Australian Government

Office of the Australian Information Commissioner

Privacy guidance for reporting entities under the AML/CTF Act

Last updated April 2026

OAIC

Contents

From 1 July 2026, obligations in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) will apply to certain services — known as 'designated services' — that are typically provided by the following businesses:

- real estate professionals
- dealers in precious stones, metals and products
- professional service providers such as lawyers, conveyancers, accountants and trust and company service providers.

We refer to these as 'Tranche 2' reporting entities.

From 31 March 2026, changes to AML/CTF obligations for current reporting entities commence, which may affect how personal information is handled. We refer to these as 'Tranche 1' entities.

For information on whether you may have AML/CTF obligations, refer to AUSTRAC's guidance on AML/CTF.

The *Privacy Act 1988* (Privacy Act) applies to personal information handling activities in relation to or in connection with AML/CTF Act obligations, regardless of whether those entities fall within the definition of a small business (which is generally exempt from the Privacy Act).

Key points

- All reporting entities or authorised agents of reporting entities that are required to comply with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) are also required to comply with the *Privacy Act 1988* (the Privacy Act) when handling personal information for AML/CTF obligations. This includes those which are small businesses with an annual turnover of less than $3 million.
- The Privacy Act does not prevent reporting entities from collecting, using and disclosing personal information (including sensitive information) that is required to comply with obligations under the AML/CTF Act and the AML/CTF Rules.
- In order to meet your privacy obligations while complying with your AML/CTF Act obligations, you must limit your collection of personal information to what is reasonably necessary to comply with your AML/CTF obligations, and other functions and activities of your organisation.
- You must have a privacy policy and collection notices with clear and transparent information about how you handle personal information for your AML/CTF obligations. You do not need to provide information in a collection notice where that would be inconsistent with your tipping off obligations.
- If personal information will be disclosed overseas (including to a third party service provider) you must generally take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles (APPs). Exceptions apply, including where the disclosure is required or authorised by the AML/CTF Act or the AML/CTF Rules.
- You must take reasonable steps to keep personal information secure. Ensure you have a data breach response plan in place so you can respond quickly if there is a data breach.

- You must take reasonable steps to destroy or de-identify personal information once you do not need it for any other purpose that you are permitted to hold it for under the Privacy Act or APPs (including an AML/CTF purpose). You do not need to destroy or de-identify personal information where you are required by or authorised under an Australian law or a court/tribunal order to retain the personal information.
- The AML/CTF Act does not require you to keep scanned copies or photocopies of identity documents themselves for record keeping purposes.[1] This applies from when the new AML/CTF laws commence: 31 March 2026 for Tranche 1 reporting entities and 1 July 2026 for Tranche 2 reporting entities. You should take reasonable steps to destroy (or de-identify) copies of full identification documents you collect (such as driver's licenses or passports) once they are no longer needed.
    - Instead, keep records of personal information from the identification document directly relating to what you need to comply with your AML/CTF record keeping obligations (for example names, date of birth, residential address, date of expiry, passport/license number), the type of document, what you did to identify the customer and the outcome of the verification and analysis, identification or assessment of ML/TF risk.
    - The OAIC recognises that it may take time for entities to update their systems and processes to reflect these new requirements for ID documents. The obligation under APP 11.2 is to take steps that are reasonable in the circumstances to destroy (or de-identify) information that is no longer needed. The OAIC considers that relevant circumstances include the nature, size, resources and complexity of the entity, the type of personal information, recency and scale of new and changed AML/CTF requirements as well as the scale of the task to align an entity's destruction practices with those requirements.
    - For copies of identification documents made prior to 31 March 2026, these are records for the purposes of AML/CTF Act, and reporting entities are authorised to continue to keep these for 7 years following the end of the business relationship or 7 years after the date of the last occasional transaction.
    - There may be another AML/CTF purpose for holding copies of ID documents or other legislative obligations to retain them outside of the AML/CTF Act.

About this guidance

This guidance is intended to help reporting entities under the AML/CTF Act and authorised agents of reporting entities understand their key privacy obligations. It does not cover the entirety of the privacy obligations and should be read in conjunction with the Privacy Act, the Australian Privacy Principles guidelines (APP guidelines) and other OAIC resources referred to in this guidance. The OAIC also recommends reading this guidance alongside AUSTRAC's AML/CTF reforms guidance.

[1] See AUSTRAC's Overview of initial customer due diligence (Reform) Guidance and Section 111 of the AML/CTF Act. Prior to 31 March 2026, the AML/CTF Act authorised copies of identification documents to be made and retained.

OAIC's regulatory approach

As described in its Statement of Regulatory Approach and its Privacy regulatory action policy, the OAIC takes a risk-based and harm-focussed approach to regulation. This means the OAIC directs its regulatory efforts towards those activities that are likeliest to cause the most harm to the community.

The OAIC recognises that new requirements such as those imposed by these reforms may require significant changes and that aligning an entity's processes with the reforms may be a significant task. The OAIC considers these relevant factors to inform a proportionate use of regulatory powers.

Do reporting entities need to comply with the Privacy Act and the APPs?

Yes. All reporting entities or authorised agents of reporting entities that are required to comply with the AML/CTF Act are also required to comply with the Privacy Act when handling personal information for the purposes of, or in connection with, their AML/CTF obligations.[2] This includes those which are small businesses with an annual turnover of less than $3 million.

This means that you will have to comply with the Australian Privacy Principles (APPs). The Australian Privacy Principles quick reference page provides a summary of each principle with a link to our guidelines for it.

Small businesses that are reporting entities

While small businesses (defined in the Privacy Act as having an annual turnover of $3 million or less) are generally not covered by the Privacy Act, they have privacy obligations relating to the activities they undertake to comply with AML/CTF obligations.

Specifically, small businesses that are 'reporting entities' under the AML/CTF Act (and their authorised agents) are required to comply with the Privacy Act in relation to the activities for the purposes of, or in connection with their obligations under the AML/CTF Act and the AML/CTF Rules.[3]

Examples of 'activities' for the purposes of, or in connection with, obligations under the AML/CTF Act and AML/CTF Rules include:

- collection, use and storage of personal information for customer due diligence
- collection, use, storage and disclosure of personal information for monitoring and reporting obligations
- holding personal information for AML/CTF record keeping obligations

[2] *Privacy Act 1988* (Cth) s 6E(1A). The Privacy Act provides that if a small business operator is a reporting entity or an authorised agent of a reporting entity because of anything done in the course of a small business carried on by the small business operator, the Privacy Act applies, in relation to the activities carried on by the small business operator for the purposes of, or in connection with, activities relating to the AML/CTF Act or AML/CTF rules or regulations.

[3] *Privacy Act 1988* (Cth) s 6E(1A). Examples of other small businesses that need to comply with the Privacy Act include health service providers (including GPs, dentists and pharmacists), those trading in personal information, and operators of residential tenancy databases.

- collection, use and storage of personal information for personnel due diligence (where the employee record exemption under the Privacy Act does not apply).

Current reporting entities that are small businesses (including those in the financial services, bullion, gambling and digital currency exchange sectors) have existing obligations under the Privacy Act.

