Queensland Law Society

Privacy Compendium

SME Firm

Table of Contents

PART A

INTRODUCTION AND REGULATORY FRAMEWORK

Chapter 1: Purpose and Scope of This Manual

1.1. Introduction

This Privacy Compendium has been prepared to assist small law firms in Queensland to understand and implement their privacy obligations under the *Privacy Act 1988* (Cth). It is always preferable to consult a specialist Privacy consultant as part of a compliance project, but if that is not possible this compendium is intended as a starting point.

The compendium – as the name suggests – is not intended to be a definitive resource. It is a summary of material prepared by third parties, in particular the Office of the Australian Information Commissioner. For more information and confirmation always read the full context in the resource referenced.

For many law firms new Privacy obligations arise for the first time as a consequence of the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Tranche 2 reforms that commence on 1 July 2026.[1] These obligations are in addition to a solicitor's general duty of client confidentiality.

Any firm (irrespective of turnover) that provides *'designated services'*[2] becomes an AML reporting entity and therefore will have Privacy Act obligations relating to at least some of its data.[3]

Firms with an annual turnover of more than $3 Million are already Privacy Act regulated and have obligations with respect to all Personal Information held.

This resource is largely a compendium, providing a brief overview of material published by regulators and others. There are extensive links to the underlying publications. The underlying regulatory publication should always be treated as the source of truth in the case of ambiguity or inconsistency.

Importantly: the resources and templates that accompany this resource presume that the firm's turnover is less than $3 Million, and as such it is only AML-CTF related data holdings that are regulated.

---

[1]Office of the Australian Information Commissioner Privacy guidance for AML reporting entities
[2]Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024 (Cth), which received Royal Assent on 10 December 2024.
[3]Privacy Act 1988 (Cth), s 6C(1), definition "Organisation" usually excludes an entity with turnover less than $3Million. Exceptions apply, one of which is if the entity is a 'reporting entity' for AML/CTF purposes.

1.2. How to Use This Manual

While a cover-to-cover read will provide the best context, chapters are designed to contain enough stand-alone information to address specific issues. Other resources, such as the Privacy Program Starter Guide may be a more user-friendly overview of what is required. This compendium is intended to provide supplemental information if needed.

Who?	Objective	Most relevant chapters and toolkit documents
Principal	Understand what is changing and overview what will be needed.	Part A (Chapters 1–3), Chapters 4, 5 and 8.
a	Compliance program for a very small firm (undertaking all work yourself).	Start with the Privacy Program Starter Guide. Refer back to this compendium as required.
b	Compliance program for small firm (delegating or getting assistance).	N/a – use the Privacy Program Starter Guide instead.
c	Ongoing supervision: ensuring programs are operating correctly (as time permits).	Part E: Operationalising Privacy.
Privacy Officer	Setting up a new privacy compliance program for an enterprise up to $3M.	**Essential:** Chapter 1 (introduction); Chapter 2 (2026 changes); Chapter 6 (getting ready); Chapter 8 (APPs most relevant to law firms); Chapters 10–12 (using the toolkit); Chapter 13 (implementation roadmap). **Secondary:** Chapter 3 (the regulations); Chapters 4–5; Chapter 7 (more about the APPs); Chapter 9 (privacy Y AML); Chapter 14 (security measures). **Toolkit (use in detail):** all seven — begin with Doc 03 (Personal Information Inventory) to scope holdings, then Docs 01, 02, 04, 05, 06 and 07.
Privacy Officer	Managing an existing program (ongoing operation and maintenance).	**Essential:** Chapter 12 (record keeping); Chapter 15 (breach response); Chapter 16 (access and correction requests); Chapter 17 (staff training); Chapter 18 (privacy complaints). **Secondary:** Chapter 2 and 1.6 (currency and legislative change); Chapter 10; Chapter 14 (security measures — ongoing review). **Toolkit (use in detail):** Doc 03 (Inventory) and Doc 04 (Retention Schedule) — maintain; Doc 05 (Breach Response Plan); Doc 07

Who?	Objective	Most relevant chapters and toolkit documents
		(Training Framework). Review Docs 01 and 02 periodically.
Practice Manager	Implementing the training program; handling access requests; responding to data incidents.	Chapter 1 (orientation; how to use the manual); Chapter 14 (security measures); Chapter 15 (breach response); Chapter 16 (access and correction requests); Chapter 17 (staff training). **Toolkit (use in detail):** Doc 05 (Breach Response Plan) and Doc 07 (Training Framework). Reference Doc 03 (Inventory).
AML/CTF Compliance Officer	Ensuring appropriate record keeping, that necessary information is collected, and that collection and disclosure are properly notified.	**Essential:** Chapter 2 (AML/CTF and Privacy Act interaction; scope); Chapter 9 (integrating privacy and AML/CTF — the core chapter for this role); Chapter 11 (collection notices — when are we collecting AML information?); Chapter 12. **Secondary:** Chapter 8 (APPs 3, 5, 6 and 11 — collection, notification, use/disclosure, security); Chapter 15 (breach response for AML/CTF data incidents). **Toolkit (use in detail):** Doc 02 (Collection Notice), Doc 03 (Inventory) and Doc 04 (Retention Schedule). Reference Doc 05 (Breach Response Plan).

This assumes the following breakdown of responsibilities:

Firm Principals, and Legal Practitioner Directors who bear ultimate responsibility for the firm's compliance with legal obligations, including privacy obligations.

Privacy Officers are responsible for the day-to-day management of privacy policies. This manual and the accompanying toolkit provide the Privacy Officer with the resources needed to implement and maintain the firm's privacy management framework. This manual is only intended as a summary so reliance on primary OAIC guidance will be necessary.[4]

Practice Managers and Support Staff may be called upon to assist with implementing privacy procedures, delivering training, or handling access and correction requests.

AML/CTF Compliance Officers appointed under the AML/CTF regime should understand the interaction between AML/CTF and privacy obligations, particularly as explained in Chapter 9 of this manual. Privacy and AML/CTF compliance are closely connected, and in many small firms the same person may hold both roles.

IT Staff and Information security officers must understand what security promises have been made in the Privacy Act materials.

1.3. How This Manual is Organised

This manual is organised into seven parts, each addressing a distinct aspect:

[4]Links to OAIC guidance may be found in each relevant chapter and is also collated in Chapter 19.

Background

Part A: Introduction and Regulatory Framework (Chapters 1-3) overview, regulatory changes from 1 July 2026, the interaction between the Privacy Act, Australian Privacy Principles ("APPs"), and the AML/CTF regime.

Part B: From Confidentiality to Privacy Compliance (Chapters 4-6) the distinction between confidentiality obligations solicitors have always observed and the new statutory privacy obligations.

Part C: The Australian Privacy Principles Explained (Chapters 7-9) provide a brief overview of each of the 13 APPs, with particular focus on those most relevant to law firm practice and their interaction with AML/CTF obligations.

Getting compliance ready

Part D: Using the Compliance Toolkit (Chapters 10-12) provides document-by-document guidance on implementing the seven toolkit templates that accompany this manual.

Part E: Implementation Roadmap (Chapters 13-15) sets out a phased implementation plan, staff training requirements, and ongoing monitoring.

Running a privacy program once it is established

Part F: Handling Privacy Events (Chapters 16-18) provides operational guidance on handling access and correction requests, responding to data breaches, and managing privacy complaints.

Part G: Resources and References (Chapters 19-21) consolidates OAIC guidance, provides a glossary of key terms, and includes quick reference checklists for common compliance activities.

1.4. The Compliance Toolkit — Documents at a glance

This manual is accompanied by seven basic compliance documents, collectively referred to as the 'Compliance Toolkit'.

These documents have been designed to implement the **core** requirements of the OAIC's Privacy Management Framework[5] and to satisfy the obligation under APP 1.2 to take reasonable steps to implement practices compliant with the APPs.[6] Using these basic templates will not necessarily implement best practice.

The toolkit documents are:

Doc	Document Title	Primary Purpose
01	Privacy Policy Template	APP 1 compliant privacy policy for publication on the firm's website, integrating AML/CTF-specific collection and retention requirements
02	Collection Notice Template	A generic collection notice has been published by the OAIC intended for parties collecting AML related information. A version adapted for law firm context is supplied.
03	Personal Information Inventory	Register template for documenting categories of personal information held by the firm. Filling this out is an important first step in determining what regulated information you might hold.

[5]OAIC, *Privacy management framework: enabling compliance and encouraging good practice* (May 2025), available at <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/privacy-management-framework-enabling-compliance-and-encouraging-good-practice>.
[6]Australian Privacy Principle 1.2,

04	Data Retention Schedule	Your firm's plan for document retention, having regard to requirements of the Privacy Act, Legal Profession Act 2007 (Qld), QLS Document Retention Guidance.
05	Data Breach Response Plan	Four-step procedure for responding to data breaches under the Notifiable Data Breaches scheme, with assessment form and emergency contacts
06	Privacy Impact Assessment	Two-part PIA framework: threshold assessment tool plus comprehensive PIA template.
07	Staff Training Framework	Multi-module training program with requirements matrix and training record template

Each toolkit document contains bracketed placeholders (such as [Firm Name] or [Privacy Officer contact details]) that must be replaced with firm-specific information before the document is used. Detailed guidance on customising each document is provided chapters dedicated to each primary document.

The toolkit documents have been designed to work together as an integrated system, but each should only be regarded as a starting point. Modification in addition to adding firm details will be required, especially for the Privacy Policy.

1.5. OAIC Guidance Informing This Manual

This manual draws on guidance published by the Office of the *Australian Information Commissioner* (OAIC), which is the regulator responsible for the Privacy Act. The principal OAIC publications informing this manual and toolkit are listed in Chapter 19. Where ambiguity exists the OAIC publications should be preferred.

