Artists, privacy and the private sector

Introduction

The *Privacy Act 1988* (Cth) (**Privacy Act**) deals with information privacy rights and how the organisations and government agencies that are covered by the Privacy Act must handle personal information. It consolidates the previous 'National Privacy Principles' and 'Information Privacy Principles' into 13 Australian Privacy Principles (**APPs**) which regulate the collection, use, storage and disclosure of personal information by covered entities, including how personal information can be used for direct marketing and whether information can be disclosed overseas.

It's important that artists and people in creative industries are aware of the expectations and standards of Australia's privacy laws. While most artists and creatives may not consider their work to involve the handling of data, the reality is that artistic practice and creative businesses often *do* involve personal information. This can take the form of collecting and sharing email addresses for a newsletter, photographing street scenes or using surveillance in exhibition spaces.

In an increasingly digital world, the Privacy Act and its latest amendments (most recently through the *Privacy and Other Legislation Amendment Act 2024* (Cth)) reflect growing concerns about how personal information can be used:

Penalties for serious or repeated breaches for individuals are up to $2.5 million and, for companies, is calculated at the greater of $50 million or three times the value of any benefit obtained through the misuse of personal information or 30% of the company's turnover	New penalties for less serious breaches, up to $66,000 for individuals and $330,000 for companies
Increased powers to the Office of the Australian Information Commissioner (**OAIC**) to issue infringement notices and conduct investigations	A new statutory tort for serious invasions of privacy (as set out in more detail below)

Are you caught under the Act?

The Privacy Act applies to 'organisations', which include individuals, bodies corporate, partnerships, unincorporated associations and trusts". This definition can include not for profits and co-operatives.

Relevant to creative industries, the Privacy Act specifically exempts organisations with an annual turnover of $3 million or less, classifying them as "small businesses". This means that organisations of this size are not subject to the Privacy Act.

Despite the general exemption, the Privacy Act applies to small businesses in certain circumstances, for example where the small business:

- **trades in personal information** in exchange for any benefit, service or advantage ;
- **is related to a larger entity with** an annual turnover greater than $3 million;
- **collects personal information on behalf of another entity** for a benefit, service or advantage;
- **provides health services** and holds health information (other than employee records); or
- **acts as a contracted service provider** for a Commonwealth government contract.

This could capture the following scenarios:

© 2026 Arts Law Centre of Australia

A small theatre company enters a sponsorship deal with a sponsor corporation, and as part of that deal the theatre's customer list is passed to the sponsor corporation	A creative studio or arts organisation offers wellness-related services (for example, dance therapy or performance coaching that collects health data) it may be deemed a health services provider	A photographer is contracted to take portraits for a local council's campaign
A podcaster collects detailed analytics and demographic information through its app or website and shares that data with advertisers to monetise the show	A small gallery installs facial recognition technology for security reasons during events	A small, independent record label runs an online store and uses customer purchase history to create targeted advertising campaigns through a third-party platform

Opt-in provision:

Small businesses otherwise exempt can choose to be treated as an organisation under the Privacy Act by opting in. The OAIC maintains a public register of businesses that have opted in and businesses may later decide to opt-outby submitting written notice .

The exemptions under the Privacy Act:

Some activities and entities are specifically exempt from the Privacy Act, including:

- **employee records exemption:** acts or practices directly related to a current or former employment relationship , though the exemption does not cover information beyond the employment relationship, records regarding unsuccessful applicants and contractor or records;
- **media organisations:** acts done in the course of journalism, provided the media organization commits to observing privacy standards; and
- **political entities:** registered political parties, , members of Parliament, local government councillorsand their contractors, subcontractors and volunteers

State and Territory privacy laws:

State and territory government agencies are subject to local privacy laws (where they exist). In the ACT, for example, the *Information Privacy Act 2014* (ACT) sets out privacy principles similar to the APPs.

What information is caught under the Act?

The Privacy Act specifically relates to the collection, handling and use of 'personal information' of individuals. The Privacy Act defines 'personal information' as "information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a. whether the information or opinion is true or not; and
b. whether the information or opinion is recorded in material form or not.

'Personal information' therefore includes any form of data that has the ability to identify an individual. For example, it would include information like a person's phone number, email address, postal address, income bracket, marital status, name of partner and name of any dependants or children, as long as such information can be linked to an identifiable individual.