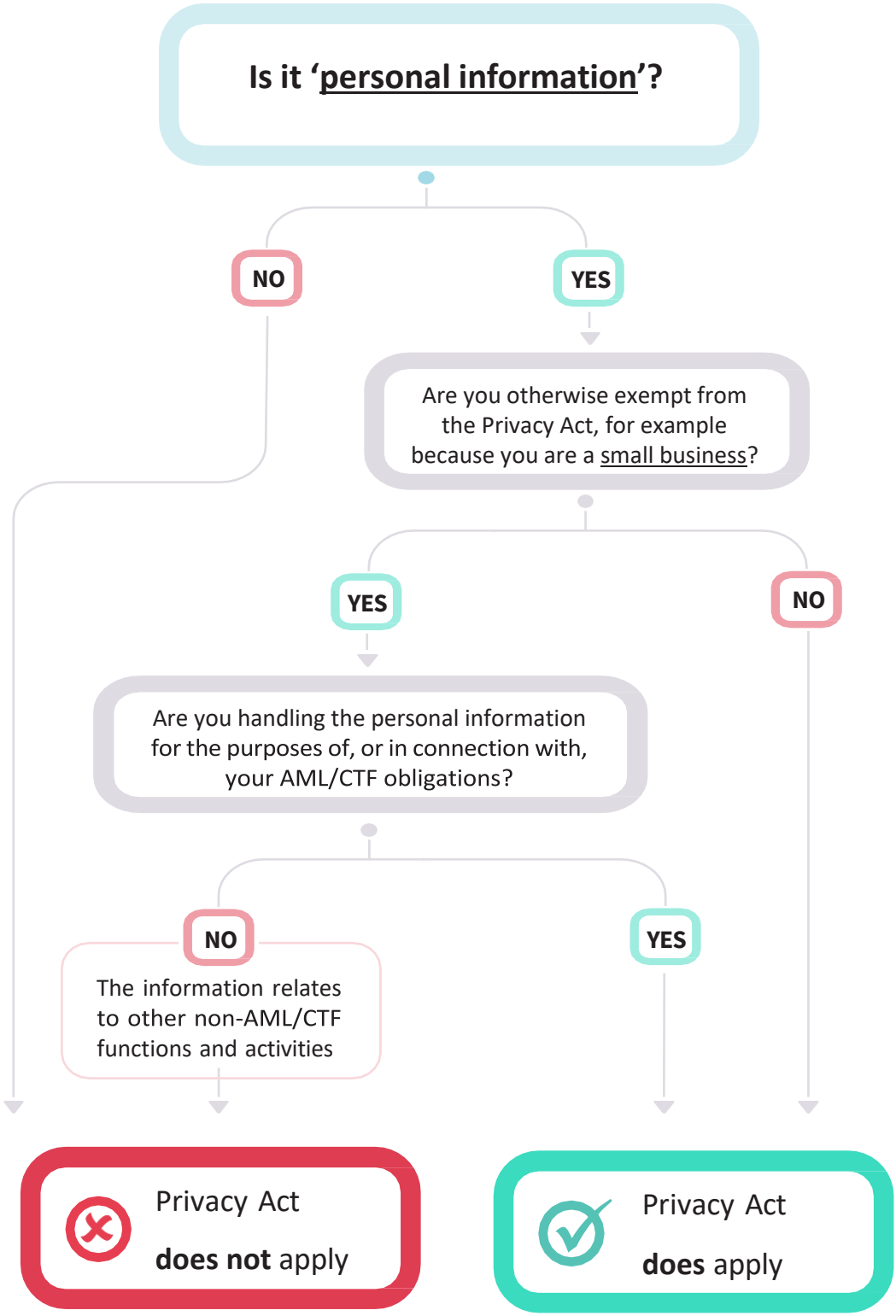
From 1 July 2026, the Privacy Act will also apply to tranche 2 entities once they become reporting entities under the AML/CTF Act.

Small businesses are not covered by the Privacy Act in relation to the non-AML/CTF business activities they undertake, unless the small business is covered by the Privacy Act for a different reason.

Where a small business has privacy obligations for another reason (for example if it is a health service provider, an operator of a residential tenancy database or trades in personal information, or needs to comply with the *Privacy (Tax File Number) Rule 2015* when handling tax file numbers), those privacy obligations apply in addition to privacy obligations that arise in the small business's capacity as a reporting entity under the AML/CTF Act. For further information on whether the Privacy Act covers your business for another reason, see our guidance on who has rights and responsibilities under the Privacy Act.

If a small business is covered by the Privacy Act because it is a reporting entity or an authorised agent of a reporting entity and AUSTRAC grants an exemption that removes or modifies certain AML/CTF obligations, the small business continues to have Privacy Act responsibilities to the extent that it continues to handle personal information for any remaining AML/CTF activities.

Flowchart on Privacy Act coverage for reporting entities under the AML/CTF Act



Case study

Real Houses Australia is a real estate agency with an annual turnover of $1.1 million (and is not an operator of a residential tenancy database), which means it is a small business under the Privacy Act. As part of the changes to AML/CTF laws which expands obligations to tranche 2 entities, it will become a reporting entity with AML/CTF obligations. Real Houses Australia must handle personal information, for example, as part of its customer due diligence and personnel due diligence obligations.[4]

Real Houses Australia must comply with the Privacy Act in relation to the personal information it handles as part of its customer due diligence and personnel due diligence obligations because this relates to Real Houses Australia's AML/CTF obligations. However, Real Houses Australia is not required to comply with the Privacy Act for other personal information-handling activities that do not relate to its AML/CTF obligations.

Where Real Houses Australia collects personal information for an AML/CTF purpose as well as a non-AML/CTF purpose (for example, where it collects customer details and transaction records to provide a real estate service as well as for their AML/CTF obligations), the Privacy Act applies to the personal information.

For information on considerations when using or disclosing personal information related to AML/CTF obligations, see section F on using and disclosing personal information collected for AML/CTF Act purposes (APP 6). You can learn more about customer due diligence and personnel due diligence obligations on the AUSTRAC website.

Privacy Tip

There may be multiple purposes for which you collect personal information. This may include compliance with the AML/CTF Act, but also purposes for other functions and activities of your organisation. Maintaining a central personal information inventory is one way that could assist you to understand how you can use the personal information, where it is stored and when you must destroy or de-identify it. For example, you could keep a list or register in a Word document, Excel spreadsheet, a separate database or a system to retrieve information about your organisation's personal information holdings.

The inventory should generally not include any personal information within it, but rather, could describe:

- the purpose/s the information was collected (including AML/CTF compliance and any other purposes)
- the legal authority under which the information was collected (including the AML/CTF Act and any other legislative instruments that may be relevant to the information)
- how and where the personal information is stored
- who is authorised to access the information

[4] *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (*AML/CTF Act)* Pt 2.

- how long the information will be retained and when the information will be de-identified or destroyed
- whether the information is sensitive information
- whether third-parties are involved.

Assessing your privacy maturity and readiness to comply

The OAIC's Privacy Foundations self-assessment tool may be a useful resource to consider if your business is coming within the operation of the Privacy Act for the first time, or a useful refresher for existing Privacy Act entities.

The tool has been designed for businesses who want to embed a culture of privacy, and establish or improve privacy practices, procedures and systems. Completing the tool should take 15-20 minutes.

Following your self-assessment, the tool will make recommendations to implement in your day-to-day operations to achieve a more robust privacy culture. The results could also be used to create a Privacy Management Plan for your business.

A club is licensed to operate 20 electronic gaming machines (EGMs) and has existing obligations under the AML/CTF Act and the Privacy Act. The club's AML/CTF Act obligations will change from 31 March 2026. The club will be required to handle different personal information for customer due diligence obligations under the AML/CTF Act, depending on the customer risk. The club considers that it will need new and changed ways of handling personal information, and uses the Privacy Foundations self-assessment tool to assess the maturity of their existing privacy practices, procedures and systems. The club identifies they will need to update their privacy policy, collection notices, complete staff training, and review existing agreements with third party providers ahead of their changing AML/CTF Act obligation.

Practical steps toward compliance

A. Implementing good governance to ensure APP compliance and having a privacy policy (APP 1)

You must have a clearly expressed and up-to-date APP privacy policy that considers how you manage personal information (APP 1.3), including how personal information is being collected, held, used and disclosed for the purposes of complying with the AML/CTF Act and AML/CTF Rules.

If you are a reporting entity or an authorised agent of a reporting entity that would otherwise be exempt from the Privacy Act (e.g. a small business), the APP privacy policy need only include information about your personal information-handling activities for the purposes of obligations under the AML/CTF Act and AML/CTF Rules. There is no requirement to include information about your business's other personal information-handling activities that are not subject to AML/CTF obligations.