1.6. Currency of information.

Privacy law and regulatory guidance evolve over time. The last revision of this compendium was April 2026.

Chapter 2: Privacy act changes in 2026

2.1. The AML/CTF & Privacy Act interaction.

For most small law firms in Queensland, privacy compliance has not previously been a regulatory concern. The *Privacy Act 1988* (Cth) generally exempts 'small businesses' — defined as businesses with annual turnover of $3 million or less — from the requirement to comply with the Australian Privacy Principles.[7] Many law practices have operated below this threshold and have not been required to implement formal privacy compliance frameworks.

This position changes fundamentally from 1 July 2026. The AML/CTF Tranche 2 reforms extend anti-money laundering and counter-terrorism financing obligations to lawyers who provide 'designated services'.[8] When a business becomes a 'reporting entity' under the AML/CTF Act, it also becomes subject to the Privacy Act in respect of data collected for AML/CTF purposes — regardless of its annual turnover.[9]

This means that a law firm with annual turnover of, say, $800,000 that does conveyancing (a designated service) will need to comply with the APPs when handling personal information collected "*for or in connection with"* AML/CTF purposes — such as client identification documents, beneficial ownership information, and AML risk determination records.[10]

The Privacy Act may not apply to other records held by the firm relating to services that are not "designated services" or which were not collected for AML purposes.

When considering the content of this manual it is critically important to keep your firm's turnover in mind. If under $3M only some limited aspects of your data holdings and activities are affected. If over $3M, all of your data is potentially in scope.

For many firms the inconvenience of operating two independent data collection and management regimes *may* mean at least some elements of the Privacy compliant systems should be applied across the board. (Information security measures, for example).

However, opting into additional privacy regulatory obligation should be carefully considered before it is done. This could be either deliberate, using the formal opt-in process set out in the act,[11] or accidental by publishing statements or policies which do not clearly articulate that they only apply to a limited subset of data held. If, for example, your firm adopts a general Privacy Policy without clearly stating that it only applies to AML information it may be held to any broader promises made.

---

[7]Privacy Act 1988 (Cth), s 6D defines 'small business' as a business with annual turnover of $3 million or less.
[8]AUSTRAC, *Professional services*, Table 6 summary available at <https://www.austrac.gov.au/new-austrac/designated-services-newly-regulated-entities/professional-designated-services>.
[9]*Privacy Act* s.6E(1A)
[10]AUSTRAC, *Record keeping overview*, which confirms the 7-year retention period for AML/CTF records.
[11]OAIC: *opting into the Privacy Act*, available at <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/opting-in-to-the-privacy-act>

2.2. Key Dates and Timeline

The following timeline sets out the key dates for law firms preparing for AML/CTF and associated privacy compliance:[12]

Date	Milestone
10 December 2024	AML/CTF Amendment Act 2024 received Royal Assent, establishing the legal framework for Tranche 2 reforms.
31 March 2026	AUSTRAC enrolment opens for newly captured reporting entities including law firms providing designated services. Law firms should have a clear understanding of designated services and whether they intend to supply them by this point.
1 July 2026	AML/CTF obligations commence for law firms providing designated services. Privacy Act obligations commence concurrently for personal information collected for AML/CTF compliance.
10 December 2026	New APP 1 obligations commence requiring disclosure of automated decision-making that significantly affects individuals' rights or interests.

2.3. What are designated services?

A law firm will be affected if it provides any of the 'designated services' specified in the AML/CTF Act. AUSTRAC has also published guidance explaining the designated services law firms may typically provide.[13] These include:

- Assisting in the planning or execution of a transaction to buy or sell real estate;
- Assisting in the planning or execution of a transaction to buy, sell or transfer a business (including shares in a body corporate);
- Managing a client's money, securities or other property
- Assisting in loan transactions;
- Assisting in the creation, operation or management of trusts, companies or similar structures;
- Acting as, or arranging for another person to act as, a nominee director, secretary or shareholder, Providing a registered office for a body corporate.

Importantly, certain legal services are **excluded** from the designated services definition. These exclusions include:

- Legal advice only (even if about a designated service);
- Representation in court, tribunal or other dispute resolution proceedings (provided that a designated service is not provided as part of that work); and
- Trust account disbursements made on client instructions *in connection with legal services*.

The effect of these exclusions is that many law firm activities remain outside the AML/CTF regime, and will – provided their turnover is below $3Million, also remain outside the Privacy Act as well.

A firm that provides only family law assistance, for example, would not necessarily be providing designated services and would not need to worry about the Privacy Act provided it does not exceed the annual turnover threshold **and** can implement processes to ensure a designated service is not supplied accidentally.

For example, a family law property client agrees on a property division and consent order. One party is buying out the other's interest in a business premises. You refer the conveyancing work to a

[12]AUSTRAC, *about the reforms*, available at < https://www.austrac.gov.au/industry-and-business/about-amlctf-reforms/about-reforms >.
[13]

property firm, but your client came back to you for a guarantor's certificate. It is arguable[14] that advising on and witnessing the guarantor's certificate was a designated service. There is no *de minimis* exemption for either AML or Privacy Act obligations – once a single designated service is supplied the firm must adopt a regulatory compliance framework.

Practical Note

If you conclude that your firm does not provide designated services and want to keep it that way, your firm will need a clear understanding what is on and off the list and an effective policy to ensure that staff do not accept instructions within the AML regime.

If your firm provides any designated services — even occasionally — you will need to implement both AML/CTF compliance and privacy compliance frameworks. The privacy obligations apply to all personal information collected, used or disclosed for AML/CTF purposes, which includes client identification documents, beneficial ownership records, and transaction records retained for the mandatory 7-year period.

2.4. Consequences of Non-Compliance

Non-compliance with privacy obligations carries significant consequences across three dimensions: regulatory, professional, and reputational.

Regulatory consequences

The OAIC has a range of enforcement powers under the Privacy Act. Where a privacy complaint is substantiated or the OAIC identifies non-compliance through an investigation, possible outcomes include enforceable undertakings, adverse findings and civil penalties. For serious or repeated interferences with privacy, penalties of up to $50 million (or higher amounts based on benefit obtained or turnover) may apply.[15]

Separately, failure to comply with the Notifiable Data Breaches scheme, including failure to notify the OAIC and affected individuals of an eligible data breach, is an interference with privacy that may attract enforcement action.[16]

Professional consequences

Failure to comply with statutory obligations may also attract disciplinary attention from the legal services commission.

Reputational consequences

High-profile data breaches in the legal sector attract media attention and can significantly damage client trust , particularly given that clients entrust law firms with their most sensitive personal and financial information.

2.5. Benefits of Strong Privacy Practices

While this chapter has focused on the regulatory requirements and consequences of non-compliance, privacy compliance should not be viewed solely as a burden or risk mitigation exercise. Strong privacy practices deliver genuine benefits to law firms and their clients, including enhanced trust and streamlined information handling.

Improvements in cybersecurity are a particularly effective risk mitigation tool.

---

[14]But not certain – an area of frustration in interpreting the new obligations.
[15]Privacy Act 1988 (Cth), s 13G. Civil penalty provisions carry maximum penalties of the greater of $50 million, three times the value of the benefit obtained, or 30% of adjusted turnover: s 13G(4).
[16]Privacy Act 1988 (Cth), Part IIIC (Notifiable Data Breaches scheme), inserted by Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth).

The OAIC's Privacy Management Framework emphasises that privacy compliance is not a one-time project but an ongoing commitment.[17] The four-step cycle: Embed, Establish, Evaluate, Enhance, reflects the need to build privacy into firm culture, implement appropriate practices, monitor their effectiveness, and continuously improve. This manual provides the foundation for that ongoing commitment.

[17]OAIC: Privacy Management Framework, accessed: < https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/privacy-management-framework-enabling-compliance-and-encouraging-good-practice >

Key Takeaways — Chapter 2

- AML/CTF Tranche 2 reforms bring law firms providing designated services partially under the Privacy Act from 1 July 2026, regardless of annual turnover.
- Designated services include conveyancing, business sales, managing client property, and company/trust structuring , but exclude litigation and legal advice.
- Only information acquired or retained for AML/CTF purposes is regulated under the Privacy Act **if** your firm's turnover is less than $3M

Chapter 3: Sources of regulation and how they fit together

3.1. The Privacy Act 1988 (Cth)

The *Privacy Act 1988* (Cth) is the principal Commonwealth legislation governing the handling of personal information by Australian Government agencies and private sector organisations.

Who is covered?

The Privacy Act applies to 'APP entities', which include Australian Government agencies and 'organisations'.[18] For private sector purposes, an 'organisation' is generally trading entity that is not a small business operator.

A 'small business operator' is a business with annual turnover of $3 million or less.[19] Small business operators are generally exempt from the Privacy Act.

However, this exemption does not apply to businesses that fall within specified categories, including businesses that are reporting entities under the AML/CTF Act.[20] (See chapter

The AML/CTF & Privacy Act interaction.).

What is covered?

The Privacy Act regulates collection and use of 'personal information'. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether recorded in a material form or not.[21]

This definition is broad.[22] It includes obvious identifiers such as names, addresses, and dates of birth, but also extends to any information that could be used to identify an individual, either on its own or in combination with other information. For law firms, personal information likely to arise in relation to AML enquiries might include:

- client names, addresses, contact details, and dates of birth;
- identity documents (driver's licence, passport copies);
- financial information (bank account details, tax file numbers);
- information about third parties mentioned in client matters (trust beneficiaries, for example);
- beneficial ownership information.
- recruitment information (noting the employee records exemption for current employees).

Statutory obligations relating to personal information **are in addition to** a firm's confidentiality obligations to clients and others. A solicitor who wrongfully disclosed confidential information could be dealt with by the Legal Services Commissioner in addition to the OAIC.

