ACC: Privacy and Data Security for Churches

Webinar

August 2025

Presented by Simon Mason, Senior Associate

VOCARE LAW

Introduction

CORNEY & LIND
LAWYERS

→

VOCARE
LAW

A little about us...

Same

- Same team, same mission
- Still called to deliver Just, Redemptive Outcomes®
- General practice of law with a particular focus on not -for-profit & charity law.

Different:

- Name change - Vocare (pronounced vo -ka-ray); latin meaning "to be Called.
- Additional new office in North Ryde, Sydney.

Note

This training is provided for professional development purposes only.

The material in this training does not constitute legal advice.

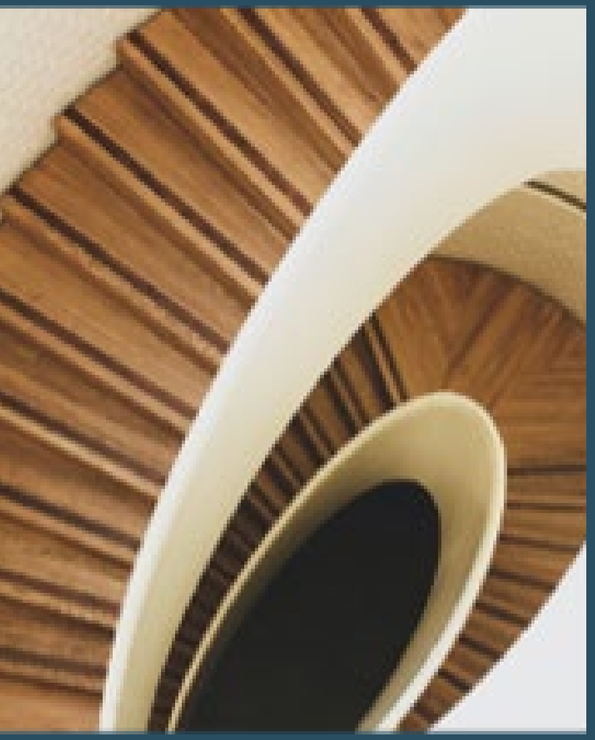
If you have a legal concern or matter you should consult with an appropriate practitioner.

Topics

1. Understanding AI
2. Use Cases for Churches
3. Legislation
- APP
- Recording
- Conversations
4. Upcoming Changes

Artificial intelligence provides significant benefit for time saving and increased efficiency. However, there are a number of specific pitfalls that ought to be considered before utilizing AI powered tools in the context of churches.

What is Artificial Intelligence?



- Nominally, Artificial intelligence (AI) refers to the ability of computer systems to perform tasks that typically require human intelligence, such as learning, reasoning, and problem-solving.

- Strictly, an AI system is not an intelligence per se, but rather a sophisticated language emulator, that is, a Large Language Model. There is no judgement being applied. Rather the results emulate the responses human intelligence might provide. AI results that appear to display reasoning are volume effects from large training data pools.

Why Now?

- Three factors have powered the AI Revolution
  - Big Data
  - Machine Learning and Automation advances
  - Increases in Computing Processing Power

  The software is still deeply rudimentary.

Generative AI

- Generative AI is a type of artificial intelligence that uses machine learning to create new content like text, images, audio, and videos, by learning from existing data and generating new outputs that reflect the characteristics of the training data
  - Chat GPT, DeepSeek etc
  - Generative AI is trained on datasets, mostly from westernised and English data sets in the public (or at least, semi - public) domain.
  - A dataset is limited information.
  - Information behind paywalls or not in the public domain is generally excluded (or at least not disclosed to constitute part of the training data).

Extractive AI

- Summative/Extractive AI is a type of artificial intelligence that focuses on identifying and extracting key information from existing data sources. Unlike its generative AI counterpart, which creates new content, extractive AI excels at finding and summarising relevant information within documents, databases, and other structured or unstructured data formats (including recordings).
  - Ie. Patient Notes, etc.
  - Summative AI is also trained on public data and will have a clear orientation to processing data from a westernised perspective.
  - There are shortcomings in Summative AI that may not be readily apparent.