For information on what must be included in an APP privacy policy, see our Guide to developing an APP privacy policy (which includes a checklist to help you consider the relevant requirements of an APP privacy policy).

You must also take reasonable steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs, and ensure that you are able to receive and respond to privacy inquiries and complaints (APP 1.2).

If an individual has a privacy complaint about how your organisation handles their personal information, they usually need to first make their complaint to your organisation.[5] You should be able to respond to privacy complaints within a reasonable timeframe (the OAIC recommends 30 days).

This means you should have processes in place to be ready to receive and respond to privacy complaints and ensure that staff are able to recognise privacy complaints. For further information and a checklist for addressing privacy complaints see our Guide to handling privacy complaints.

For further information see Chapter 1: APP 1 Open and transparent management of personal information of the APP Guidelines.

B. Collecting personal information for AML/CTF Act purposes (APP 3)

You are required to collect personal information to comply with your obligations under the AML/CTF Act and AML/CTF Rules, for example, when conducting customer due diligence or personnel due diligence. When collecting personal information about individuals, you or your authorised agent, must limit collection to what is 'reasonably necessary' (under APP 3.2) for your organisation's functions and activities, including your AML/CTF obligations. The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the collection is necessary. It is your responsibility to be able to justify that the particular collection is reasonably necessary.

APP 3 is intended to operate objectively and practically by allowing you to collect personal information that is reasonably necessary (from the point of view of a reasonable person) to pursue your legitimate functions or activities.

The benefit of limiting your collection to what is reasonably necessary is not only to comply with APP 3.2 – it also makes good business sense. Collecting and retaining personal information that you do not need may create cyber security risks, for your business, and to the people whose information you hold.

To determine whether a particular collection of personal information is permitted in the AML/CTF context, you should consider:

1. **Your functions or activities**. Identifying what functions or activities are required to comply with your AML/CTF obligations will involve understanding your obligations under the AML/CTF Act and AML/CTF Rules, and AUSTRAC's guidance. Your AML/CTF program will set out what

[5] Privacy Act s40(1A).

your business must do and when to meet its AML/CTF obligations. This will be a useful reference point to determine your specific organisation's AML/CTF functions and activities. Functions and activities include both current functions and activities and proposed functions and activities that you have decided to carry out and for which you have established plans.

2. **Whether the particular collection of personal information is reasonably necessary for those specific functions or activities**. In determining whether a collection is reasonably necessary in the AML/CTF context, relevant factors include:

    a. whether the type of personal information and amount of personal information you are seeking to collect is reasonably necessary for your functions and activities

    b. whether your organisation could undertake its functions and activities without collecting the personal information (or by collecting less information), and

    c. whether the collection is proportionate to the objective of undertaking the function or activity.

You can also collect personal information for the other functions and activities of your organisation that do not relate to AML/CTF obligations.

For more information on collection of personal information see Chapter 3: APP 3 Collection of solicited personal information and Chapter 4: APP 4 Dealing with unsolicited personal information. The term 'reasonably necessary' is also discussed further in Chapter B: Key concepts.

Privacy considerations when collecting personal information at the point of onboarding for customer due diligence

The OAIC recognises that reporting entities have an obligation under the AML/CTF Act to collect and verify certain personal information about a customer *before* a designated service is provided.

AUSTRAC provides guidance on what information you are required to collect to comply with your AML/CTF obligations and when you need to collect it, including for customer due diligence. For example, AUSTRAC's program starter kits advise that to meet the initial CDD deadline under the AML/CTF Act, you should complete the initial CDD in the window between when reasonably concluding that the engagement may involve the provision of a designated service and starting to provide the designated service.

The Privacy Act will not prevent you from collecting personal information from your customers at the point of onboarding to meet your AML/CTF obligations.

However, the AML/CTF obligations do not provide you with a 'blank cheque' to collect any personal information from all prospective clients without regard to what is reasonably necessary (see guidance on the meaning of 'reasonably necessary' above).

An organisation that decides to conduct customer due diligence on all its customers at the point of onboarding merely because this is helpful, desirable or convenient would unlikely meet the reasonably necessary test under the Privacy Act. An organisation would also be unlikely to meet the 'reasonably necessary' test under Privacy Act if it has not reasonably concluded under

the AML/CTF framework that the engagement may involve a designated service prior to collection.

Example 1

A multi-disciplinary law firm is onboarding a new client, who is seeking advice about a family law matter, and he mentioned he is considering selling his house and would like assistance with the conveyancing. While providing advice about family law is not a designated service under the AML/CTF Act, assisting with the sale of real estate is, which means that customer due diligence must be completed before the designated service is provided. Based on the nature of the engagement and the client's instructions, it appears the law firm may provide a designated service to the client as part of the engagement. The law firm makes this decision even though a buyer for the property has not yet been identified and it is unclear whether a sale of his house will materialise. In these circumstances, the law firm determines that collecting personal information at the point of onboarding is reasonably necessary to meet its AML/CTF obligations, and they collect the personal information in line with their customer due diligence procedures and AML/CTF policies.

Even if the law firm does not ultimately complete the sale of the client's house, the collection of personal information at onboarding is still permitted, as it was reasonably necessary at the time to ensure compliance with the firm's customer due diligence obligations. The firm must keep the client's customer due diligence records in accordance with its obligations under the AML/CTF Act, regardless of whether the sale of the house materialises.

Example 2

An accountant works for a firm where one section of the organisation provides designated services and another part provides services that are not regulated by the AML/CTF Act. The accounting firm is consulting with a potential client, who has requested a non-designated service. The accountant considers if it has AML/CTF obligations in the circumstance, but does not consider that a designated service will be provided. The accountant does not conduct the customer due diligence at the point of onboarding, as it is not reasonably necessary to meet the AML/CTF obligations.

Example 3

A real estate agent is brokering the sale of a property via auction. The real estate agent identifies that it must complete initial CDD on both the vendor and the buyer of the property. The real estate agent does not complete customer due diligence on all prospective buyers that inspect the property or bid at auction as this is not reasonably necessary to meet its AML/CTF obligations – it only needs to complete customer due diligence on the vendor and the individual who is the successful buyer. However, the real estate agent may still collect personal information about its prospective buyers that is reasonably necessary for its other functions and activities (such as managing the sale and gathering feedback for the seller).

Case study: adverse media searches for personnel due diligence

An organisation conducts an adverse media search on a prospective employee for an AML/CTF role to meet its personnel due diligence requirements under its AML/CTF policies. While conducting the media search, the organisation finds a media article reporting on the prospective employee's rare health condition. If the personal information is not reasonably necessary to fulfil its functions and activities (for example because the information does not relate to the person's role and ML/TF risks associated with it), the personal information cannot be collected for inclusion in a record or used by the organisation (even if it is publicly available information and regardless of whether consent is sought).

Privacy tip: Carefully consider the questions in your customer onboarding form(s). For example, you may wish to limit the free text fields to prevent customers providing you with unnecessary personal information.

C. Collecting personal information from other sources

Generally, personal information must be collected directly from the individual, unless this is unreasonable or impracticable.

In the context of the AML/CTF Act, it may be unreasonable or impracticable to collect personal information directly from the individual where the reporting entity is required or authorised to collect another individual's personal information from their customer, such as the beneficial owners of a customer's company, or about the customer's agent.[6]

You must not collect personal information directly from an individual that would or could reasonably be expected to prejudice an investigation (tipping off).[7]

D. Collecting sensitive information for AML/CTF Act purposes

Some sensitive information may be collected for the purposes of complying with the AML/CTF Act. For example, information about an individual's membership of a political association may be collected where relevant to determining whether the customer is a politically exposed person or subject to sanctions.

Sensitive information under the Privacy Act is afforded a higher level of privacy protection and must generally be collected with the individual's consent. However, you may collect sensitive information without consent if an exception in APP 3 applies, including if the collection is required or authorised by Australian law (APP 3.4(a)). This includes the AML/CTF Act or the AML/CTF Rules. The meaning of 'required or authorised' by or under law is discussed in more detail in Chapter 3 (Collection of solicited personal information) and Chapter B (Key concepts) of the APP Guidelines.