It is important to note that *Privacy Act* obligations may apply with respect to information held about opposing parties, staff and anyone else whose personal information is entrusted to you.[23]

---

[18]Privacy Act 1988 (Cth), s 6(1) defines 'APP entity' to mean an agency or organisation. Section 6C sets out when an organisation is covered by the Act.
[19]Privacy Act 1988 (Cth), s 6D. Annual turnover includes all income from all sources; it does not include assets held, capital gains or proceeds of capital sales.
[20]Privacy Act 1988 (Cth), s 6C(1), item 2 of the table. See also OAIC, *Small business* guidance. Other extension categories apply, such as recipients of health information and contractors under some Commonwealth tenders.
[21]Privacy Act 1988 (Cth), s 6(1). The definition was amended by the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth) to clarify that information can be 'about' an individual even if it does not directly name them.
[22]See extended definitions in Chapters 7 and 20 for more information.
[23]For example, a client's or opposing party's customer database supplied in a business sale will likely include personal information relating to many people. In this example your firm's collection is not "for or in relation to AML" purposes but your client may be an APP regulated entity. Your firm may have both direct and indirect privacy obligations with respect to that data. You are also potentially liable to each person in the database under sch. 2 of the Privacy Act – serious invasion of privacy statutory tort regime. There is no small business exemption.

Sensitive information

'Sensitive information'[24] is a subset of personal information that attracts additional protections under the APPs. Sensitive information includes information about an individual's racial or ethnic origin, political opinions, religious beliefs, sexual orientation, criminal record, health information, genetic information, and biometric information.[25] It is likely that firms will need to consider sensitive information to undertake some AML/CTF enquiries (political affiliation, enquiries about Politically Exposed Persons and geographic source of funds information, for example.)

Law firms commonly hold sensitive information about clients and third parties, particularly in family law, criminal law, personal injury, and estate planning matters.

The collection of sensitive information generally requires consent from the individual concerned, unless an exception applies[26] (such as collection required by law for AML/CTF purposes where politically exposed person status must be determined).

Law firms may hold sensitive information without consent of the person to whom it relates if an exception applies[27]. The most common exception is necessity to establish legal claims or to comply with the law.

3.2. The Australian Privacy Principles

The Australian Privacy Principles (APPs) are contained in Schedule 1 to the Privacy Act.[28] There are 13 APPs covering the complete lifecycle of personal information: how it may be collected, what must be disclosed about its collection, how it may be used and disclosed, how it must be kept accurate and secure, and what rights individuals have to access and correct their information.

The APPs are principles-based rather than prescriptive. They establish outcomes that must be achieved but allow flexibility in how those outcomes are met. Many APP obligations are expressed in terms of 'reasonable steps', which means the steps that are appropriate will depend on the circumstances, including the size and resources of the entity, the amount and sensitivity of the information held, and the possible adverse consequences of a privacy breach.[29]

The 13 APPs may be grouped into five categories:

Category	APPs and Focus
Governance	APP 1 (open and transparent management) establishes the foundation: privacy policies, practices, procedures and systems
Collection	APPs 2-5 (anonymity, solicited collection, unsolicited collection, notification) govern how personal information may be collected and what individuals must be told
Use and Disclosure	APPs 6-9 (use/disclosure, direct marketing, cross-border disclosure, government identifiers) govern how information may be used and shared

[24]OAIC APP guidelines, key concepts, R-Z; < https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts >
[25]Privacy Act 1988 (Cth), s 6(1). Sensitive information includes information about racial or ethnic origin, political opinions, religious beliefs, sexual orientation, criminal record, health information, genetic information, and biometric information.
[26]APP 3.3(a), subject to limited exceptions where collection is “required or authorised by or under an Australian law or a court/tribunal order) (APP 3.4(a)) : this can be difficult where the collection is not specifically required by a court order but only from statements of good practice (information concerning a beneficiary’s capacity to manage finances, for example.). Another exception is where there is a “general situation”, most pertinent is where collection is necessary to establish a legal or equitable claim : Privacy Act s.16A(1), Item 1)
[27]App 3.4
[28]Privacy Act 1988 (Cth), Schedule 1 (Australian Privacy Principles). The APPs replaced the earlier National Privacy Principles and Information Privacy Principles from 12 March 2014.
[29]OAIC, *Australian Privacy Principles Guidelines*, Chapter A (Introduction), [A.7].

Data Quality and Security	APPs 10-11 (quality, security) require information to be accurate and protected
Individual Rights	APPs 12-13 (access, correction) give individuals (including non-clients) rights to see and correct their information

Detailed guidance on each APP is provided in the OAIC's APP Guidelines, which should be consulted when questions arise about specific obligations. See also APPs Most Relevant to Law Firms.

3.3. The Notifiable Data Breaches Scheme

Part IIIC of the Privacy Act establishes the Notifiable Data Breaches (NDB) scheme.[30] Under the NDB scheme, APP entities must notify the OAIC and affected individuals when a data breach occurs that is likely to result in serious harm.

A data breach occurs when personal information is subject to unauthorised access or disclosure, or is lost in circumstances where unauthorised access or disclosure is likely. An 'eligible data breach' occurs when a reasonable person would conclude that the breach is likely to result in serious harm to any of the individuals whose information was involved.

Where an entity suspects an eligible data breach may have occurred, it must conduct an assessment within 30 days. If the assessment confirms an eligible data breach, the entity must notify the OAIC and affected individuals as soon as practicable. The notification must include specific information about the breach and recommendations about steps individuals should take in response.

For law firms, data breaches may be particularly serious given the sensitive and confidential nature of legal information. Detailed guidance on breach response is provided in Chapter 17 of this manual, and the Data Breach Response Plan (Document 05 of the toolkit) provides a practical procedure for responding to incidents.

It should be noted that while the NDB may only apply to a small subset of information lost (that collected for AML purposes if a small business) our professional obligations usually require disclosure of lost and stolen data even if the data is not regulated.

3.4. The AML/CTF Act and Rules

Key AML/CTF obligations[31]

The principal AML/CTF obligations that might lead to collection of regulated information include:

Customer due diligence (CDD): Reporting entities must identify and verify the identity of customers before providing designated services. This requires collecting personal information including name, date of birth, and address, and verifying that information using reliable documents or electronic verification.[32] Even if you are also undertaking VOI to comply with other obligations (PEXA authorisation, for example) the fact that one of the purposes for which you collect or use the information brings it within the regulatory regime.[33]

Beneficial ownership identification: For corporate and trust clients, reporting entities must identify beneficial owners, the individuals who ultimately own or control the entity.

Ongoing due diligence: CDD is not a one-time activity. Reporting entities must monitor customer relationships and keep identification information up to date. Records relating to ongoing compliance activities are likely to be to be “for or in relation to AML”[34]

Record keeping: Reporting entities must retain CDD records and transaction records for seven years after the end of the customer relationship or the transaction, whichever is later.[35]

Suspicious matter reporting: Reporting entities must report suspicious matters to AUSTRAC. There are strict prohibitions on 'tipping off' , informing anyone that a report has been or may be made, including clients. This requires careful navigation of competing obligations under the AML/CTF regime, Legal Professional Privilege, the Privacy Act and the ASCR. SMR reports are rare. (In NZ on average, only one firm per year makes a SMR).

---

[30]Privacy Act 1988 (Cth), Part IIIC, inserted by Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth), commencing 22 February 2018.
[31]AUSTRAC, *Professional services (Reform)*, Table 6: Designated services for lawyers.
[32]Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), s 81 (reporting obligations) and Part 3 (customer due diligence).
[33]OAIC: Privacy guidance for reporting entities under the AML CTF Act, < https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/privacy-guidance-for-reporting-entities-under-the-anti-money-laundering-and-counter-terrorism-financing-act >
[34]Quare whether data referenced in such ongoing assessment is necessarily “collected for or in relation to” AML.
[35]Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), s 107 (record keeping for 7 years). See also AUSTRAC, *Record keeping overview*.

The Privacy Act governs how that personal information must be handled. Chapter 9 of this manual provides detailed guidance on the interaction between AML/CTF and privacy obligations.

3.5. Professional Obligations

Queensland solicitors are subject to professional obligations under the *Legal Profession Act 2007* (Qld) and the Solicitor's Conduct Rules. These obligations operate alongside, and in addition to, statutory privacy obligations.

Confidentiality

Rule 9 of the Australian Solicitors' Conduct Rules imposes a duty of confidentiality. A solicitor must not disclose any information which is confidential to a client and acquired during the client's engagement, except in limited circumstances.[36] The exceptions include disclosure required or permitted by law, disclosure with the client's consent, and disclosure to prevent serious criminal offences.[37]

The relationship between confidentiality and privacy obligations is discussed in detail in Chapter 4 of this manual.

Trust account obligations

The Legal Profession Act imposes detailed requirements for the operation of trust accounts, including record-keeping requirements that interact with both privacy and AML/CTF obligations.[38] Trust account records must be retained for seven years, which aligns with AML/CTF record-keeping requirements.

Professional conduct and discipline

Breach of statutory obligations, including privacy obligations, may constitute professional misconduct or unsatisfactory professional conduct under the Legal Profession Act. A solicitor who fails to implement reasonable security measures and suffers a data breach affecting client information may face disciplinary proceedings in addition to regulatory action by the OAIC.

Legal Professional Privilege (Client Legal Privilege) ("LPP")

LPP is preserved under the AML/CTF regime although specifics are unclear.[39]

Other

There are a variety of other confidentiality and data security obligations that apply to certain matters. Inspection of some types of subpoena information in the Family Court might require adherence to very detailed undertakings, and notification to the Court if information is lost for example.Family Court and DV proceedings are also generally confidential under their specific legislation.