Use Cases for Churches

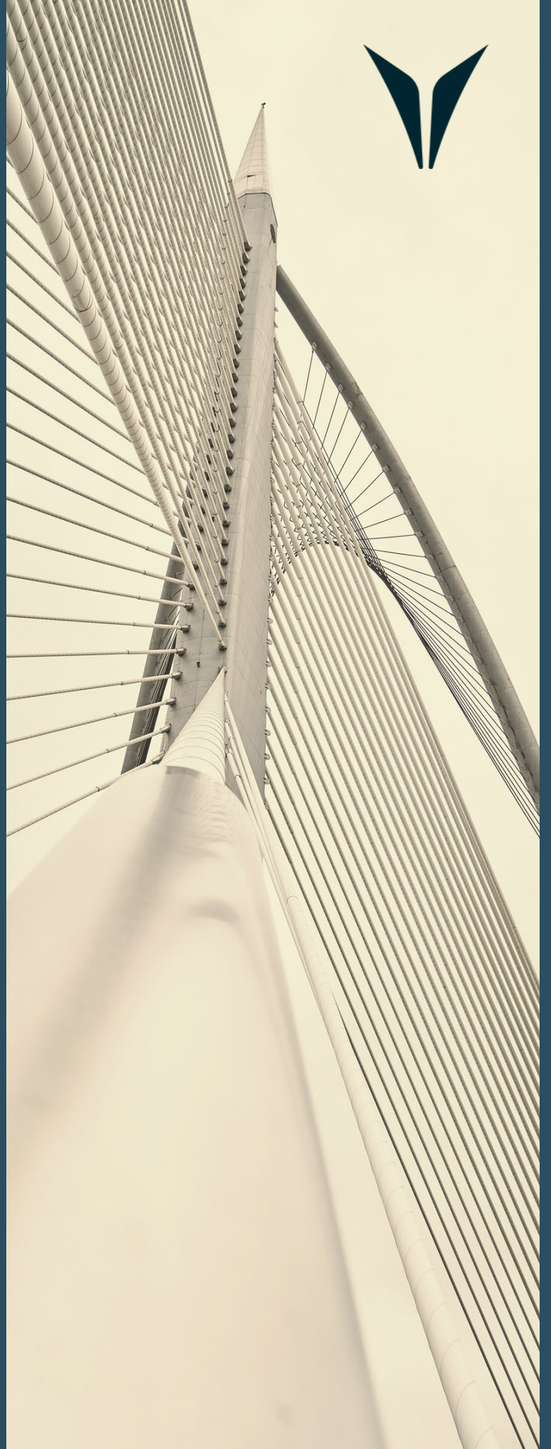
- Generative AI
  - Drafting letters and reports.
  - Drafting sermons.
  - Drafting public correspondences.

- Extractive AI
  - Counselling Note-taking Software.
  - Recording and summarising meetings.

- Future Use Cases
  - Integrations with Management Software.

CAN I RECORD CONVERSATIONS?

A large number of AI tools require recording either integrated into the video conferencing software or alternatively independently through associated apps.

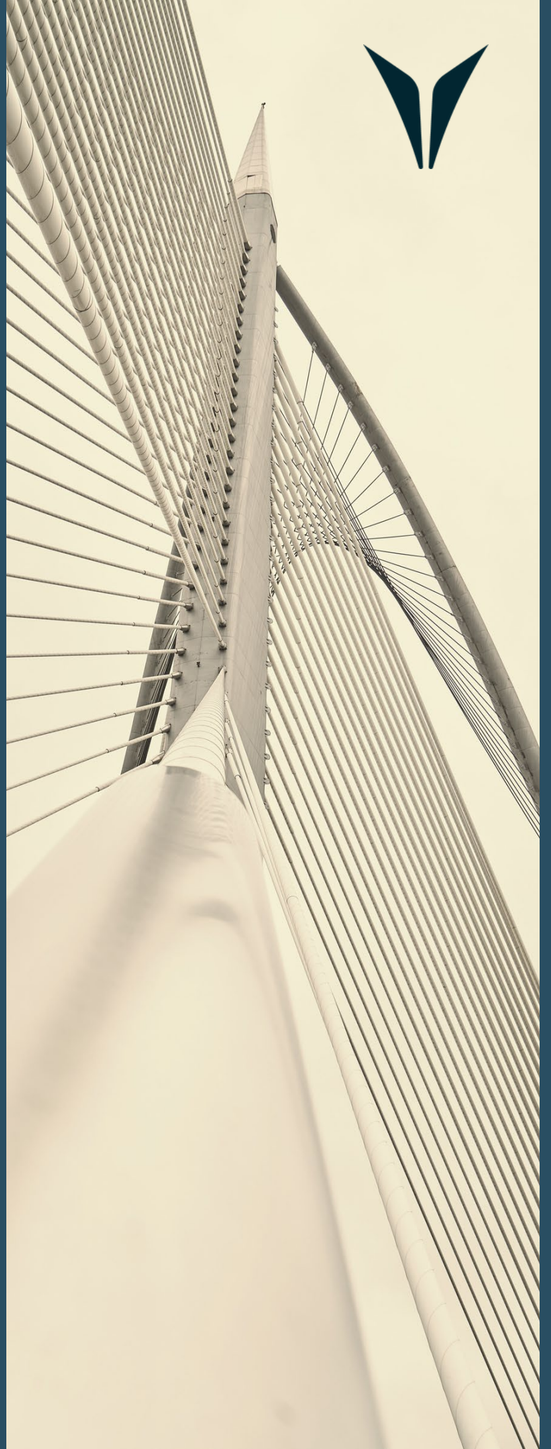


Can I record Conversations?