'Sensitive information' is a subset of personal information[8] and is defined as:

- information or an opinion (that is also personal information) about an individual's:

[6] *AML/CTF Act* Pt 2; *AML/CTF Rules* Pt 6.

[7] *AML/CTF Act* s 123.

[8] For more detail about sensitive information see Chapter B: Key concepts.

    - racial or ethnic origin
    - political opinions
    - membership of a political association
    - religious beliefs or affiliations
    - philosophical beliefs
    - membership of a professional or trade association
    - membership of a trade union
    - sexual orientation or practices, or
    - criminal record
- health information about an individual
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or biometric templates (s 6(1)).

Biometric information

Biometric information, including when used for verification or identification purposes, is considered sensitive information under the Privacy Act.

Any collection of biometric information must be necessary and proportionate in the circumstances. If you or your third party agent are considering collecting or using biometric information or generating biometric templates for identification or verification, you will also need to ensure:

- the individual provides consent or
- an exception applies, such as where the collection is required or authorised by Australian law (3.4(a)) or a 'permitted general situation' exists such as when it is necessary to address unlawful activity or serious misconduct.

In the OAIC's view, consent should generally be sought from the individual before conducting biometric identification or verification for customer due diligence in the AML/CTF context. In addition, the individual must be provided with sufficient information in your collection notice.

See guidance about collecting only what is 'reasonably necessary' under section 'B. Collecting personal information for AML/CTF Act purposes (APP 3)'.

E. What should customers be notified about? (APP 5)

You must be open and transparent with your customers about why their personal information is being collected and how it will be used.

APP 5.1 acknowledges it may be reasonable for an entity not to take any steps to provide a notice or ensure awareness of all or some of the above matters.

You are not required to provide a collection notice or ensure an individual's awareness where that would be inconsistent with the prohibition against disclosing information that would or could reasonably be expected to prejudice an investigation (tipping off).

Before collecting personal information for the purposes of complying with the AML/CTF Act (or if that is not practicable, as soon as practicable after collection), you must take reasonable steps to notify your customers of a range of matters, including:

- Your organisation's identity and contact details.
- The fact, circumstances and purpose of collection (for example, by explaining what personal information you need, why you are collecting it and the method of collection).
- Whether the collection is required or authorised by law or a court/ tribunal order. You should include the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection (for example, the AML/CTF Act or AML/CTF Rules). You could also include the name of the specific provisions relied upon for collection.
- The consequences if the personal information is not collected, for example, that you may not provide a service, or the customer may not be able to apply for particular products.
- The entity's usual disclosures of personal information, including third party providers and high-level information about when you may disclose personal information to AUSTRAC or another entity.
- The likelihood of any cross-border disclosure of the personal information and the countries in which such recipients are likely to be located.
- Information about access and correction processes in your APP Privacy Policy.

You can find information about matters that must be covered in a collection notice in Chapter 5: APP 5 Notification of the collection of personal information.

The OAIC has also developed a privacy collection notice template for AML/CTF reporting entities, which aims to help reporting entities develop clear and accessible collection notices explaining how personal information is handled when collecting it for customer due diligence.

F. Using and disclosing personal information for AML/CTF or other purposes (APP 6)

Generally, under APP 6, you can only use or disclose personal information for the purpose you collected it (the primary purpose). You can't use or disclose personal information for another reason (a secondary purpose) unless an exception applies or you obtain consent. An example of an exception is where the use or disclosure is required or authorised under an Australian law, which includes the AML/CTF Act or AML/CTF Rules.

For example, the primary purpose of collection in the context of customer due diligence could be to meet your obligations under the AML/CTF Act and AML/CTF Rules and carry out your AML/CTF functions and activities (which include identifying your customers and understanding the ML/TF risk associated with providing designated services). In these circumstances, personal information may be used or disclosed for these reasons as they fall within the primary purpose of collection. Any other use or disclosure will be a secondary purpose.

If you are required or authorised to use or disclose the personal information under the AML/CTF Act or AML/CTF Rules, you are permitted to use and disclose the personal information (including without

consent).[9] For example, the AML/CTF Act requires you to submit a suspicious matter report to AUSTRAC in certain circumstances, and these reports will contain personal information.[10] Practically, this means that you will be able to use or disclose the personal information whether the use or disclosure is for the primary or secondary purpose of collection.

If you are seeking to use or disclose personal information collected for AML/CTF for another function and activity undertaken by your organisation, you will need to consider whether the use or disclosure is permitted by an exception to APP 6 or whether you need to obtain consent. Common exceptions for secondary uses and disclosures include:

- where the individual would reasonably expect the secondary use or disclosure, and that is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose
- where the use or disclosure is required or authorised under an Australian law
- where a permitted general situation applies (such as for an enforcement related activity).

You must also ensure any uses or disclosures of personal information are not inconsistent with your information-handling obligations under the AML/CTF Act. For example:

- secrecy provisions within ss 121(1), 121(5), 121(6), 124, 128 and 129 of the AML/CTF Act which restrict access, use or disclosure of 'AUSTRAC information' to a limited range of purposes[11]
- the prohibition against disclosing information that would or could reasonably be expected to prejudice an investigation (tipping off)[12]
- the obligations regarding the use and disclosure of credit reporting information for identity verification.

G. Ensure overseas recipients comply with the APPs (APP 8)

If you are disclosing personal information to recipients located overseas under APP 8 and section 16C of the Privacy Act you must take such steps as are reasonable in the circumstances to ensure the recipients handle personal information in accordance with the APPs. You will generally be accountable if the overseas recipient mishandles the information. For example, if you disclose personal information to a contractor located overseas to perform services on your behalf, APP 8 and s

[9] For example, to report suspicious matters to AUSTRAC, providing information to comply with a notice issued under section 49 or 49B of the AML/CTF Act, passing on certain information about payers and payees to other institutions for the purposes of transfers of value. Depending on the context of collection of the personal information, these disclosures may also fall within the primary purpose of collection.

[10] AML/CTF Act s 41.

[11] AUSTRAC information means (s 5 of the AML/CTF Act):

- information obtained by, or generated by, an AUSTRAC entrusted person under or for the purposes of this Act
- information obtained by an AUSTRAC entrusted person under or for the purposes of any other law of the Commonwealth or a law of a State or a Territory;
- information obtained by an AUSTRAC entrusted person from a government body;
- FTR information (within the meaning of the Financial Transaction Reports Act 1988).

[12] *AML/CTF Act* s 123.

16C will apply in relation to, and you will be responsible for, the overseas contractor's handling of that information.

There are exceptions, such as where the disclosure to an overseas recipient is required or authorised by law. For example, you will not be responsible for the act or practice of the overseas recipient when disclosing personal information about payers and payees when providing value transfer services, if required or authorised by the AML/CTF Act.

In addition, section 6A(4) of the Privacy Act provides that an act or practice required by an applicable law of a foreign country will not breach the APPs if it is done, or engaged in, outside Australia and the external Territories. This means that where an overseas recipient of personal information does an act or practice that is required by an applicable foreign law, this will not breach the APPs. The APP entity will also not be responsible for the act or practice under the accountability provision.

A bank discloses personal information overseas, and the USA PATRIOT Act requires the overseas recipient to disclose personal information to the Government of the United States of America. In these circumstances, the bank would not be responsible under the accountability provision for the disclosure required by that Act.

For further information, see Chapter 8: APP 8 Cross-border disclosure of personal information of the APP Guidelines.

H. Ensuring the quality of personal information collected for AML/CTF Act purposes (APP 10)

Under the Privacy Act, you must take reasonable steps to ensure the personal information you collect is accurate, up-to-date, and complete. You must also take reasonable steps to ensure the personal information you use and disclose is — having regard to the purpose of the use or disclosure — accurate, up-to-date, complete and relevant. You can find more information about keeping accurate personal information, including examples of reasonable steps, in the APP Guidelines Chapter 10: APP 10 - Quality of Personal Information.