Material acquired through compulsory Court processes, subpoenas and discovery are subject to the "Implied Undertaking / Harman Undertaking" obligation not to use it for a collateral purpose. [40]

Cybersecurity, data handling obligations and incident reporting obligations often apply to the users of electronic networks, such as Electronic Conveyancing systems, court portals and many tender/retainer arrangements with clients will contain specific obligations as well. Insurers (Such as Lexon and Chubb) may have minimum requirements.

While only the Privacy Act issues are within the scope of this compendium, it is important to keep other obligations in mind when constructing firm systems and processes.

---

[36]Australian Solicitors' Conduct Rules 2012 (Qld), r 9.1.
[37]Australian Solicitors' Conduct Rules 2012 (Qld), r 9.2 sets out the exceptions permitting disclosure, including where required by law, to prevent serious criminal offences, or with client consent.
[38]Legal Profession Act 2007 (Qld), Part 3.4 (Trust money and trust accounts), particularly Division 2 (Trust accounts).
[39]See the Law Institute of Victoria resource here: 20251211_Ethics Guideline_Balancing_LPP_and_AML_Final.pdf
[40]See Hearne v Street [2008] HCA 36

3.6. The OAIC's Role

The Office of the Australian Information Commissioner (OAIC) is the regulator primarily responsible for privacy in Australia. The OAIC's functions include guidance, complaints handling[41], investigations[42] and enforcement. They also administer the NDB scheme.[43] However, multiple regulators may be involved.

Key Point: Multiple Regulators

Law firms providing designated services from 1 July 2026 will be subject to oversight by multiple regulators:

- OAIC for privacy compliance under the Privacy Act
- AUSTRAC for AML/CTF compliance and record keeping
- Legal Services Commission / Law Society or Institute, Courts — for professional conduct

Compliance frameworks should be designed to meet all applicable obligations concurrently.

[41]Privacy Act 1988 (Cth), Part V (Investigations). See also OAIC, Guide to Privacy Regulatory Action, Chapter 1 (Privacy complaint handling process).
[42]Privacy Act 1988 (Cth), s 13G (civil penalties) and s 80W (enforceable undertakings).
[43]Privacy Act 1988 (Cth), s 33C (functions of the Information Commissioner).

PART B

FROM OBSERVING CONFIDENTIALITY TO PRIVACY COMPLIANCE

Chapter 4: Confidentiality vs Privacy — Key Distinctions

Confidentiality is hardwired into a Law Firm's DNA. Confidentiality and privacy, while related, are distinct concepts with different sources, scope, and practical requirements.

4.1. The Familiar Territory: Solicitor's Duty of Confidentiality

The duty of confidentiality is fundamental to legal practice. Every solicitor understands that they must not disclose information that is confidential to a client, about a client's matter or acquired through court processes about someone else. These duties arise from professional rules, fiduciary obligations and contractual agreements.

4.2. New Privacy Obligations

Privacy obligations under the Privacy Act represent a distinct layer of obligation that operates alongside confidentiality and privilege. Understanding how privacy differs from confidentiality is essential for Principals implementing compliance frameworks.

Different scope

As discussed above, Privacy obligations apply to 'personal information' , information about an identified or reasonably identifiable individual. This is broader than 'confidential information' in some respects (it includes information that may not be confidential, such as a client's publicly available business address) but narrower in others (it does not include information about corporations, which may be confidential). Where the holder is also a small business only AML related personal information is regulated.

Different focus

The duty of confidentiality is primarily about *non-disclosure* — not revealing information to others. Privacy obligations are broader: they govern the entire lifecycle of information handling, including *how* information is collected, *what* individuals must be told about its collection, how it must be kept *secure*, and what *rights* individuals have to access and correct it.

Different requirements

Privacy compliance requires specific actions that confidentiality does not:

Published privacy policy: APP 1 requires a clearly expressed, up-to-date privacy policy that is made available free of charge.[44] Confidentiality has no equivalent requirement.

Collection notices: APP 5 requires notification to individuals at or before the time personal information is collected, explaining what is collected and why.[45] Confidentiality imposes no such notification requirement.

---

[44]Australian Privacy Principle 1.3-1.4, requiring a clearly expressed and up-to-date privacy policy.
[45]Australian Privacy Principle 5, requiring notification of collection at or before the time of collection, or as soon as practicable afterwards.

Access and correction rights: APPs 12 and 13 give individuals rights to access personal information held about them and to request correction.[46] Confidentiality creates no such individual rights, although clients have access and correction rights arising through other sources.

Breach notification: The NDB scheme requires notification to the OAIC and affected individuals when a serious data breach occurs.[47] Where a breach of confidentiality has occurred only disclosure to clients is necessarily triggered, although professional duties might require disclosure to courts and counterparties as well.

4.3. How They Interact in Practice

The three frameworks, confidentiality, privilege, and privacy, operate concurrently. Compliance with one does not satisfy the others. A law firm must meet all applicable obligations.

Information that is confidential AND personal information

Most client information handled by law firms will be both confidential to the client and personal information about an individual. For example, a client's identity documents collected for AML/CTF purposes are confidential (the firm must not disclose them without authority or legal necessity) and personal information (the APPs govern how they must be handled).

For such information, the firm must:

- maintain confidentiality (not disclose without authority or lawful reason);
- comply with APP collection requirements (collect only what is necessary, notify of collection);
- comply with APP use and disclosure requirements;
- maintain security (APP 11);
- respond to access and correction requests (APPs 12-13).

Information that is confidential but NOT personal information

Some client information may be confidential but not personal information. For example, a corporation's commercial strategy or trade secrets. Such information is subject to the duty of confidentiality but not the APPs (since the APPs only apply to information about individuals).

Information that is personal information but NOT confidential

Some personal information may not be confidential. For example, a client's publicly listed business address or information obtained from public registers (once it has been disclosed that the firm acts for the client).

The APPs still apply to such information (the firm must still handle it in accordance with the APPs), even though confidentiality obligations may be less stringent.

Reminder: if your firm is under the annual $3M turnover threshold, only the AML/CTF related information is subject to the Privacy Act. All other confidentiality obligations apply.

Key Insight:

A firm that has always maintained strict confidentiality is NOT automatically privacy compliant.

Confidentiality focuses on non-disclosure; privacy requires proactive management , telling people what you collect and why (APP 5), giving them access to their information (APP 12), maintaining documented security systems (APP 11), and having a published privacy policy (APP 1).

These are new, additional requirements that must be implemented alongside existing confidentiality practices.

[46]Australian Privacy Principles 12 and 13, giving individuals rights to access and correct personal information held about them.
[47]Privacy Act 1988 (Cth), Part IIIC (Notifiable Data Breaches scheme), requiring notification to the OAIC and affected individuals of eligible data breaches.

4.4. Practical Implications

Broad conceptual alignment:

Confidentiality exceptions align with most privacy exceptions

Both the confidentiality rules and the APPs recognise that disclosure may be required or permitted by law.[48] [49] This means that disclosures required by law under legislation such as the AML/CTF Act (eg, suspicious matter reports to AUSTRAC) are authorised under both frameworks.

As privilege is maintained under the AML/CTF regime, disclosure of privileged information is not required by the legislation and therefore not permitted by the conduct rules.

Privacy rights create new obligations

The individual rights under APPs 12 and 13 (access and correction) create obligations that do not exist under confidentiality law insofar as they apply to non-clients. A firm must have procedures for handling access requests, including within the reasonable timeframes expected by the OAIC.[50]

Documentation is required

Privacy compliance requires documentation that confidentiality does not: a published privacy policy, collection notices, security procedures, breach response plans, and records of compliance activities. The toolkit documents accompanying this manual provide templates for this documentation.

Key Takeaways — Chapter 4

• Confidentiality, legal professional privilege, and privacy are related but distinct legal concepts with different sources, scopes, and requirements.

• Confidentiality focuses on non-disclosure; privacy requires proactive information management throughout the information lifecycle.

• Privacy compliance requires documentation (policies, notices, procedures) that confidentiality does not.

• Privacy creates individual rights (access, correction) that do not exist under confidentiality law.

• A firm that maintains strict confidentiality is not automatically privacy compliant. Additional steps are required.

[48] Australian Solicitors' Conduct Rules 2012 (Qld), r 9.2.1 (disclosure compelled by law).
[49] Australian Privacy Principle 6.2(b) permits use or disclosure required or authorised by or under an Australian law; See OAIC Australian Privacy Principles: < https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information >
[50] OAIC, Chapter 1: APP 1 — Open and transparent management of personal information, APP Guidelines (October 2025), [1.4]-[1.5].

Chapter 5: What Changes for Your Firm

Chapter 4 explained the conceptual distinction between confidentiality and privacy.

This chapter turns to practical matters: what specific new requirements will your firm need to implement? Understanding these changes is essential for planning your compliance program and allocating appropriate resources.

5.1. New Documentation Requirements

Privacy compliance requires specific documentation that most smaller law firms will not currently have. The following table summarises the key documentation requirements and identifies the toolkit document that addresses each:

APP Requirement	What This Means	Toolkit Document	New for Most Firms?
APP 1.3-1.4: Privacy policy	A clearly expressed, up-to-date policy describing how you handle personal information, available free of charge[51]	Doc 01: Privacy Policy Template	Yes
APP 1.2: Privacy practices and systems	Documented practices, procedures and systems for ensuring APP compliance	Doc 03: PI Inventory Doc 04: Retention Schedule	Yes No
APP 5: Collection notification	Notice to individuals at or before collection explaining what you collect and why. For many firms some additions to your letter of engagement may be enough.	Doc 02: Collection Notice Template	Yes
APP 11: Security measures	Documented security procedures to protect personal information from misuse, loss, and unauthorised access	Doc 05: Data Breach Response Plan (Suggested: SMB 1001)	Partial
NDB scheme: Breach response	A documented plan for assessing and responding to data breaches, including notification procedures	Doc 05: Data Breach Response Plan	Yes
APP 1.2: Risk assessment	Assessment of privacy risks for new projects or significant changes to information handling	Doc 06: Privacy Impact Assessment	Yes
APP 1.2: Staff training	Training for staff on privacy obligations and the firm's privacy procedures	Doc 07: Staff Training Framework	Yes

The 'Partial' notation for security measures reflects that most law firms already have some security controls in place (password policies, locked premises, secure document disposal). However, these measures may not be documented and systematic.