The Telecommunications (Interception and Access) Act 1979 (Cth Act) prohibits the use of devices to “intercept” communications transmitted over a telecommunications system. Section 6(1) states:

(I)nterception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

This includes any inbuilt recording software on videoconferencing (ie. Zoom AI). Likely does not include recording on a separate device separately to the videoconferencing device.

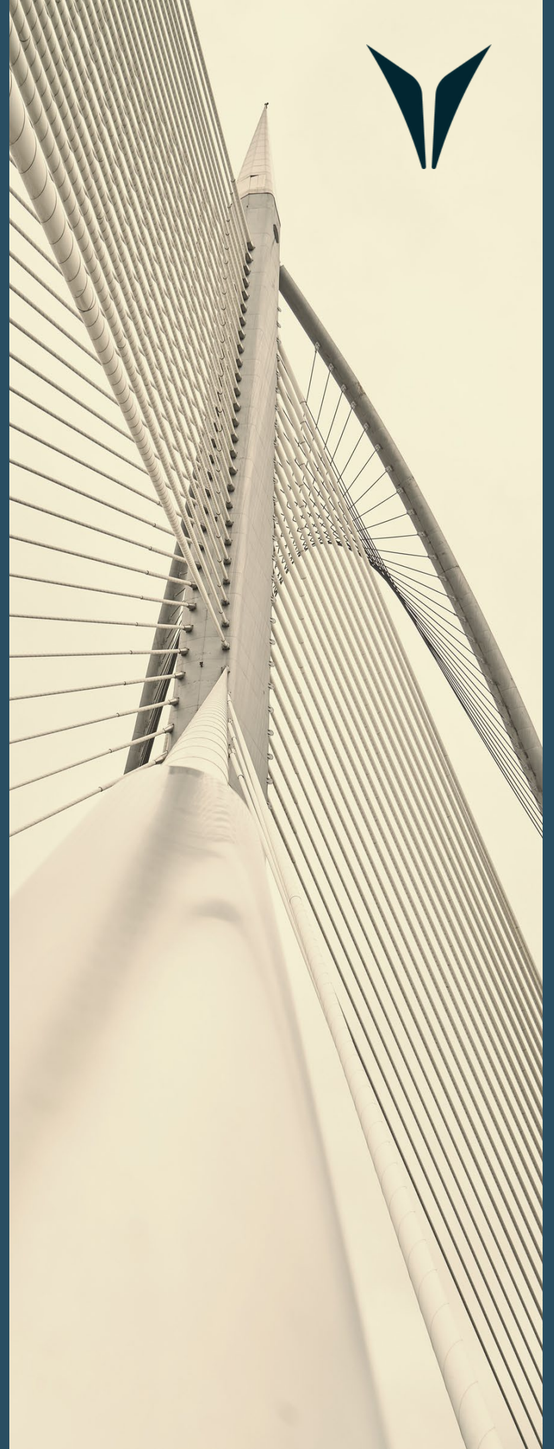


Can I record Conversations?

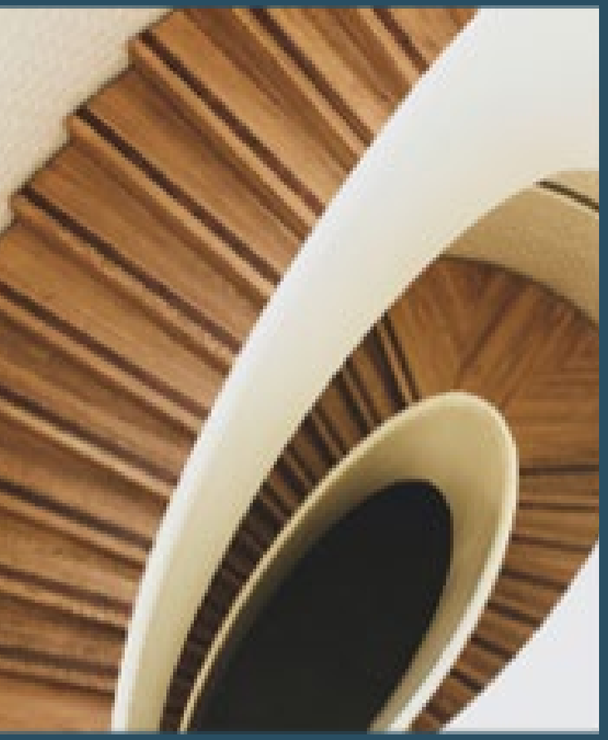
Most states and territories prohibit recording conversations without two party consent:

Section 5 (1) of the Surveillance Devices Act 1998 (WA)
Section 7 of the Surveillance Devices Act 2007 (NSW)
Section 6(1) of the Surveillance Devices Act 1999 (Vic)
(the exception is Queensland).