In addition to the steps under the Privacy Act, reporting entities may have AML/CTF Act obligations to review and update their customer's KYC information.[13] You can find more information about these obligations in AUSTRAC's guidance on ongoing customer due diligence.

I. Securing personal information you hold for AML/CTF purposes (APP 11)

You must take active measures to protect the security of the information you hold. Specifically, APP 11.1 states you must take reasonable steps to protect personal information you hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure. This includes technical and organisational measures.

Entities that collect and retain information for AML/CTF purposes often hold large amounts of sensitive data, and may hold that data for long periods of time. This 'honey pot' of valuable data may attract malicious or criminal enterprises, and may increase the risk that an entity's information

[13] *AML/CTF Act* s 30.

systems are hacked. Holding larger amounts of personal information for longer may also increase the risk of unauthorised access by staff or contractors.

Examples of steps your entity can take to mitigate the risk and impact of a cyber incident include:

- Understanding of what kind(s) of personal information your entity holds and where that information is stored. As part of this, you should also know what specific systems your entity uses, who has access to those systems and what privileges users have within those systems.
- Turn on multifactor authentication and minimum password complexity requirements, and ensure that passwords are required to be regularly changed.
- Update software and install relevant patches, which are used to correct a problem or vulnerability with a software program or a computer system.
- Implement audit logs and access monitoring for all your systems, including email accounts. Maintaining a chronological record of system activities (by both internal and external users) is often the best way for reviewing activity on a computer system to detect and promptly investigate privacy incidents.
- Ensure your contractual arrangements with your service provider impose specific obligations about the handling of personal information and mechanisms or penalties to ensure the obligations are fulfilled.
- Have a data breach response plan.

If you are a small business, your size and level of resources, and the complexity of your business model, would be relevant factors the OAIC would consider when determining if the steps you took to prevent or mitigate a cyber incident were reasonable. The OAIC's expectations for small business are not the same as those for large businesses. A scaled approach may be appropriate. However, this does not mean it would be reasonable for a small business to take no steps to avoid a data breach. You should seek out resources to assist you to prevent your business from being the victim of a cyber incident. For example, the Australian Cyber Security Centre has a small business cyber security guide that may be useful for helping to protect your business against common cyber threats.

You can find more information on security responsibilities in Chapter 11: APP 11 Security of personal information.

The OAIC has outlined the key steps to respond to data breaches in our data breach preparation and response guidance.

J. Retaining and destroying/de-identifying personal information (APP 11)

Under APP 11, you are generally required to take steps that are reasonable in the circumstances to destroy or de-identify information that is no longer needed for any purpose for which the information may be used or disclosed under the APPs. You do not need to destroy or de-identify personal information where you are required by or under an Australian law or a court/tribunal order to retain the personal information or another permitted purpose under the Privacy Act or APPs.

Under the AML/CTF Act, you are required to retain certain AML/CTF records as part of your record-keeping obligations. The Privacy Act allows you to retain these records.[14] For example, s.111 of the AML/CTF Act requires retention of information that is reasonably necessary to demonstrate compliance with customer due diligence obligations. This includes records which demonstrate the type and contents of the data collected and records of analysis, identification or assessment of ML/TF risk or decision making undertaken. Refer to AUSTRAC's guidance for more information about your record keeping obligations.

It is important that personal information is only retained as long as it is needed to comply with your AML/CTF obligations or for another permitted purpose under the Privacy Act or APPs. If there is no requirement or justification for retaining the information, entities must take reasonable steps to destroy or de-identify the personal information, as required by APP 11.2.

The 'reasonable steps' that an organisation should take to destroy or de-identify personal information will depend upon the circumstances, which include:

- the amount and sensitivity of the personal information
- the nature of the organisation (including the organisation's size, resources and its business model)
- the possible adverse consequences for an individual if their personal information is not destroyed or de-identified
- the organisation's information handling practices, such as how it collects, uses and stores personal information, including whether personal information handling practices are outsourced to third parties
- the practicability, including time and cost involved — however an organisation is not excused from destroying or de-identifying personal information by reason only that it would be inconvenient, time-consuming or impose some cost to do so.
- the recency and scale of new and changed AML/CTF requirements as well as the scale of the task to align an organisation's destruction practices with those requirements.

Destruction and retention for copies of ID documents for record keeping: reasonable steps

You must only retain the minimum information that you need. For example, if you need to keep records to demonstrate compliance with customer due diligence, you should only record personal information from identification documents relevant to your record keeping requirements (for example names, date of birth, residential address, date of expiry, passport/license number), the type of document, what you did to identify a customer, the outcome of your verification and analysis, identification or assessment of ML/TF risk.

You should take reasonable steps in the circumstances to destroy (or de-identify) copies of full identification documents (such as driver's licenses or passports) after you no longer need them for your AML/CTF obligations or for another purpose under the Privacy Act or the APPs.

From 31 March 2026, the AML/CTF Act does not require you to keep scanned copies or photocopies of identity documents themselves for record keeping purposes. Prior to 31 March 2026, the

[14] *AML/CTF Act* Pt 10.

AML/CTF Act authorised copies of identification documents to be made. Copies of identification documents made prior to 31 March 2026 are records for the purposes of AML/CTF Act that must be kept for 7 years following the end of the business relationship or 7 years after the date of the last occasional transaction.

The OAIC acknowledges that some Tranche 1 reporting entities and their agents have longstanding practices, procedures and systems to retain copies of ID documents for AML/CTF record keeping. The OAIC also acknowledges that under the AML/CTF transitional rules, some Tranche 1 entities will be using the Applicable Customer Identification Procedures (ACIP) instead of the new initial CDD framework while they update their systems, processes and AML/CTF programs.

While entities are transitioning to compliance with the new record keeping requirements, the OAIC expects entities to take reasonable steps to destroy (or de-identify) copies of ID documents, including to:

- Commit to destroy or de-identify copies of ID documents as soon as this practically becomes possible, in a manner and reasonable timeframe appropriate to the nature, size and complexity of the business.
- Have a documented plan to be actively working towards implementing technical and organisation measures to ensure copies of full ID documents are not retained for longer than they are needed.
    - The plan should include the reasons why the copies of full ID documents cannot be destroyed (or de-identified) immediately from 31 March 2026, the reasonable steps being taken in the circumstances to destroy (or de-identify documents) and the period of time by which the organisation will destroy (or de-identify) information in compliance with APP 11.2.
    - Senior management should have oversight of the organisation's progress against the plan to ensure accountability on the route to achieving compliance.
- Consider the privacy risks to individuals, and seek to mitigate these risks. For example, the reporting entities could consider putting the copy of the ID document 'beyond use' to reduce the likelihood of a data breach until it becomes possible to destroy (or de-identify) the document – see information below about the meaning of 'beyond use'.

Copies of ID documents which were made prior to 31 March 2026 may continue to be retained in accordance with the AML/CTF obligations (7 years following the end of the business relationship or 7 years after the date of the last occasional transaction). Once the relevant AML/CTF obligation is discharged, the entity should take reasonable steps to destroy or de-identify those documents.

Example

A financial advisor's AML/CTF program required them, until 31 March 2026, to collect and retain certified copies of identification documents they used to meet their AML/CTF obligations.
The financial advisor can continue to retain these certified copies for the timeframe required under the AML/CTF laws that applied before 31 March 2026. They do not need to destroy or de-identify these copies to meet their APP 11 obligations.

For identification documents collected from 31 March 2026, they change their AML/CTF program and take reasonable steps to only keep records of personal information from the identification document and the date it was cited, and do not retain a copy of the identification document itself.