[51] OAIC, *Guide to developing an APP privacy policy* (September 2024), available at <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/guide-to-developing-an-app-privacy-policy>.

5.2. New Processes

Beyond documentation, privacy compliance requires implementing new operational processes. These processes will need to be integrated into the firm's existing workflows.

Collection notification

APP 5 requires notification to individuals at or before the time of collection (or as soon as practicable afterwards).[52] In addition to having template notice/s, you need to embed new processes to ensure they are given as required.[53]

For law firms, this typically means:

- Including a collection notice in engagement letters or as an attachment to the costs agreement;
- Providing a specific notice when collecting identity documents for AML/CTF purposes;
- Providing a notice to beneficial owners and **other third parties** from or about whom information is collected;[54]
- Including a privacy notice on website contact forms.

Data breach assessment and notification

The Notifiable Data Breaches scheme requires a formal process for **assessing** and **responding** to data breaches, and Privacy Act compliance requires that a basic framework plan be in place before hand[55] The OAIC website contains useful information and decision-trees.

When a breach occurs (or is suspected), the firm must:

1. Contain the breach and take immediate steps to limit any damage;
2. Assess the breach to determine whether it is an 'eligible data breach' (within 30 days);
3. Notify the OAIC and affected individuals if the breach is eligible; and
4. Review the incident and implement improvements to prevent recurrence.[56]

This requires having a documented plan, designated personnel, and practised procedures *before* a breach occurs. The Data Breach Response Plan (Document 05) provides this (very basic) framework. In most cases a firm will call in outside assistance in the event of a data breach.

Privacy impact assessment

APP 1.2 requires entities to take reasonable steps to implement practices, procedures and systems for managing personal information in accordance with the APPs.[57] One element of this is conducting privacy impact assessments (PIAs) when planning new projects or significant changes that involve personal information.[58]

For small law firms, PIAs are most likely to be relevant when:

- Implementing new practice management or document management systems;
- Engaging new IT service providers or cloud platforms;
- Implementing AI tools that process client information;
- Expanding into new practice areas that involve different types of personal information; or
- Making significant changes to information security arrangements.

---

[52]Australian Privacy Principle 5.1. The nine matters that must be notified are set out in APP 5.2.
[53]OAIC, Chapter 5: APP 5 — Notification of the collection of personal information, APP Guidelines (October 2025), [5.1]-[5.8].
[54] Keep ASCR R.33 ("No-Contact Rule") in mind.
[55]Privacy Act 1988 (Cth), Part IIIC (Notifiable Data Breaches scheme), ss 26WE-26WK.
[56]OAIC, *Data breach preparation and response* (February 2025), Part 2: Responding to data breaches — four key steps.
[57]Australian Privacy Principle 1.2..
[58]OAIC, *Guide to undertaking privacy impact assessments* (September 2024), available at <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments>.

The Privacy Impact Assessment (Document 06) includes a threshold assessment tool to help determine when a full PIA is warranted.

5.3. Individual Rights: New Obligations

Some APPs create rights do not exist under confidentiality law and represent genuinely new obligations for most law firms, especially as they relate to people who are not clients.

Right to access (APP 12)

Individuals have a right to request access to personal information that the firm holds about them.[59] The firm must respond to such requests within a reasonable period. The OAIC indicates that 30 calendar days is generally reasonable.[60] Clients have always had the right to collect their file, but this extends to third parties.

Access requests require no particular form , they can be made verbally or in writing, and need not use specific language. Staff must be trained to recognise access requests.

There are exceptions that permit refusal of access in certain circumstances, including where access would reveal legally privileged information, would prejudice legal proceedings, or would reveal evaluative information in a commercially sensitive decision-making process.[61]

These exceptions are particularly relevant to law firms. In practical terms, many requests by non-clients can be refused, however a structured process to assess and respond is needed. See chapter 16 provides detailed guidance on handling access requests.

Again, right of access looks different for firms under or over the turnover threshold. For firms below, only AML / CTF related holdings are subject to the access right. Most firms will hold little if any such data that does not relate to clients[62] so there will likely be little practical application. Firms over the threshold might hold information about more non-clients with a prima-facie access right, but even in this case many exceptions will apply.

Access to information where a firm has submitted a Suspicious Matter Report and terminated their retainer is complicated, and careful consideration is needed to avoid accidentally “tipping off” the former client that an SMR has been submitted.

Right to correction (APP 13)

Individuals have a right to request correction of regulated personal information that is inaccurate, out of date, incomplete, irrelevant or misleading.[63] If the firm refuses to correct information as requested, it must give written notice of the refusal and allow the individual to request that a statement be associated with the information.[64]

For law firms, correction requests might relate to contact details, identification information, or factual assertions recorded in file notes or correspondence. Care must be taken not to alter information that forms part of the legal record of a matter. In most cases an accompanying notation indicating that a “fact” is in dispute is more appropriate.

Right to complain

Individuals have a right to complain to the firm if they believe their privacy has not been handled in accordance with the APPs. The firm should have an internal complaint handling process.[65] If a complaint is not resolved to the individual's satisfaction, they may escalate the complaint to the OAIC.[66]

---

[59]Australian Privacy Principle 12.1
[60]OAIC, *Dealing with requests for access to personal information* (July 2025). The OAIC indicates that 30 calendar days is generally a reasonable period for responding to access requests.
[61]Australian Privacy Principle 12.3, , sets out the exceptions to the access requirement.
[62]The notable exception being beneficial ownership data relating to the identities and characteristics of beneficiaries of trusts, including testamentary trusts, related individuals.
[63]Australian Privacy Principle 13.1
[64]Australian Privacy Principle 13.2. If the entity refuses to correct, APP 13.3 requires the entity to associate a statement with the information.
[65]OAIC, *Handling privacy complaints* (September 2024), available at <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/handling-privacy-complaints>.
[66]Privacy Act 1988 (Cth), s 36 (complaints to the Information Commissioner).

The firm's privacy policy must explain how individuals can complain and how complaints will be handled. Chapter 18 provides guidance on complaint handling.

5.4. What Stays the Same

While privacy compliance introduces new requirements, it is important to recognise that the core of legal practice remains unchanged. Privacy obligations are *additional* to existing obligations , they do not replace or diminish them.

Confidentiality duty continues

The solicitor's duty of confidentiality under the Australian Solicitors' Conduct Rules continues to apply.[67] Privacy obligations do not override, diminish, or replace this duty. Rather, they operate alongside it. A solicitor must continue to maintain confidentiality of client information *and* comply with the APPs.

Legal professional privilege protections continue

Legal professional privilege continues to protect privileged communications.[68] The APPs do not override privilege. In particular:

- APP 12 (access) includes an exception for information that would reveal information to which a claim to legal professional privilege applies;[69]
- APP 12 includes exceptions for information relating to existing or anticipated legal proceedings;[70]
- The privilege belongs to the client, and the client's ability to claim or waive privilege is unaffected by the APPs.

Core legal practice unchanged

Privacy compliance does not change how legal services are provided. Solicitors continue to:

- Collect information necessary to provide legal services;
- Use that information for the purpose of providing those services;
- Disclose information as necessary to conduct matters (to courts, opposing parties, third parties);
- Retain files in accordance with professional obligations;

However, each firm must consider its information handling processes and determine whether collection and retention really is necessary. Material collected and stored out of habit should be identified and practices adjusted accordingly. Even if data is not regulated collection and retention practices should be considered as part of this review. Data captured and kept is an ongoing responsibility. If your firm does not have to expose itself to risk and ongoing management costs not doing so benefits both the firm and the clients.

What changes is that these activities must now be conducted within a documented privacy framework, with appropriate notices to individuals about information handling, and with procedures for responding to individual rights requests.

Key Message for Practitioners

Privacy compliance is about how you document and manage information handling, not about fundamentally changing how you practise law.

You will continue to collect information to serve clients, maintain confidentiality, and exercise professional judgment. The new requirements ensure that individuals understand how their information is handled and have rights to access and correct it , principles that align with the values of the legal profession.

---

[67] Australian Solicitors' Conduct Rules 2012 (Qld), r 9.1.
[68] Evidence Act 1995 (Cth), ss 118-119. Legal professional privilege continues to apply to privileged communications regardless of Privacy Act obligations.
[69] Australian Privacy Principle 12.3(h), which permits refusal of access where giving access would reveal evaluative information in connection with a commercially sensitive decision-making process.
[70] Australian Privacy Principle 12.3(d)-(e).

It has always been a good idea not to collect and store more confidential / sensitive data than you have to.

Chapter 6: Getting ready for privacy compliance.

Before implementing new privacy compliance measures, it is valuable to assess your firm's current practices. Many law firms already have practices in place that contribute to privacy compliance — they simply have not been documented or labelled as such. This chapter provides assessment tools to help you identify what you already do well and where gaps exist.