Generally, these provisions will prohibit any recording of another person absent consent. While they may permit implied consent as a defense, it is prudent to ensure consent is explicit and informed.



The Privacy Act 1988 (Cth)

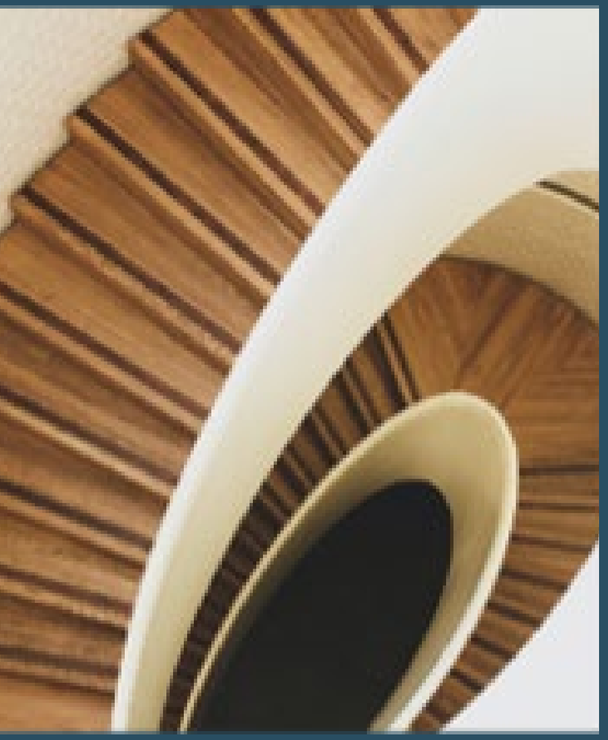


The Privacy Act 1988 (Cth) places significant emphasis on the protection of Personal Information.

The Act applies to all entities unless it is a small business operator.

In general, a small business operator is an individual (including a sole trader), body corporate, partnership, unincorporated association or trust that has an annual turnover of $3,000,000 or less for a financial year.

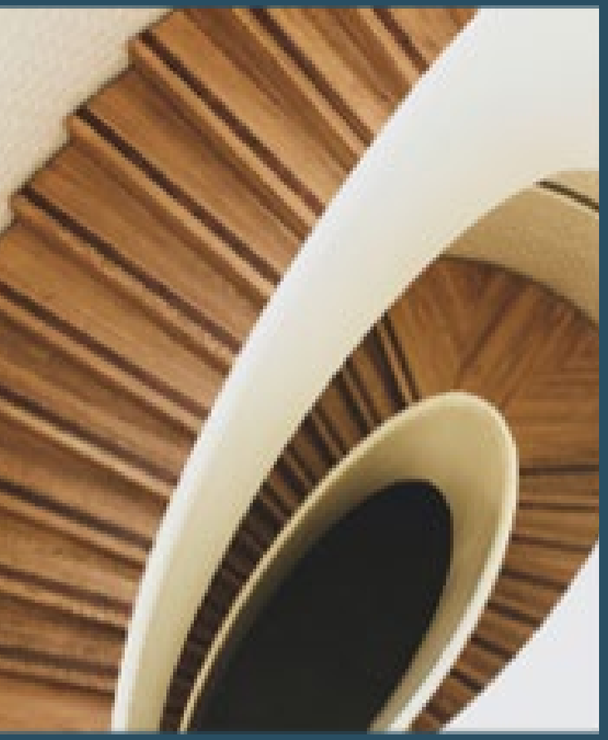
Ethical Obligations



Even if you do not fall within definition of an APP entity, The church should still consider its broad ethical obligations in handling its congregation members' personal information.

To this extent, the APP is normative in that it sets out standards of behavior.

Do I need a Privacy Policy



Yes. If you are an APP Entity. APP 1.3 states:

An APP entity must have a clearly expressed and up to date policy (the APP privacy policy) about the management of personal information by the entity.

A privacy policy is a statement that explains in simple language how a practice handles your personal information in accordance with the APP.