Reasonable steps that you could consider putting into place to ensure compliance with your retention and destruction obligations include:

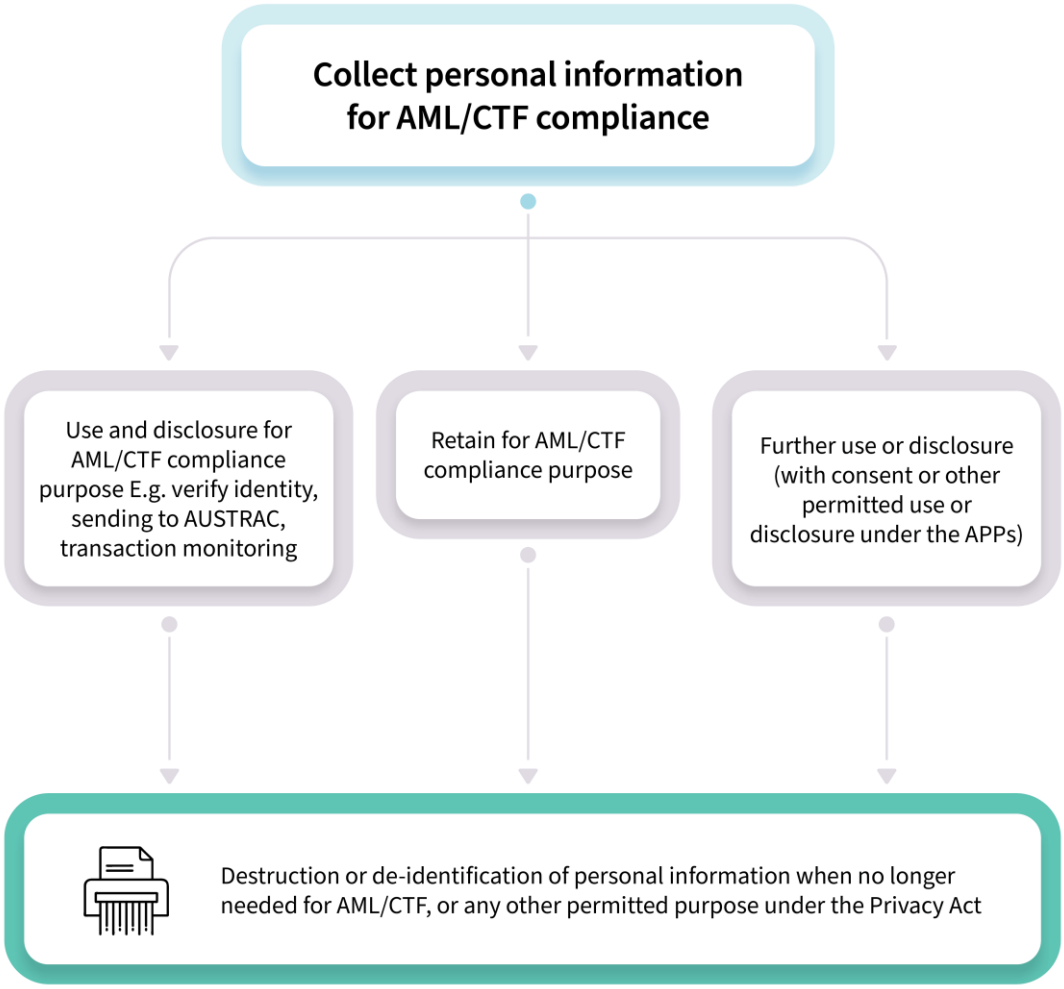
- having systems and processes in place to specify retention periods and identify if retention is still necessary under AML/CTF obligations (such as an alert system or destruction schedule to notify staff when the personal information must be destroyed or de-identified)
- ensuring that processes for the retention and destruction of personal information are well known to all staff, and conducting regular training and monitoring to ensure compliance
- keeping detailed records of your arrangements with third party providers to ensure you know what personal information the party holds on your behalf and the associated retention periods.

Where it is not possible to irretrievably destroy personal information, an organisation could instead take reasonable steps to de-identify the personal information or put the information 'beyond use'. It is expected that only in very limited circumstances would it not be possible for an organisation to destroy personal information held. For example, where technical reasons may make it impossible to destroy personal information in the short term. Personal information is 'beyond use' if the organisation:

- is not able, and will not attempt, to use or disclose the personal information
- cannot give any other entity access to the personal information
- surrounds the personal information with appropriate technical, physical and organisational security, and
- commits to take reasonable steps to irretrievably destroy the personal information if, or when, this becomes possible.

For more information on the retention, destruction or de-identification of personal information see Chapter 11: APP 11 Security of personal information and the Guide to Securing Personal Information.

Flowchart on personal information handling for reporting entities



K. Have a data breach response plan

A data breach occurs when personal information is lost or subjected to unauthorised access or disclosure. For example, when a database with personal information is hacked or personal information is mistakenly given to the wrong person.

Data breaches can cause significant harm in multiple ways, and might include identity theft, financial loss, or physical harm. Individuals whose personal information is involved in a data breach, such as your clients, may be at risk of serious harm, whether that is harm to their physical or mental wellbeing, financial loss or damage to their reputation given the nature of personal information relating to AML/CTF obligations. Data breaches may also increase the ML/TF risks your business faces, as criminals may misuse information drawn from data breaches to exploit your business and avoid detection.

Ensuring your organisation has a data breach response plan in place, and that you are familiar with it, will enable you to respond quickly to a data breach. By responding quickly, you can minimise the risk of harm and substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result.

The Notifiable Data Breaches (NDB) scheme applies to all entities with personal information security obligations under the Privacy Act. The NDB scheme requires entities to notify affected individuals and the OAIC when a data breach has occurred that is likely to result in serious harm.

There are some exceptions to the notification requirement. For example, the requirement to notify individuals and the OAIC about a data breach does not apply where that notification would be inconsistent with a secrecy provision (s 26 WP of the Privacy Act). If an eligible data breach occurs, and it is inconsistent with a secrecy provision in the AML/CTF Act, entities should apply the notification requirements in the Privacy Act only to the extent necessary to avoid inconsistency with a secrecy provision. Examples of secrecy provisions in the AML/CTF context include the provisions within ss 121(1), 121(5), 121(6), 124, 128 and 129 of the AML/CTF Act which restrict access, use or disclosure of 'AUSTRAC information' to a limited range of purposes[15] and the prohibition against disclosing information that would or could reasonably be expected to prejudice an investigation (tipping off).[16]

For example, if providing a statement to the OAIC would not be inconsistent with a secrecy provision, but notifying the individual would be, the entity would only be required to notify the OAIC.

If you do not have a data breach response plan, our Data breach preparation and response guide will help you in preparing for and responding to a data breach.

L. Providing access to personal information (APP 12)

Under the Privacy Act, if you hold personal information about an individual, you must generally provide that individual with access to their information on request, unless there are grounds for refusal (APP 12). You must respond to the request for access to the personal information within a reasonable time (usually 30 days).

You must not provide information to an individual under an access request that is inconsistent with your information-handling obligations under the AML/CTF Act. For example, you must not provide access to personal information or explain why you are denying access if it would breach the tipping off offence in section 123 of the AML/CTF Act. Refer to AUSTRAC's guidance for information on tipping off obligations.

When dealing with requests for access to personal information under APP 12, you must verify the individual's identity to ensure the access request has been made by the individual concerned, or by another person who is authorised to make the request on their behalf (such as a legal representative). The information you have collected and verified about the customer for the purposes of complying with your customer due diligence obligations may help you do this, as the individual's identity will already be known to you. For example, if a regular client requests access during an appointment, it is unnecessary to verify identity further.