6.1. Assess what you have and list what you need

Privacy Requirement	Assessment Question	Toolkit Reference	Yes	No
Published privacy policy	Does your firm have a privacy policy published on its website that describes how you handle personal information?	Doc 01	☐	☐
Collection notices	Does your firm provide written notices to clients explaining what personal information you collect and why?	Doc 02	☐	☐
Personal information inventory	Does your firm maintain a register of the categories of personal information held and where it is stored?	Doc 03	☐	☐
Documented retention schedule	Does your firm have a documented schedule specifying retention periods for different types of records?	Doc 04	☐	☐
Data breach response plan	Does your firm have a documented plan for responding to data breaches, including notification procedures?	Doc 05	☐	☐
PIA process	Does your firm have a process for assessing privacy risks when implementing new systems or processes?	Doc 06	☐	☐
Privacy-specific training	Do staff receive specific training on privacy obligations and the firm's privacy procedures?	Doc 07	☐	☐
Access request procedure	Does your firm have a documented procedure for handling requests from individuals to access their personal information?	Manual Ch 16	☐	☐
Correction request procedure	Does your firm have a documented procedure for handling requests to correct personal information?	Manual Ch 16	☐	☐
Privacy complaint procedure	Does your firm have a documented procedure for handling privacy complaints?	Manual Ch 18	☐	☐

6.2. Preparing for Implementation

Before proceeding to implement the toolkit documents, ensure the following preparatory steps are completed:

1. **Designate a Privacy Officer:** Identify who will be responsible for privacy compliance. In a small firm, this is typically a Principal, but may be delegated to a Practice Manager or other senior staff member. The Privacy Officer will be the primary user of this manual.[71]
2. **Assess designated services:** Determine which of your firm's services are 'designated services' under the AML/CTF Act. This will confirm whether your firm becomes a reporting entity from 1 July 2026 and the scope of your privacy obligations.[72]
3. **Allocate implementation time:** Privacy compliance implementation requires focused effort. Block time in the Privacy Officer's schedule for the initial implementation project. Although the work required for many firms is not onerous, leaving plenty of time to do it will minimize stress.
4. **Brief key stakeholders:** Ensure all Principals and senior staff understand the project and why it needs to happen.
5. **Gather existing documentation:** Collect copies of existing documents that may inform the implementation: engagement letter templates, employment contracts, IT policies, office procedures, and any existing privacy-related documents. These will help customise the toolkit documents to your firm's context.

Timeline Alert

Privacy obligations commence on 1 July 2026 for firms providing designated services.

Working backwards from this date, your implementation project should commence as soon as possible to allow adequate time for compliance activities, bearing in mind that AML / CTF preparation will also place a heavy burden on your firm’s resources.

Key Takeaways — Chapters 5 and 6

- Privacy compliance introduces new documentation (privacy policy, collection notices, inventory, retention schedule, breach plan, PIAs, training) and new processes.
- Individual rights under APPs 12-13 create new obligations to respond to access and correction requests insofar as these relate to regulated personal information.
- Core legal practice, confidentiality duties, and legal professional privilege protections continue unchanged.
- Most law firms have foundational practices (security, file management, staff obligations) that support privacy compliance.
- The gap assessment checklists identify where implementation effort is needed — privacy-specific gaps are expected for firms new to the Privacy Act.

[71]OAIC, Chapter 1: APP 1 — Open and transparent management of personal information, APP Guidelines (October 2025), [1.10]-[1.15].
[72]Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), Part 2 (Customer identification procedures).

PART C

UNDERSTANDING THE AUSTRALIAN PRIVACY PRINCIPLES

Chapter 7: Introduction to the APPs

The Australian Privacy Principles (APPs) are the cornerstone of privacy regulation for private sector organisations in Australia. This chapter provides an introduction to the APPs , their structure, and how to read and apply them. Skip this section if you are already broadly familiar with the APPs.

More detailed guidance on specific APPs most relevant to law firms follows in Chapter 8. Detailed guidance for each APP can also be found on the OAIC website.

7.1. What Are the APPs?

The APPs are contained in Schedule 1 to the Privacy Act 1988 (Cth).[73] They establish legally binding requirements for how APP entities (including organisations covered by the Act) must handle personal information. The APPs are supplemented by the OAIC's APP Guidelines, which provide detailed guidance on how each APP should be interpreted and applied.[74]

7.2. Structure and Overview of the 13 APPs

The 13 APPs cover the complete lifecycle of personal information handling. They can be grouped into five categories:

APP	Title	Core Requirement
GOVERNANCE AND STANDARDS		
APP 1	Open and transparent management	Take reasonable steps to implement practices, procedures and systems; have a clearly expressed privacy policy
COLLECTION OF PERSONAL INFORMATION		
APP 2	Anonymity and pseudonymity	Give individuals the option to interact anonymously or pseudonymously where practicable
APP 3	Collection of solicited information	Only collect personal information that is reasonably necessary; collect sensitive information only with consent or under exception
APP 4	Dealing with unsolicited information	Determine if unsolicited information could have been collected under APP 3; if not, destroy or de-identify

[73]Privacy Act 1988 (Cth), Schedule 1 (Australian Privacy Principles). The APPs commenced on 12 March 2014, replacing the National Privacy Principles.
[74]OAIC, *Australian Privacy Principles Guidelines* (October 2025), Chapter A (Introduction), [A.1].

APP 5	Notification of collection	Notify individuals at or before collection about what is collected, why, and how to access/correct it
USE AND DISCLOSURE OF PERSONAL INFORMATION		
APP 6	Use or disclosure	Only use or disclose for the primary purpose of collection, or for a secondary purpose where an exception applies
APP 7	Direct marketing	Do not use personal information for direct marketing unless specific conditions met
APP 8	Cross-border disclosure	Take reasonable steps before disclosing overseas (such as using software processed on overseas servers) to ensure the recipient does not breach the APPs
APP 9	Adoption, use or disclosure of government identifiers	Must not adopt government identifiers as own identifier; limited circumstances for use/disclosure
DATA QUALITY AND SECURITY		
APP 10	Quality of personal information	Take reasonable steps to ensure personal information is accurate, up-to-date, complete and relevant
APP 11	Security of personal information	Take reasonable steps to protect from misuse, interference, loss, unauthorised access, modification or disclosure; destroy or de-identify when no longer needed
ACCESS AND CORRECTION		
APP 12	Access to personal information	On request, give individuals access to their personal information unless an exception applies
APP 13	Correction of personal information	Take reasonable steps to correct personal information to ensure it is accurate, up-to-date, complete, relevant and not misleading

7.3. Key Definitions

Understanding the APPs requires familiarity with several key definitions:

Personal information

Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether recorded in a material form or not. This is a broad definition , it includes not just obvious identifiers (name, address) but any information that could be used to identify someone.

Sensitive information

A subset of personal information that attracts additional protections. Sensitive information includes information about racial or ethnic origin, political opinions, membership of political associations, religious beliefs, philosophical beliefs, membership of professional or trade associations, membership of trade unions, sexual orientation or practices, criminal record, health information, genetic information, biometric information, and biometric templates.

Collection

The gathering, acquiring, or obtaining of personal information from any source and by any means. This includes information provided directly by individuals, information obtained from third parties, and information generated through observation or monitoring.

Use

The handling of personal information within the entity. This includes accessing, reading, analysing, referencing, or otherwise doing something with personal information within the organisation.

Disclosure

Making personal information accessible to others outside the entity or releasing it from the entity's effective control. Disclosure to courts, opposing parties, and regulators are all disclosures for privacy purposes.

7.4. The 'Reasonable Steps' Standard

Many APP obligations are expressed in terms of taking 'reasonable steps'.[75] What constitutes 'reasonable steps' is not fixed, it depends on the circumstances. Factors that may be relevant include:

- the amount and sensitivity of the personal information held;
- the possible adverse consequences for individuals if the information is mishandled;
- the nature and size of the entity;
- the practicability of implementing the step, including time and cost;
- the availability and effectiveness of the step.

The sensitivity of legal information — some of it literally life and death — means that a high degree of care and protection is warranted.

A small law firm is not expected to implement the same technical security measures as a large one, but it is expected to take steps proportionate to the risks posed by its information holdings.

The same approach applies to determining what is reasonable from the perspective of confidentiality obligations. Even a small firm is expected to think about consequences of information it holds being lost and taking especial care with highly sensitive material.

Practical Application: 'Reasonable Steps' for Small Law Firms

For a small law firm handling sensitive client information including identity documents and financial details:

- Reasonable security steps (APP 11) might include: strong passwords, multi-factor authentication, adding extra encryption for sensitive documents (medical reports, negotiations in criminal matters for example), secure physical storage, and staff training on security practices.[76]
- Reasonable collection steps (APP 3) might include: ensuring that only essential ID records are collected and if stored long term, that clients and third parties know what is being collected and why.
- The steps do not need to be perfect, but they do need to be genuine and proportionate to the risk.

---

[75]OAIC, *Australian Privacy Principles Guidelines*; Key Points (para 1.6, 1.7), see also para 5.1 – 5.6), Chapter A, [A.7]-[A.10], Chapter B [B.110] – [B.112] (explanation of 'reasonable steps' standard).
[76]See Australian Cyber Security Centre (Joint initiative with Australian Signals Directorate) *Small business cyber security guide*. < https://www.cyber.gov.au/business-government/small-business-cyber-security/small-business-hub/small-business-cyber-security-guide >

A recognized cybersecurity standard such as SMB-1001 (small firm) or ISO-27001 (big firm) can assist in demonstrating that reasonable steps were taken to protect client information.

Chapter 8: APPs Most Relevant to Law Firms

While all 13 APPs apply to law firms that are APP entities, some are more significant in day-to-day practice than others. This chapter provides detailed guidance on the APPs that most directly affect how law firms operate.

8.1. APP 1: Open and Transparent Management

APP 1 is the foundation principle. It requires entities to take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs and enable the entity to deal with inquiries or complaints.[77]

The privacy policy requirement

APP 1.3 requires a clearly expressed and up-to-date policy about the entity's management of personal information.[78] This policy must be available free of charge and in an appropriate form , typically on the firm's website.