© 2026 Arts Law Centre of Australia

The following things will be considered when establishing whether an individual is reasonably identifiable from the information:

How much and what kinds of information were collected?	How was the information collected?
Whether the information is accessible and to whom?	Could the person be identified by a reasonable member of the public is the information was publicly released?

The Privacy Act prevents the use of a tax file number as an identifier, and individuals have the right to withhold this information. Where a tax file number is provided, its use is usually limited to tax-related, assistance agency and superannuation purposes. The Privacy Act also strictly governs the handling of credit reports and other credit worthiness information about individuals by credit reporting agencies and credit providers.

As mentioned above, the Privacy Act also protects all records if they are held by an organisation that is a health service provider, even if the organisation's annual turnover is less than the $3 million threshold. Additionally, there is a general exemption for the handling of employee records that is directly related to a current or former employment relationship. Any health information in those employee records would usually be covered by the exemption.

In some circumstances a person's image could be regarded as 'personal information' and its publication by an entity subject to the Privacy Act would breach that Act. The website of the Office of the Australian Information Commissionerdiscusses this issue in more detail.

Please note that there are also obligations under the various State and Territory legislation that are separate and additional to the obligations in the Privacy Act. In Victoria, for example, the *Health Records Act 2001* imposes obligations on the collection and handling of health information, despite the fact that the organisation may be exempt from compliance with the Privacy Act.

What are the obligations?

Once an organisation falls within the definition of an APP entity, the Privacy Act requires that the organisation complies with the 13 APPs. The APPs are legally binding principles which set the basic standard for privacy protection and stipulate how organisations can collect, use and disclose personal information.

In essence, the APPs require an organisation to take reasonable steps to advise individuals that it is collecting personal information about them, the purpose for which it is collecting the information and who it might pass that information on to. The APPs also impose restrictions on how personal information can be used and when it can be disclosed or transferred overseas. Generally, individuals will have the right to get access to their personal information held by an organisation and to have that information corrected.

The APPs include:

APP	**What it addresses:**	**What it says:**
APP 1	**Open and Transparent management of personal information**	Sets out the requirements for a privacy policy and requires entities to take reasonable steps to make their policies freely available. APP 1 also establishes a compliance framework requiring entities to take reasonable steps to implement practices, procedures and systems relating to the entities activities that will ensure compliance with the APPs.

© 2026 Arts Law Centre of Australia

APP 2	**Anonymity and pseudonymity**	Requires entities to provide individuals with the option of dealing with an APP entity anonymously or through the use of a pseudonym unless it is impracticable for the entity or the entity is required to do so under Australian law or a court/tribunal order.
APP 3	**Collection of solicited personal information**	Applies to any personal information solicited by the entity and provides that personal information should only be collected if reasonably necessary, by lawful and fair means and from the individual themselves if reasonable and practicable. An APP entity must not collect sensitive information unless consent has been obtained from the individual.
APP 4	**Dealing with unsolicited personal information**	Sets out requirements for situations where the entity did not solicit the information. Within a reasonable period of time, the entity must determine whether that information could have been collected under APP 3. If APP 3 does not apply, the entity must as soon as practicable, but only if it is lawful and reasonable to do so, destroy or deidentify the information.
APP 5	**Notification of the collection of personal information**	Provides that an entity must take reasonable steps to notify an individual at the time of, before or as soon as practicable after the collection.
APP 6	**Use or disclosure of personal information**	Stipulates that an entity must not use or disclose personal information about an individual unless the individual has consented or the use of the information falls within another exception.
APP 7	**Direct marketing**	Specifies that an entity may only use an individual's personal information for direct marketing purposes where it meets certain specific requirements.
APP 8	**Cross-border disclosure of personal information**	Sets out that entities must take reasonable steps to ensure overseas recipients do not breach the APPs in relation to that information, unless an exception applies.
APP 9	**Adoption, use of disclosure of government related identifiers**	Restricts the use of government related identifiers by the private sector.
APP 10	**Quality of personal information**	Requires entities to take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.
APP 11	**Security of personal information**	Provides that an entity must take reasonable steps to protect the personal information they possess from misuse, interference, loss, unauthorised access, modification or disclosure.
APP 12	Access to personal information	Requires entities to provide an individual with access to the information at their request.
APP 13	Correction of personal information	States that where an individual can establish that the personal information is not accurate, complete or up-to-date, the entity must take reasonable steps to correct the information.

- If your organisation is caught by the Privacy Act, the *'Australian Privacy Principles Fact Sheet'* and the *'Australian Privacy Principles Guidelines'*, available on the Australian Information Commissioner's website are essential reading.