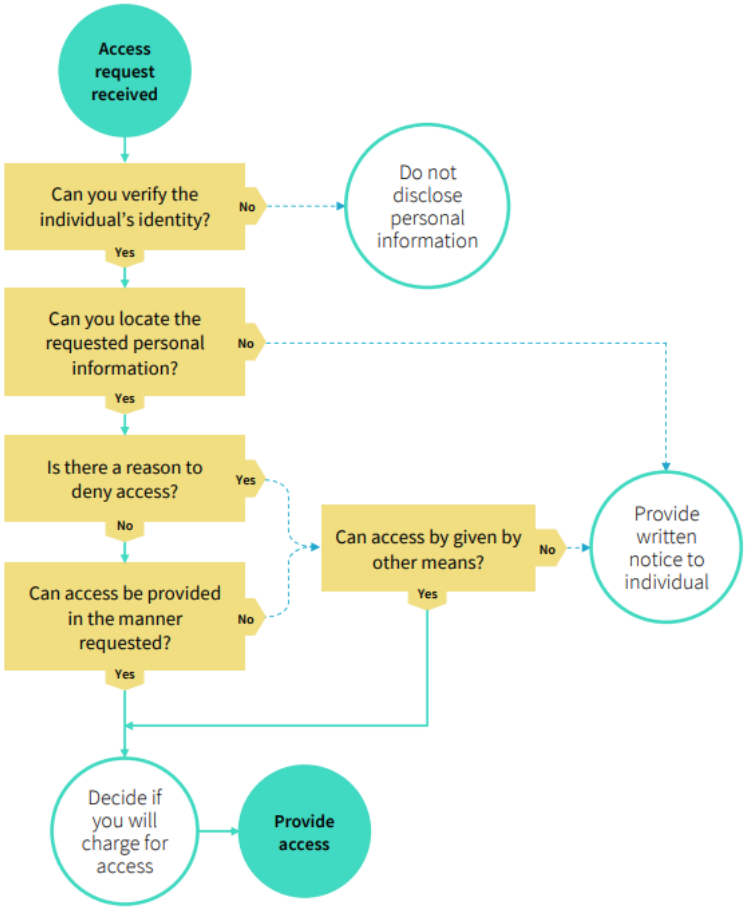
---

[15] AUSTRAC information means (s 5 of the AML/CTF Act):

- information obtained by, or generated by, an AUSTRAC entrusted person under or for the purposes of this Act
- information obtained by an AUSTRAC entrusted person under or for the purposes of any other law of the Commonwealth or a law of a State or a Territory;
- information obtained by an AUSTRAC entrusted person from a government body;
- FTR information (within the meaning of the Financial Transaction Reports Act 1988).

[16] *AML/CTF Act* s 123.

The flow chart below sets out the key steps to help you respond to a request for access to personal information.



APP 12.3 outlines the grounds on which you may refuse to give access when an individual requests access to their personal information. The most common grounds for refusing access in the AML/CTF context include (but are not limited to):

- where giving access would be unlawful, for example, where it may constitute tipping off under the AML/CTF Act
- there is reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the organisation's functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body
- denying access is required or authorised by or under an Australian law.

If you refuse to give access, or refuse to give access in a manner requested, you must give the individual a written notice setting out:

- the reasons why you have refused access, or refused to give access in the manner requested, except to the extent it would be unreasonable to do so, such as where it would be inconsistent with your tipping off obligations
- how the individual may make a complaint about your decision, how you will deal with the complaint and any information about external complaint avenues (such as the OAIC).

If you are refusing to give access to personal information because it is inconsistent with your legal obligations (for example tipping off), your written notice must not explain why you have refused access.

The OAIC's guide on dealing with requests for access to personal information provides information about each step in the access process, including verification and locating the requested personal information from records. You can also find more information about access requests in Chapter 12: APP 12 Access to personal information.

M. Correcting clients' Know Your Customer information (APP 13)

A reporting entity or an authorised agent of a reporting entity should provide a means to rectify incorrect personal information and take reasonable steps to correct personal information it holds. You can find more information about the right to correct information in Chapter 13: APP 13 – Correction of Personal Information.

APP 13 complements and does not replace other correction obligations under the AML/CTF Act. For example, under the AML/CTF Act, as part of customer due diligence reporting entities have obligations to review and update KYC information, which includes the personal information collected as part of customer due diligence.[17]

If reasonable steps are taken to correct personal information under APP 13, an entity can better ensure it complies with the AML/CTF requirements to review and update KYC information. Similarly, when an entity reviews and updates KYC information, and the entity makes this correction, this reduces the likelihood that personal information will need correction under APP 13.

You can find more information about these obligations in AUSTRAC's guidance on ongoing customer due diligence.

N. Considerations when engaging a third party provider

You may choose to engage a contractor to handle your clients' personal information. For example, you could engage a contractor to help you carry out customer due diligence, or for your customer management systems. See AUSTRAC's guidance on using outsourcing to help meet your AML/CTF obligations.

Before entering into arrangements with a third party, make sure the arrangements (such as a contract) cover how personal information will be handled and the third party is aware of the Privacy Act obligations. This is particularly important if the third party is located offshore as you may be held

[17] *AML/CTF Act* s 30.

liable for the acts of those third parties (see the information above about sending information overseas).

Before entering into a contract with a third party, review the terms of the agreement to understand how personal information is collected, handled and stored, and make sure you are satisfied the third party has appropriate processes in place to protect personal information and comply with any obligations it has under the Privacy Act. You could consider:

- requesting relevant documentation, such as the third party's privacy policy, information security policy and data breach response plan
- conduct due diligence, for example by carrying out a quick search for any past security incidents associated with the product or service
- including contractual arrangements with your service providers to include terms to deal with specific obligations about the handling of personal information and mechanisms to ensure the obligations are being fulfilled
- conducting periodic reviews of the personal information handling requirements of the arrangements
- keep detailed records of your arrangements with the third party to maintain an audit trail and ensure you know what personal information the party holds on your behalf
- at the end of the contract, ask the third party to confirm that they have deleted any personal information in accordance with the contract terms.

Privacy act coverage for authorised agents of reporting entities

In addition to reporting entities, all authorised agents of reporting entities are required to comply with the Privacy Act when handling personal information for the purposes of, or in connection with, AML/CTF obligations. This includes those which are small businesses with an annual turnover of less than $3 million.

An agent of a reporting entity is a person authorised on behalf of the reporting entity in carrying out applicable customer identification procedures or identification verification procedures on the reporting entity's behalf. [18]

Where a reporting entity provides a designated service to a customer through an agent, both the reporting entity and the authorised agent have responsibilities under the Privacy Act.

[18] The Privacy Act s 6(1) defines an authorised agent as a person authorised to act on behalf of the reporting entity as mentioned in section 37 of the AML/CTF Act regarding applicable customer identification procedures that may be carried out by an agent of a reporting entity.

O. Identity verification using the credit system

The AML/CTF Act authorises the use and disclosure of certain personal information held by a credit reporting body (CRB) to a reporting entity for the purpose of verifying an individual's identity under the AML/CTF Act.[19]

The AML/CTF Act enables a CRB to prepare an assessment, upon the request of a reporting entity, of whether certain personal information provided to it by that reporting entity matches certain types of personal information held by the CRB. The matching process is limited to the individual's name, residential address and date of birth. A CRB will not be permitted to consider any other consumer credit-related personal information it holds.

Importantly, a CRB may only provide an overall assessment of the extent of the match between the personal information provided by the reporting entity and the personal information held by the CRB. The CRB is not permitted to provide separate assessments of the match between the particular categories of personal information provided by the reporting entity.

You must not make a verification request unless you have first:

- given the individual, whose identity is being verified, information about the proposed verification process, including the reasons for making the request and the personal information about the individual that may be disclosed to the CRB
- obtained the individual's express consent, and
- made available an alternative means of identity verification.

Australian Governments Digital ID System

The Australian Government Digital ID System provides a secure, convenient and voluntary way to verify who individuals are online.

The Digital ID System is being phased and currently allows individuals to use their digital ID to access government services. By December 2026, the Australian Government Digital ID System will expand to allow applications from the private sector to become accredited Digital ID providers. The OAIC will update this guidance in the future to provide expanded guidance about the Digital ID system for AML/CTF reporting entities. For more information see **Digital ID** and Australian Government's official **Digital ID system website**.

Relevant resources

- Privacy Essentials Checklist for AML/CTF reporting entities
- Privacy collection notice template for AML/CTF reporting entities
- Privacy Foundations self-assessment tool

[19] *AML/CTF Act* Div 5A, Pt 2.