13 Privacy Principles:

Open and transparent management of personal information

Anonymity and pseudonymity

Collection of solicited personal information

Dealing with unsolicited personal information

Notification of the collection of personal information

Use or disclosure of personal information

Direct marketing

Cross-border disclosure of personal information

Adoption, use, or disclosure of government -related identifiers

Quality of personal information

Security of personal information

Access to personal information

Correction of personal information

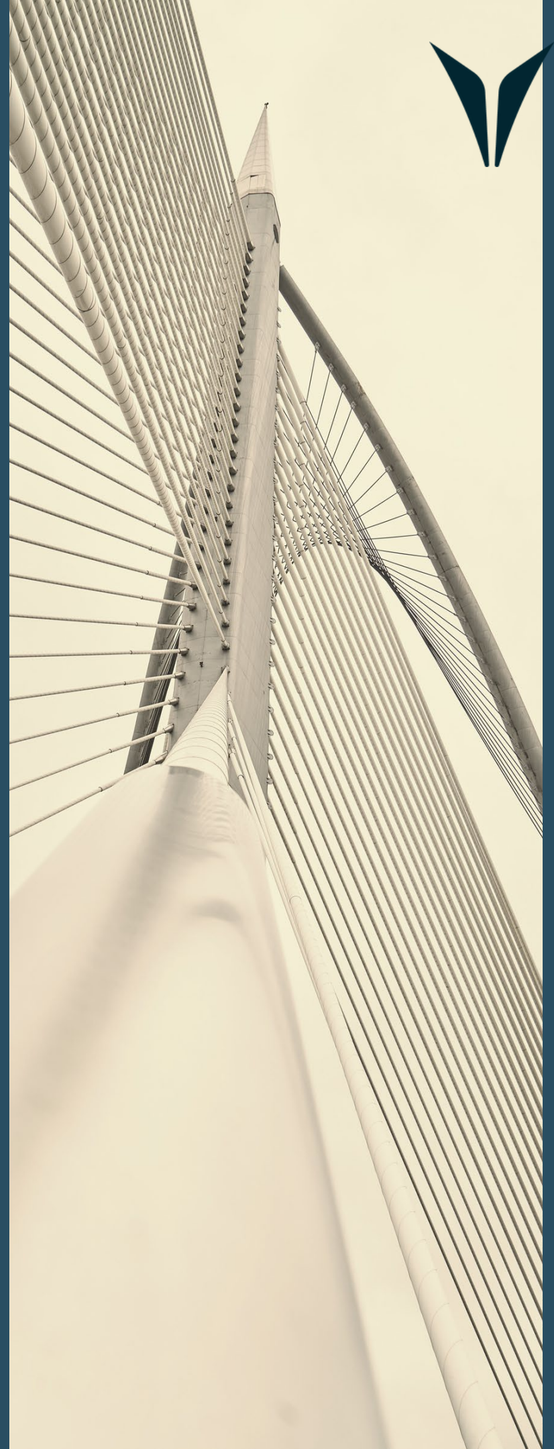
Why are the APPs relevant to Artificial Intelligence?

Community expectations may not be open to general use of AI in delivery of pastoral services or in relation to personal information. Thus consent to uses of AI in relation to personal information will be required.

AI Applications will frequently store personal information. This may be stored outside Australia. Consent will be required.

AI systems may seek to use sensitive personal information in its training data. This is a disclosure and may be problematic.

AI programs may not permit the kind of corrections the APP requires data storage systems to include.



Principles of the APP

- An APP entity must not collect personal information unless it is reasonably necessary or directly related to its function or activities (APP 3).
- If that information is sensitive, namely health information, you must obtain consent to the collection (APP 3).
- At the time of collecting that information, you should let the person know why you are collecting the information (APP 5).

Principles of the APP

Personal Information defined in the APP includes an individual’s name, signature, address, phone number, or date of birth.

Sensitive Information is a subset of personal information and includes information relating to a person’s health, religious beliefs, and political opinions.

Principles of the APP

General Principle:

You will need consent to collect Personal Information (& Sensitive Personal Information).

You need to explain the reason for collection of Sensitive Personal Information at the time of collection

Principles of the APP

Do I Need Consent to use AI to access or otherwise process Personal Information?

Principles of the APP

You should only use and disclose that information for the reason you said you were collecting it (APP 6).

If you want to use or disclose the information for any other reason, you should obtain consent (APP 6).

APP 6 – Use & Disclosure of Personal Information

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.