© 2026 Arts Law Centre of Australia

Can you develop your own privacy code?

The Privacy Act allows organisations to develop their own privacy code which, when approved by the Australian Information Commissioner, replaces the obligations of the APPs for that organisation. In order for the code to be approved, the Act requires that the Australian Information Commissioner be satisfied, amongst other things, that the obligations in the code are at least equivalent to the APPs and that members of the public have been given adequate opportunity to comment on a draft of the code. It should be noted that the Australian Information Commissioner has the power to revoke the code at any time.

What happens if an individual's privacy is breached?

Where an organisation has implemented an approved privacy code, all complaints about the breach of an individual's rights under the Privacy Act should follow the code's complaints handling procedure.

In relation to an individual's privacy, the Australian Information Commissioner has power to:

- investigate complaints made to the Office of the Australian Information Commissioner by an individual or a code adjudicator;
- investigate all complaints made about a Federal Government contractor;
- investigate, on the Australian Information Commissioner's initiative, an act or practice that may be a breach of privacy, even if no complaint has been made;
- seek an injunction from the court to stop conduct that does or would breach the Privacy Act; and
- review the code adjudicator's decision if an individual requests.

Under the latest amendments, the Australian Information Commissioner has further enhanced powers to investigate an interference with an individual's privacy and can:

- seek civil penalties in the case of serious or repeated breaches of an individual's privacy;
- accept enforceable undertakings; and
- conduct an investigation and/or an audit of the performance for both agencies and businesses.

A serious or repeated breach of the Privacy Act will allow the Commissioner to make a determination and apply to the Federal Court to enforce the determination. Civil penalties may be sought from a company calculated at the greater of $50 million or three times the value of any benefit obtained through the misuse of personal information or 30% of the company's turnover and up to $2.5 million for an individual.

Complying with the *Privacy Act*

Once an organisation has established that the private sector provisions apply to it, it must consider what it needs to do to comply with these provisions. The following are some suggestions as to what an organisation should do to comply with the Privacy Act provisions:

- **Appoint a privacy officer** to be responsible for developing and implementing privacy policies. The privacy officer should be the first point of contact in the organisation when a privacy issue arises and is responsible for ensuring the organisation's privacy policy and procedures are fully implemented.
- **Check procedures for collecting personal information** and ensure that these procedures include the new notification requirements and provide a process for handling unsolicited information.
- **Conduct a privacy audit** to determine what sort of personal information the organisation collects, holds and discloses. The audit should also reveal how the organisation protects the personal information it collects, and how it is updated.

© 2026 Arts Law Centre of Australia

- **Compare current practices with requirements in the Privacy Act and keep up to date with amendments** to determine what discrepancies, if any, exist and whether updates to policies and procedures are necessary to comply with updates to the law.
- **Formulate a privacy policy for the organisation that complies with the APPs.** The privacy officer should be responsible for co-ordinating and implementing the privacy policy for the organisation. This policy needs to comply with the new minimum requirements and be made freely available to individuals, such as on your website.
- **Review third party contracts with subcontractors and service providers** especially where they involve the disclosure of any personal information to offshore providers.
- **Review your complaints policy and processes** to ensure that it enables you to deal with complaints and inquiries about your compliance with the APPs.
- **Review your marketing consents and opt out statements** to ensure they comply with the requirements of the direct marketing privacy principle and that they cover how you intend on using personal information.
- **Train staff** on privacy procedures and the organisation's privacy policies.

Your actual practice in dealing with personal information must be consistent with your published privacy policy. Promising something in a privacy policy and then failing to deliver may be misleading or deceptive conduct and breach section 18 of the Australian Consumer Law (ACL).

The Office of the Australian Information Commissioner publishes ? and government agencies.

Key development: tort for serious invasions of privacy

As of 10 June 2025, individuals will have the right to take legal action and seek remedies in court for serious invasions of their privacy, including compensation for emotional distress and injunctions to prevent further invasions of privacy, even without proof of financial loss. The claim can be made against an individual as well as an organisation.