- Australian Privacy Principles quick reference
- Australian Privacy Principles guidelines
- Guide to developing an APP privacy policy
- Guide to handling privacy complaints
- Data breach preparation and response guide
- Guide to undertaking privacy impact assessments
- Dealing with requests for access to personal information
- AUSTRAC AML/CTF guidance
- AUSTRAC Program starter kits
- Australian Signals Directorate's Small business cyber security guide
- Australian Signals Directorate's Strategies to mitigate cyber security incidents
- OAIC statement of regulatory approach
- OAIC regulatory priorities

Privacy Essentials Checklist for AML/CTF reporting entities

This checklist is intended to help 'reporting entities' under the AML/CTF Act and authorised agents of reporting entities prepare for key privacy obligations. Changes to AML/CTF obligations for current reporting entities come into effect on **31 March 2026**. AML/CTF obligations commence for tranche 2 entities on **1 July 2026.** The checklist does not cover the entirety of privacy obligations and should be read in conjunction with the OAIC's Privacy guidance for reporting entities under the AML/CTF Act, as well as the Privacy Act, the Australian Privacy Principles guidelines (APP guidelines) and other OAIC resources referred to in this checklist.

☐	**Does your organisation have someone responsible for overall privacy management?**	
	• Guidance	• Resources
	An appropriately resourced role or team should be given accountability for privacy matters in the business.	Chapter 1: APP 1 Open and transparent management of personal information
☐	**Does your organisation have a privacy policy?**	
	• Guidance	• Resources
	Have a privacy policy that describes in plain English what personal information you collect, how you collect that information, and how and why you use that information. See Section A. Implementing good governance to ensure APP compliance and having a privacy policy (APP 1) for more information.	Chapter 1: APP 1 Open and transparent management of personal information. Guide to developing an APP privacy policy What is personal information?
☐	**Does your organisation have a process for recording and considering privacy risks and issues?**	
	• Guidance	• Resources
	Have an established process for reporting privacy risks to the person or team responsible for privacy management. For example, establish a privacy risk register where management is responsible for signing off on privacy risks, include privacy issues as a	Guide to undertaking privacy impact assessments

	standing agenda item in team meetings, and undertake a privacy impact assessment of business systems and processes relating to AML/CTF obligations.	
☐	**Does your organisation have a process for assessing a third party for privacy risk when procuring their solution or service?**	
	• Guidance	• Resources
	Before entering into a contract with a third party, review the terms of the agreement to understand how personal information is collected, handled and stored, and make sure you are satisfied the third party has appropriate processes in place to protect personal information and comply with any obligations it has under the Privacy Act. See Section N. Considerations when engaging a third party provider for more information.	Guide to securing personal information
☐	**Does your organisation take reasonable steps to notify your customers why their personal information is being collected and how it will be used?**	
	• Guidance	• Resources
	Make sure individuals are clearly informed of why their personal information is being collected and how it will be used. However, you should not notify the individual if it would be inconsistent with your AML/CTF tipping off obligations. See Section E. What should customers be notified about? (APP 5) for more information.	Chapter 5: APP 5 Notification of the collection of personal information. Tipping off | AUSTRAC Privacy collection notice template for AML/CTF reporting entities
☐	**Does your organisation only collect the minimum amount of personal information you need to carry out your AML/CTF obligations or your other functions and activities?**	
	• Guidance	• Resources

	You must limit your collection to what is 'reasonably necessary' (under APP 3.2). See Section B. Collecting personal information for AML/CTF Act purposes (APP 3) for more information.	Chapter 3: APP 3 Collection of solicited personal information
☐	**Does your organisation only use and disclose personal information for the purpose you collected it, or where an exception applies?**	
	• Guidance	• Resources
	Generally, under APP 6, you should only use or disclose personal information for the purpose you collected it (the primary purpose). You can't use or disclose personal information for another reason (a secondary purpose) unless an exception applies or you obtain consent. If you are required or authorised to use or disclose the personal information under the AML/CTF Act or AML/CTF Rules, you are permitted to use and disclose it (including without consent). See Section F. Using and disclosing personal information collected for AML/CTF Act purposes (APP 6) for more information.	Chapter 6: APP 6 Use or disclosure of personal information | OAIC
☐	**Does your organisation have an inventory of your personal information holdings?**	
	• Guidance	• Resources
	Have a personal information inventory if it helps you to understand and manage your privacy risks, including keeping track of personal information with multiple purposes. Having an inventory of personal information holdings is best practice under the Privacy Act.	What is personal information? Rights and responsibilities

☐	**Does your organisation have cyber security processes and controls in place to secure personal information you hold for AML/CTF purposes?**	
	• Guidance	• Resources
	You must take reasonable steps to protect personal information you hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure. This includes technical and organisational measures. Implement cyber security controls on systems that store personal information. Controls could include role-based access controls and multi-factor authentication. See Section I. Securing personal information you hold for AML/CTF purposes (APP 11) for more information.	Chapter 11: APP 11 Security of personal information Small business cyber security guide | Cyber.gov.au
☐	**Does your organisation have a process to identify and manage a data breach?**	
	• Guidance	• Resources
	Assign roles and responsibilities to legal advisers/leadership in responding to a data breach. Include staff, like IT, whose support is necessary not only to prevent a breach, but to identify affected individuals. Document the process. Organisations are responsible for the actions of third party providers when outsourcing their personal information handling. Organisations that implement strong supplier risk management frameworks, together with more robust security measures, can substantially minimise the impact of a data breach in the supply chain. See Section K. Have a data breach response plan for more information.	Data breach preparation and response guide

☐	**Does your organisation have processes in place to ensure that personal information is de-identified or destroyed once it is no longer needed, including for any AML/CTF purposes?**	
	• Guidance	• Resources
	Give a role or team responsibility for regularly destroying personal information your business no longer needs. Instate a register or schedule which tracks when to destroy or de-identify personal information. Enforce data destruction periods. Ensure staff are adequately trained and aware of the need for de-identification or destruction. Audit de-identified data to ensure it remains de-identified. See Section J. Retaining and deleting personal information (APP 11) for more information.	Chapter 11: APP 11 Security of personal information Guide to securing personal information
☐	**Does your organisation have processes for receiving and responding to privacy enquiries, complaints or requests from an individual that relates to their personal information? This should also include access and correction requests.**	
	• Guidance	• Resources
	Organisations should have one or more staff responsible for managing privacy, including a key privacy officer. These staff should be responsible for handling internal and external privacy enquiries, complaints, and access and correction requests in a timely manner. Small-sized service providers may have one person occupying this role at the same time as other operational roles. For more information see:	Chapter 10: APP 10 Quality of personal information Chapter 12: APP 12 Access to personal information. Chapter 13: APP 13 – Correction of Personal Information Dealing with requests for access to personal information

	Section H. Ensuring the quality of personal information collected for AML/CTF Act purposes (APP 10) Section L. Providing access to personal information (APP 12) Section M. Correcting clients' Know Your Customer information (APP 13).	Dealing with requests for correction of personal information Handling privacy complaints
☐	**Does your organisation monitor and address new security risks and threats that may be relevant to the personal information you hold in relation to your AML/CTF obligations?**	
	• Guidance	• Resources
	Stay informed of issues and developments in privacy law and changing legal obligations by subscribing to the OAIC's newsletter for updates. Organisations should monitor and address new security risks and threats. Sign up for alerts from ASD's ACSC and follow the steps it suggests for ensuring online security, including implementing software updates and patches.	Information Matters newsletter Alerts and advisories | Cyber.gov.au
☐	**Does your organisation provide privacy training to your staff on how to appropriately handle and protect personal information in relation to or in connection with their AML/CTF Act obligations?**	
	• Guidance	• Resources
	Staff need to understand the business' privacy obligations and their role in handling personal information in relation to or in connection with their AML/CTF Act obligations correctly. Train staff on privacy and cybersecurity fundamentals. Monitor and enforce training completion.	Research and training resources