the secondary use would be reasonably expected by the individual and the purpose is related (or directly related for sensitive information) to the primary purpose.

   This takeaway is about the obligation in APP 6. Notably, the Privacy Commissioner expressly states that a secondary use may be within an individual's expectations if it was expressly outlined in a collection notice and in the entity's privacy policy, again highlighting the significance of compliance with transparency and notification obligations in APP 1 and APP 5. However, the Privacy Commissioner also cautions entities that there may be challenges in establishing a person had a reasonable expectation that personal information would be used for a secondary AI-related purpose, given the privacy risks posed by AI systems and strong levels of community concerns about AI risks. Consent may be a clearer way to comply in such cases though equally there may be difficulties relying on *implied* consent and whether that is a viable option would need to be considered in all of the circumstances.

5. **Avoid inputting personal information in public AI** – The final takeaway is a recommendation that entities do not input personal information, in particular sensitive information, into publicly available generative AI tools**.** The Privacy Commissioner considers that this practice involves significant and complex privacy risks.

What should AI Deployers do?

The Guidance for AI Deployers provides valuable insight into how the Privacy Commissioner intends to apply the APPs in the event that an entity using AI is investigated by the regulator. The Privacy Commissioner has spoken publicly about addressing AI harms as a priority and has stated that the OAIC is developing a regulatory strategy in the field of generative AI. Given these comments and the recent publication of the guidance, AI deployers are on notice of the potential for regulatory enforcement action in this space in 2025.
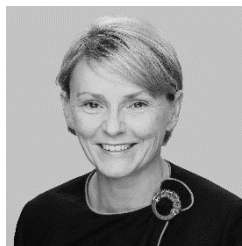
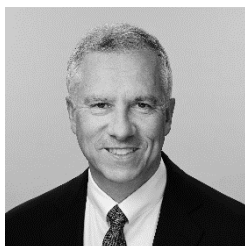## Contacts

QLP

Cate Cloudsdale
Counsel

Quay Law Partners
Level 32, 180 George Street,
Sydney NSW 2000
T +61 461 477 550
E cate@quaylaw.com
www.quaylaw.com

Angela Flannery
Partner

Quay Law Partners
Level 32, 180 George Street,
Sydney NSW 2000
T +61 419 489 093
E angela@quaylaw.com
www.quaylaw.com

Dave Poddar
Partner

Quay Law Partners
Level 32, 180 George Street,
Sydney NSW 2000
T +61 422 800 415
E dave@quaylaw.com
www.quaylaw.com