For a claim to be successful, a person will need to show that the following key elements have been met:

- that there was an **invasion of the person's privacy** caused by an intrusion of their seclusion (for example, unauthorised surveillance or recording of private activities) or a misuse of their information (for example, unauthorised disclosure of their personal information);
- that the person had a **reasonable expectation of privacy**, which will consider factors such as the nature of the information and the context of the disclosure);
- that **the conduct was intentional or reckless** (which means that it was deliberate and not just negligent);
- that **the invasion was serious**, which will consider factors such as the nature and extent of the harm and whether it was maliciously committed;
- that it outweighs the **public interest balance** (which will question whether the person's right to privacy prevails over concepts such as freedom of expression.

It's important to note that these rights do not apply to all invasions of privacy and it's also important to note that there are valid defences available to a person defending a claim. Some factors to consider:

Was there a reasonable expectation of privacy?	Was the conduct intentional?	Was the conduct reckless?

© 2026 Arts Law Centre of Australia

Was the invasion serious?	Was the invasion an intrusion into seclusion?	Was the invasion a misuse of private information?
Did the individual provide their consent?	Was the conduct in the public interest?	Could harm have been avoided or minimised?
Was the information already public?	How was the information obtained and used?	Is there a valid defence or exclusion available?

Some limited exemptions apply:

- For journalists, where the invasion of privacy involves the collection, preparation or actual publication of journalistic material (though not in every instance and subject always to other laws regarding defamation and similar);
- Intelligence agencies;
- Law enforcement bodies;
- Individuals who are disclosing information to intelligence agencies and law enforcement bodies;
- Individuals who are under the age of 18.

As this is a developing area of law, it is difficult to predict how far the courts will weigh artistic freedom against privacy rights. Here are four scenarios where a creative's work might give rise to liability under the new tort for serious invasions of privacy:

Example 1: Documentary filmmaking and filming without consent A filmmaker who produces a documentary that includes hidden-camera footage of an individual inside their home or private space (say, through a window or from a drone) without their knowledge or consent is running the risk of committing an intrusion into that individual's seclusion and committing a serious, intentional invasion of a private setting.	**Example 2: Visual arts and exhibiting intimate or sensitive material** A visual artist who uses found photographs, messages or private diary excerpts (say, from a former partner or from a member of the public) in a mixed-media installation without anonymisation or consent is running the risk of committing a public disclosure of personal material, especially if the materials are sensitive in nature (for example, sexual, medical, familial) and the individual is identifiable.
Example 3: Disclosing personal details on a podcast or a memoirA writer or podcaster sharing stories about real people (say, friends, ex-partners, colleagues) involving health issues, traumatic events or private relationships is running the risk of misusing private information if the details and the individual are still recognisable and not in the public domain and the disclosure causes distress.	**Example 4: A music video or theatre using real surveillance or social media footage**A director who uses real CCTV or social media footage (say, of an individual being visibly upset in public) in a creative work without consent is running the risk of committing an intrusion of that individual's seclusion, depending on how private the context was and whether the individual is identifiable.

It would be prudent for creatives to exercise caution and consider seeking legal advice when using real-life subjects, incorporating personal data in their works, or drawing from social media content.

Further Information

The purpose of this Information Sheet is to provide general information about privacy and the private sector. The issues surrounding the Privacy Act can be complex and require consideration on a case-by-case basis. If more information is required on how the law applies to a particular situation, please contact the Arts Law Centre of Australia or the Office of the Australian Information Commissioner 1 300 363 992 or submit an enquiry here.

© 2026 Arts Law Centre of Australia

Justice Connect, Not-for-profit Law has published the *Privacy Compliance Manual for use by Australian charities and not-for-profits*.

© Arts Law Centre of Australia 2025

Disclaimer

The information in this information sheet is general. It does not constitute, and should be not relied on as, legal advice. The Arts Law Centre of Australia (Arts Law) recommends seeking advice from a qualified lawyer on the legal issues affecting you before acting on any legal matter.

While Arts Law tries to ensure that the content of this information sheet is accurate, adequate or complete, it does not represent or warrant its accuracy, adequacy or completeness. Arts Law is not responsible for any loss suffered as a result of or in relation to the use of this information sheet. To the extent permitted by law, Arts Law excludes any liability, including any liability for negligence, for any loss, including indirect or consequential damages arising from or in relation to the use of this information sheet.

© Arts Law Centre of Australia

You may photocopy this information sheet for a non-profit purpose, provided you copy all of it, and you do not alter it in any way. Check you have the most recent version by contacting us on (02) 9356 2566 or tollfree outside Sydney on 1800 221 457.

The Arts Law Centre of Australia has been assisted by the Commonwealth Government through the Australia Council, its arts funding and advisory body.