APP 6.1: If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

the individual has consented to the use or disclosure of the information; or

the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is (if the information is sensitive information) directly related to the primary purpose; or

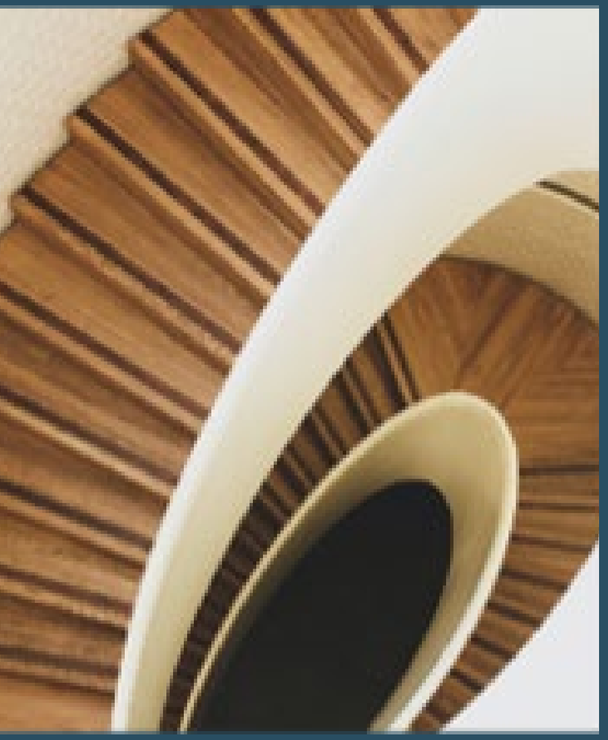
APP 6 – Use & Disclosure of Personal Information

In most cases the primary purpose of information collected by a church would be delivery of pastoral services and or notification of events.

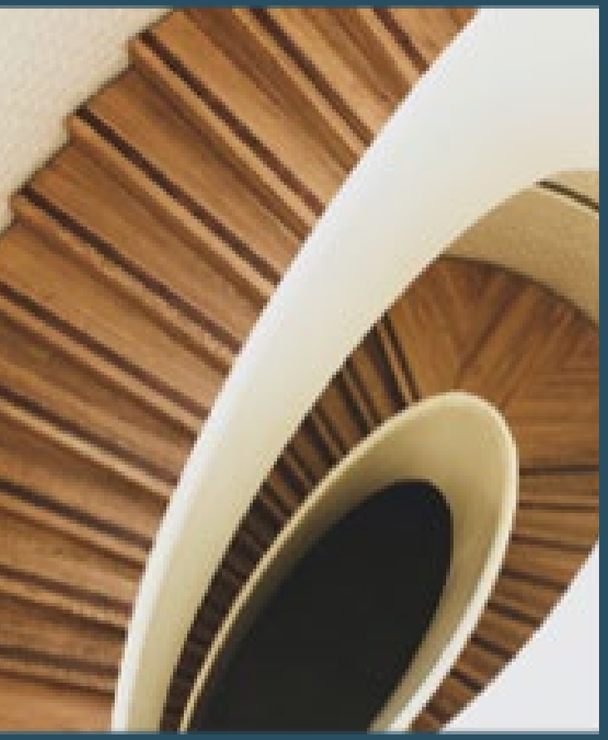
Is use of AI software directly related to the delivery of pastoral services?

It is arguable (by a potentially aggrieved member) that the secondary purpose is not reasonably expected.

Prudently you will need a system of informed consent (and an opt-out process) to utilise AI software. This requires explicit informed consent to AI software.



If consent is received to use AI, does this extend to use of AI linked to Public Training Datasets?

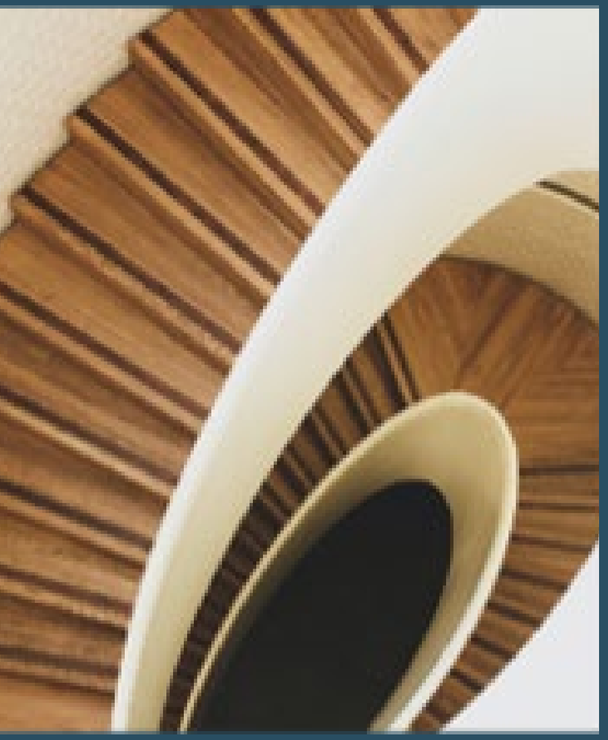


Closed AI training data: Some commercial AI products will include terms or settings that allow the product owner to collect the data input by customers for further training and development of AI technologies. Unless indiviudals specifically consent to disclosure of their data for use by a training model, this will be a breach of the APP.