APP 1.4 specifies that the policy must contain information about:[79]

- the kinds of personal information collected and held;
- how personal information is collected and held;
- the purposes for which personal information is collected, held, used and disclosed;
- how an individual may access their personal information and seek correction;
- how an individual may complain about a breach of the APPs and how the entity will deal with such a complaint; and
- whether the entity is likely to disclose personal information to overseas recipients, and if so, the countries where they are located.

From 10 December 2026, APP 1.4 will also require disclosure of any substantially automated decisions using personal information that significantly affect individuals' rights or interests.[80]

The Privacy Policy Template (Document 01) provides a template that addresses mandatory elements and some issues most relevant to law firms.

8.2. APP 3: Collection of “Solicited Personal Information”

APP 3 governs what personal information may be collected. The core principle is that collection must be limited to what is 'reasonably necessary' for the entity's functions or activities.[81]

[77]Australian Privacy Principle 1.2,
[78]Australian Privacy Principle 1.3,
[79]Australian Privacy Principle 1.4,. The matters that must be included are set out in APP 1.4(a)-(f).
[80]Privacy and Other Legislation Amendment Act 2024 (Cth), Schedule 1, item 17, inserting new APP 1.4(fa) (automated decision-making disclosure), commencing 10 December 2026.
[81]Australian Privacy Principle 3.1,

Collection must be 'reasonably necessary'

Personal information (and by extension, sensitive information) may only be collected if it is reasonably necessary for one or more of the entity's functions or activities.[82] For law firms, 'functions or activities' include providing legal services, complying with legal, regulatory and insurance obligations (including AML/CTF requirements), managing client relationships, and running the business. However, just because information might be useful for one of those functions does not necessarily mean that it should automatically be collected.

The test is not “absolutely essential” or “possibly relevant”, it is a mid point: “reasonably **necessary**”. Drawing that line is not always easy, especially when the ultimate direction and scope of a matter might not be apparent from the outset.

There is no fixed list of required information in every circumstance. What is expected is that you turn your mind to the issue and can provide a defensible rationale. In practical terms this means that firms should review types of matters they do regularly and only collect information that is genuinely needed. This will mean reviewing and maintaining your intake form checklists to ensure that information collected is really needed.

Sometimes, this kind of risk analysis might *increase* the scope of information collected. It would be a good idea to keep a record of the guidance which formed the basis of your policy. For example, if a Lexon risk checklist or Practice Direction requires that certain issues be investigated that should be noted. It will save a lot of time later if a regulator asks you to justify why certain records were collected or held.

Again, only AML related information is regulated for small businesses. Despite that, it is a good idea to turn a sceptical lens on all information collection and retention due to the risk and cost that goes with holding other people’s data.

Sensitive information: higher threshold

Sensitive information may only be collected if the individual consents and the information is reasonably necessary, *or* if an exception applies (such as collection required or authorised by law).[83]

Law firms may collect sensitive information in various contexts: health information in personal injury matters, criminal history in criminal defence matters, or information about political exposure for AML/CTF purposes. Where consent is the basis for collection, ensure the consent is informed and voluntary. Where another exception is the basis (health information concerning capacity of an at-risk beneficiary, for example) ensure that there is justification for collection. This can be difficult where collection is only good practice rather than a mandatory requirement.

Collection by lawful and fair means

APP 3.5 requires that personal information be collected only by lawful and fair means, and APP 3.6 requires that, where reasonable and practicable, information be collected directly from the individual.[84]

For law firms, collecting information about third parties (such as beneficial owners, witnesses, opposing parties or information from searches and investigations) is common and permitted, but the collection must still be lawful and fair. Most scenarios do not involve collection for AML purposes but there are some.

---

[82]Australian Privacy Principle 3.2,
[83]Australian Privacy Principle 3.3, Sensitive information includes health information, biometric information, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, and criminal record.
[84]Australian Privacy Principle 3.4.

8.3. APP 5: Notification of Collection

APP 5 requires notification to individuals at or before the time of collection, or as soon as practicable afterwards.[85] This is a significant new obligation for firms that have not previously been subject to the Privacy Act.

Required content of notification

APP 5.2 specifies nine matters that must be notified:[86]

- the entity's identity and contact details;
- if collection is from a third party, the fact and circumstances of that collection;
- if collection is required or authorised by law, that fact and the law requiring/authorising it;
- the purposes for which information is collected;
- the consequences if information is not collected;
- the entities or types of entities to which information is usually disclosed;
- that the privacy policy contains information about access and correction;
- that the privacy policy contains information about complaints; and
- if disclosure overseas is likely, the countries where recipients are located.

The Collection Notice Template (Document 02) was prepared by the OAIC as a generic notice designed for AML reporting entities. The scope is therefore very limited. Each firm should consider whether more templates specific to individual scenarios might be useful.

Where collected concerning a represented party the Collection Notice should go to that person's solicitor.[87]

8.4. APP 6: Use and Disclosure

APP 6 governs how personal information may be used and disclosed after collection. The core principle is that information should only be used or disclosed for the 'primary purpose' of collection, unless an exception applies.[88]

Primary purpose

The 'primary purpose' is the main reason the information was collected. For law firms, the primary purpose of collecting client information is typically to provide legal services in connection with the relevant matter. Use for that purpose requires no further justification.

Exceptions for secondary purposes

APP 6.2 sets out exceptions that permit use or disclosure for a secondary purpose. Exceptions most relevant to law firms include:[89]

- **Consent:** The individual has consented to the secondary use or disclosure.
- **Related purpose (reasonable expectation):** The secondary purpose is related to the primary purpose, and the individual would reasonably expect the use or disclosure.
- **Required or authorised by law:** The use or disclosure is required or authorised by or under an Australian law (including AML/CTF reporting obligations).
- **Enforcement:** A permitted general situation applies (e.g., disclosure to enforcement bodies).
- **Legal proceedings:** The use or disclosure is reasonably necessary for establishing, exercising or defending legal claims.

---

[85]Australian Privacy Principle 5.1,
[86]Australian Privacy Principle 5.2, lists the nine matters that must be notified.
[87]Cf; Rule 33 of the ASCR
[88]Australian Privacy Principle 6.1,
[89]Australian Privacy Principle 6.2, The permitted situations include: consent; required or authorised by Australian law; enforcement related purpose; necessary to lessen or prevent serious threat; and reasonably necessary for legal proceedings.

Example: Use and Disclosure in Legal Practice

Scenario: A firm collects a client's financial information for a property transaction (primary purpose). The firm then wants to use that information to send the client marketing about the firm's estate planning services.

Analysis: Marketing is a secondary purpose. Would the client reasonably expect their financial details to be used for marketing? Likely not. Unless consent is obtained, this use would breach APP 6. Better practice: Seek separate consent for marketing. In addition to the Privacy Act obligations a professional relationship can be undermined by an overly commercial approach.

8.5. APP 11: Security of Personal Information

APP 11 requires entities to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.[90] This is one of the most important APPs for law firms given the sensitivity of legal information and one of the most difficult.

What are 'reasonable steps'?

The OAIC's Guide to Securing Personal Information provides some guidance on what reasonable steps might include.[91] Key security measures include:

- **Governance:** Clear responsibility for information security; policies and procedures; regular review.
- **Technical measures:** Access controls; strong passwords and MFA; encryption; secure networks; updated software; malware protection.
- **Physical measures:** Secure premises; locked storage; clear desk policies; secure disposal.
- **Personnel measures:** Staff training; confidentiality agreements; access based on role; offboarding procedures.
-

QLS suggests that serious consideration be given to obtaining a cybersecurity certification (likely silver-level 2 or gold tier-level 3) for your firm using the SMB-1001 certification system.

This is a highly cost-effective set of control measures designed for smaller organizations which take cybersecurity seriously but can't afford to spend tens of thousands of dollars hiring consultants to design a bespoke plan for them. Certification is available at a reduced rate to QLS members.

SMB certification **does not:**

- **provide safe harbour** from regulatory action if a breach occurs; or
- satisfy all your cybersecurity requirements (from stakeholders such as PEXA/ARNECC, the Family Court, your PII insurer)

but it does provide an excellent starting point which can be built on later.

Destruction and de-identification

APP 11.2 requires that personal information be destroyed or de-identified once it is no longer needed for any purpose for which it may be used or disclosed under the APPs.[92] However, this obligation does not apply where the information is contained in a Commonwealth record or where retention is *required* by law.

For law firms, information must generally be retained for ***at least*** seven years under AML/CTF requirements (for designated services records), and legal profession requirements impose similar retention periods for trust account records. The Data Retention Schedule (Document 04) provides

[90] Australian Privacy Principle 11.1.
[91] OAIC, *Guide to securing personal information* (June 2025), Part A (Understanding reasonable steps).
[92] Australian Privacy Principle 11.2.

guidance on retention periods. Your specific policy should be informed by the QLS Client Document retention guide[93] and own risk assessment.

[93] qls.com.au/content-collections/guides/document-retention-guide

8.6. APPs 12-13: Access and Correction

APPs 12 and 13 give individuals rights to access personal information held about them and to request correction of inaccurate information. These APPs create obligations that do not exist under professional confidentiality rules but sit side-by-side with them.

APP 12: Access

On request, an entity must give an individual access to personal information it holds about them.[94] Note, this is NOT restricted to clients. Access must be provided within a reasonable period (the OAIC suggests 30 days as a benchmark) and in the manner requested by the individual if reasonable and practicable.

Exceptions to the access requirement are set out in APP 12.3. Exceptions most relevant to law firms include:[95]

- giving access would reveal information to which legal professional privilege applies;
- giving access would prejudice one or more enforcement related activities conducted by an enforcement body;
- giving access would have an unreasonable impact on the privacy of others;
- the information relates to existing or anticipated legal proceedings and would not be accessible through discovery.