Public AI training data: Given the ambiguity in use, exceptional care should be taken with personal information.

QUESTION: Can we input de-identified data into an open AI system?

ANSWER: With significant care.



General Principle:

If you are intending to use AI that utilises the inputs in its training data you should seek explicit consent for this as it equates to publishing data online.

Use of redacted data still requires considerable care.

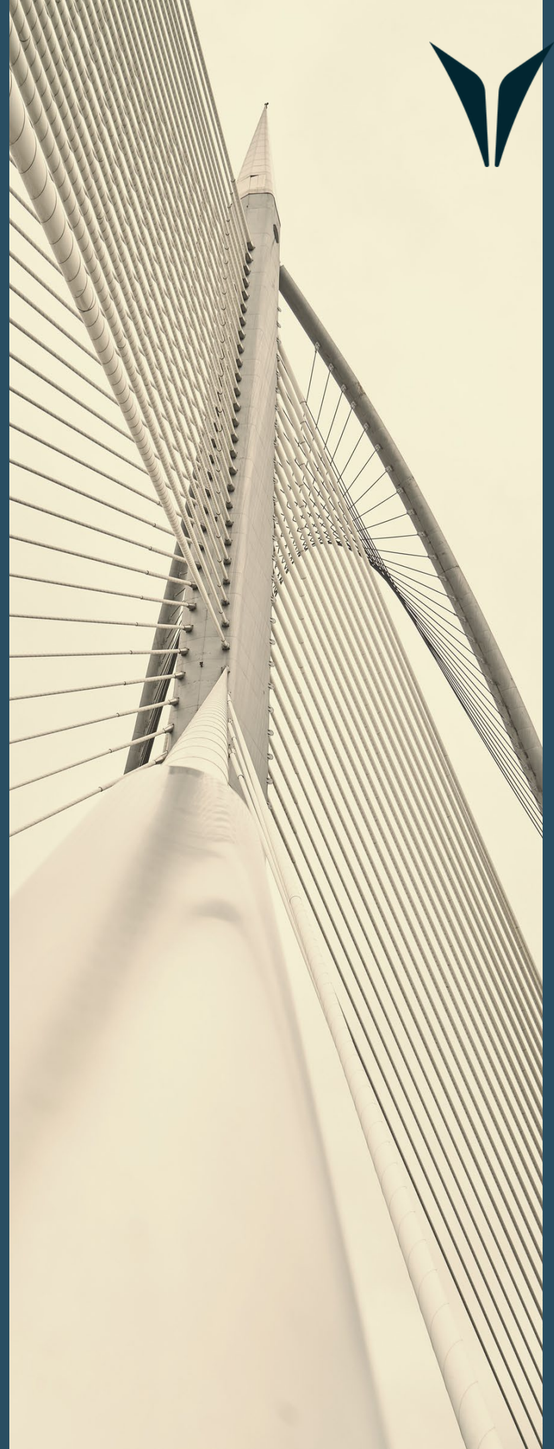
Is It Relevant Where The AI Program Is Geographically Located?

APP 8 – Cross Border Disclosure & Data Storage

Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information (APP 8.1).

An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (s 16C).

Most Software Providers will be offshore.



APP 8 – Cross Border Disclosure & Data Storage

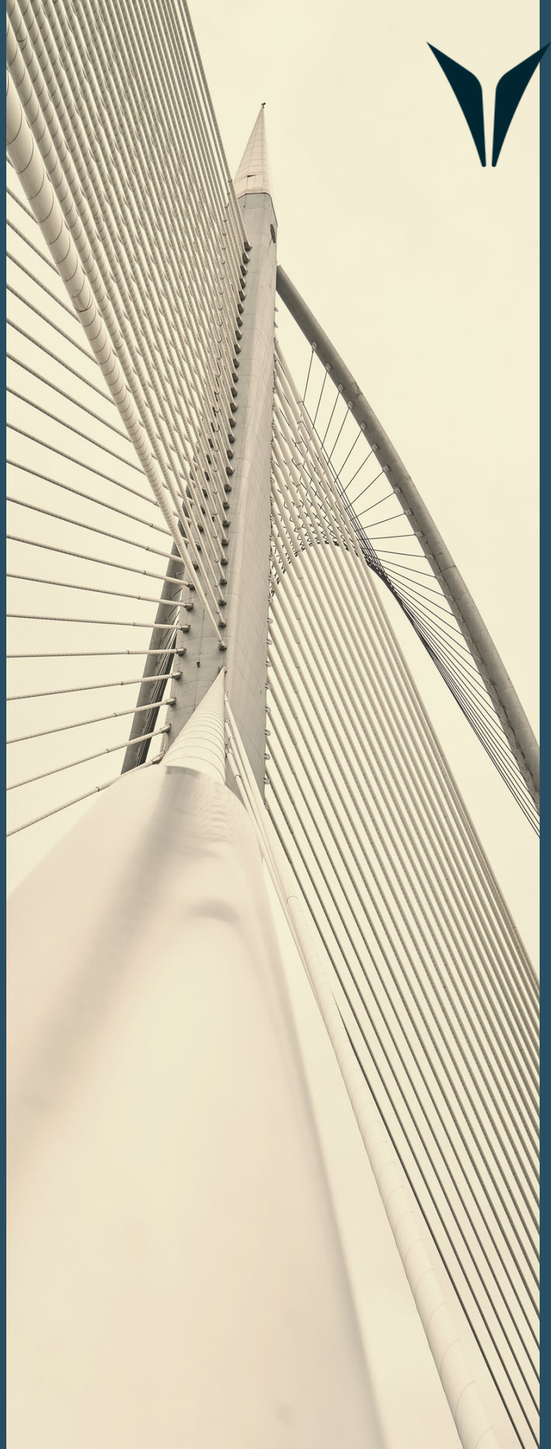
General Principle:

You should confirm the AI Software explicitly states:

It is subject to the APP; or,

It sets out that users have right equivalent to or better than the APP rights.

Notwithstanding, you should prudently seek consent for offshore disclosure.



Is Data Security Relevant?

APP 11 - Security

APP 11:1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

Is Data Security Relevant?

Risk of a Data Breach

The OAIC keeps a record of Notifiable Data Breaches.

From January to June this year, OAIC received 527 data breach notifications. This is the highest number of notifications received since July to December 2020 and an increase of 9% compared to the previous 6 months.

Is Data Security Relevant?

The Office of the Australian Information Commissioner (OAIC) plays a role in overseeing the handling of personal information. The OAIC has released helpful guidelines on maintaining compliance with Privacy Laws in the use of commercially available AI tools.

https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products

Summary

To comply with your ethical obligations and your APP obligations, you will need consent:

To record (or use any software that functionally records) a conversation.

To collect sensitive personal information.

To utilise AI software for the overall purpose of delivering psychological services.

To store data offshore (if relevant).

For the sake of ensuring the consent is informed, you may wish to provide detail on the software or steps taken.

Does my Website need a Separate Privacy Policy?

- Quite Possibly.
- Website Privacy Policy, Enquiries, Cookies, Unsolicited Emails, Other information collected in the course of running a website.
- Internal Privacy Policy for personal information, Contractors and Employees.

Recent Changes

Tranche 1:

- a new statutory tort for serious invasions of privacy;
- a tiered penalty regime to capture a broader range of contraventions;
- stronger privacy protections for children (Children's Online Privacy Code commencing 1 December 2026);
- new transparency obligations around automated decision-making;
- enhanced regulatory powers for the Office of the Australian Information Commissioner (OAIC); and
- a requirement that businesses take steps that include "technical and organisational measures" to protect personal information.

Recent Changes

Businesses that have arranged for a ‘computer program’ – a broad term encompassing pre-programmed rule-based processes, AI and machine learning processes – to make decisions that could ‘reasonably be expected to significantly affect the rights or interests of an individual’ will be required to disclose this in their privacy policies. This includes detailing the types of personal information used and whether decisions are fully automated or substantially assisted by AI.

Recent Changes

Infringement notices may now be issued by the OAIC without going to court, for minor ‘administrative’ failures where failure to meet the requirement can be easily established. These notices are intended to allow the OAIC to seek penalties against entities for minor contraventions, without the need to engage in litigation. Infringement notices can be issued for up to $66,000 for publicly listed companies, but multiple failures may "stack" on top of one another.

Examples of issues that might be dealt with by an infringement notice include:

- inadequate privacy policies (APP 1.3, 1.4)
- failure to correct personal information when requested (APP 13.5)
- inadequate notifiable data breach statement (Section 26WK(3))

VOCARE

LAW

Thank you.

Simon Mason

Senior Associate

1300 862 529

vocarelaw.com.au