A Privacy Act request needs a Privacy Act response

If you are going to refuse an access request (say, if an opposing client in a family law matter is attempting to weaponize the legislation) it is important that the refusal is framed in terms of the privacy legislation, not just our standard duty of confidentiality.

For example, if a general access request were made the first basis for refusal might be that as your firm is a Small Business, only the personal information collected for AML/CTF purposes is regulated and subject to the Access-Correction regime.

In many cases a further ground for refusal would be on the "anticipated legal proceedings" ground rather than the instinctive position that it is part of our client file and therefore confidential.

Note that where the access request comes from a client/former client, elements of the file are the client's property[96] and subject to specific access rights under the ASCR[97]. The client's entitlement to access therefore comes from all three sources: the Privacy Act, the ASCR and the common law ownership rules.

APP 13: Correction

An entity must take reasonable steps to correct personal information it holds to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.[98]

For the most part, solicitor's standard practices should address this. If an active file, our usual risk-management will ensure that pertinent information is kept up to date. Material held for retention and archiving purposes would not require active updating (except, perhaps, client contact details.)

Again, there is potential for weaponization if an opposing party seeks to demand that information held about them (their business' turnover, for example) is "misleading" and they want you to substitute different data.

If an entity refuses to correct information as requested, it must give written notice of the refusal (including reasons and complaint mechanisms), and on request, associate a statement with the

[94] Australian Privacy Principle 12.1.
[95] Australian Privacy Principle 12.3, sets out the exceptions permitting refusal of access.
[96] *Wentworth v De Montfort* (1988) 15 NSWLR 348
[97] For more information see: QLS Guidance statement No.30 Transfer of files - Queensland Law Society; and Who owns file notes? – Proctor
[98] Australian Privacy Principle 13.1.

information stating that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading.[99]

[99]Australian Privacy Principle 13.2.

Chapter 9: Integrating Privacy and AML/CTF Compliance

The AML/CTF Tranche 2 reforms and privacy compliance are intimately connected. This chapter explains how the two regulatory regimes interact and how to build a compliance framework that satisfies both sets of obligations efficiently.

9.1. The AML/CTF Trigger for Privacy Obligations

As explained in Chapter 2, the Privacy Act generally exempts small businesses (under $3 million annual turnover) from APP compliance. However, a business that is a 'reporting entity' under the AML/CTF Act is taken to be an 'organisation' for Privacy Act purposes, regardless of its turnover.[100] The Privacy Act applies to information collected for or in connection with AML/CTF purposes.

The OAIC has prepared an overview of privacy for AML entities.[101]

For the most part, the provision of legal advice (even about matters that would otherwise be designated services) and representation in courts or tribunals are *not* designated services.

9.2. The Privacy/AML/CTF Information Lifecycle

What is collected and how is it used?

AML/CTF compliance requires collecting, using, disclosing, and retaining personal information. Each stage involves both AML/CTF and privacy obligations:

Stage	AML/CTF Requirement	Privacy Requirement
Collection	Collect identity information and verify identity before providing designated services (customer due diligence)	APP 3: Collect only what is reasonably necessary; APP 5: Notify individual of collection, purposes, disclosures
Use	Use information to verify identity, assess transaction risk, monitor for suspicious activity	APP 6: Use for primary purpose (AML/CTF compliance); secondary use only with exception
Disclosure	Report suspicious matters to AUSTRAC; respond to compulsory notices	APP 6: Disclosure required by law is authorised; cannot 'tip off' client about SMR
Storage	Keep records secure and accessible for compliance purposes	APP 11: Take reasonable steps to protect from misuse, loss, unauthorised access
Retention	Retain records for 7 years after relationship ends or transaction completes	APP 11.2: Destroy when no longer needed , but AML/CTF or other statutory retention requirement overrides
Destruction	May destroy after 7-year retention period (unless other requirements)	APP 11.2: Destroy securely when no longer needed for any permitted purpose

[100]Privacy Act 1988 (Cth), s 6C(1), item 2 of the table. A business that is a reporting entity under the AML/CTF Act is taken to be an organisation for the purposes of the Privacy Act.
[101]https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/privacy-guidance-for-reporting-entities-under-the-anti-money-laundering-and-counter-terrorism-financing-act

9.3. Customer Due Diligence and Privacy

Customer due diligence (CDD) is the process of identifying and verifying the identity of customers and ultimate beneficial owners before providing designated services.[102] CDD involves verifying identity although it is not restricted to that.[103] It will usually involve collecting personal information including name, date of birth, and address, and verifying that information using reliable documents (such as driver's licence or passport) or electronic verification.[104]

Privacy compliance during CDD

When conducting CDD, the following privacy requirements apply:

Collection is authorised: Collection of identity information for CDD purposes is required by the AML/CTF Act. This means collection is 'required or authorised by or under an Australian law', which satisfies APP 3.4.[105]

Notification is required: APP 5 still requires notification of collection. The collection notice must explain that collection is required by law, the law requiring it (AML/CTF Act), and the purposes of collection. The Collection Notice Template for Designated Services (Document 02, Template B) addresses this.

Sensitive information may be collected: CDD may require collecting sensitive information, such as information about politically exposed person status. Where collection is *required* by law, consent is not required, but the collection notice should explain that sensitive information is being collected.[106]

Anonymity exception applies: APP 2 generally requires entities to give individuals the option of anonymity or pseudonymity.[107] However, this does not apply where the entity is required by law to deal with identified individuals[108] — as is the case for CDD.

9.4. Beneficial Ownership Information

For corporate and trust clients AML/CTF compliance requires identifying beneficial owners, the individuals who ultimately own or control the entity. This involves collecting personal information about people who may not be the direct client of the firm.

Privacy obligations to beneficial owners

Beneficial owners are individuals about whom personal information is collected. They have privacy rights even though they may not be the firm's direct client. Key obligations include:

Notification: APP 5 requires notification of collection. Where information is collected from a third party (such as from company records or the direct client), the notice must explain that fact. The Collection Notice Template for Beneficial Owners (Document 02, Template D) addresses this.

Access rights: Beneficial owners have rights under APP 12 to request access to personal information the firm holds about them

Correction rights: Beneficial owners have rights under APP 13 to request correction of inaccurate information.

Practically, this means the firm should ensure that beneficial owners receive a collection notice (which can be provided via the corporate client) and are aware they can contact the firm regarding their personal information - subject to the exceptions set out in Chapter 8 (commentary on APP 12 and 13)

---

[102]Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), Part 2 (Customer identification procedures), as amended by the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024 (Cth).
[103]For detailed information concerning CDD processes and oboarding information see here: Legal profession program starter kit: Document library | AUSTRAC
[104]AUSTRAC, Customer identification: Know your customer (KYC) (Reform guidance).
[105]Australian Privacy Principle 3.3(a), (collection of sensitive information with consent); APP 3.4(a) (collection required or authorised by Australian law).
[106]OAIC, Chapter 3: APP 3 — Collection of solicited personal information, APP Guidelines (October 2025), [3.35]-[3.40].
[107]Australian Privacy Principle 2.1 (anonymity and pseudonymity option).
[108]Australian Privacy Principle 2.2(b)(exception where required or authorised by Australian law).

9.5. Suspicious Matter Reporting and Confidentiality

The AML/CTF Act requires reporting entities to report suspicious matters to AUSTRAC. Importantly, the Act also prohibits 'tipping off', informing anyone that a report has been or may be made.[109] A full analysis of the interaction between SMR reporting and confidentiality/privilege is beyond the scope of this guide.

Reporting client information without telling them creates an apparent tension with both professional confidentiality and privacy obligations. However, the legal framework provides authorisation:

Privacy: APP 6.2(b) permits disclosure that is 'required or authorised by or under an Australian law'. Suspicious matter reporting is required by the AML/CTF Act, so disclosure to AUSTRAC is authorised under the APPs.[110]

Confidentiality: ASCR Rule 9.2.1 permits disclosure where the solicitor is 'compelled by law to disclose'. Suspicious matter reporting is required by law, so disclosure is permitted under the confidentiality rules.[111] Most Law Societies / Institutes have concluded that having submitted an SMR it would be inappropriate to continue to act for a client, although terminating the retainer without telling the client why is not easy.

The SMR provision preserves legal professional privilege, so only some information can be disclosed to authorities. [112]

Critical: Tipping Off Prohibition

The tipping off prohibition is strict. Do not inform the client (or anyone else other than a confidential advisor such as the QLS Ethics Centre) that you have made, or are considering making, a suspicious matter report.

Do not include any reference to suspicious matter reports in client communications, file notes that might be disclosed, or privacy-related notifications.

Ensure your record keeping processes ensure that discussions and file notes concerning the decision to make an SMR are not captured on the client file or are billed to the client.

If a client makes an access request under APP 12 for their personal information, the firm may refuse to disclose information to the extent that disclosure would reveal the existence of a suspicious matter report. – although of course the response could not specify that.

9.6. Record Retention: Aligning Requirements

The AML/CTF Act requires reporting entities to retain CDD records and transaction records for seven years after the end of the customer relationship or the transaction, whichever is later.[113] This retention requirement overrides the general APP 11.2 obligation to destroy information when no longer needed.

OAIC Guidance[114] suggests that full copies of driver's licenses & passports NOT be retained. In contrast, ARNECC's Safe Harbour VOI regime requires retention of imaged copies.[115] This contradiction is unsatisfactory and the QLS and Law Council of Australia have requested that urgent attention be given to harmonizing these obligations.

The Data Retention Schedule (Document 04) aligns AML/CTF, Privacy Act, Legal Profession Act, and other retention requirements into a single framework. Key points:

- CDD/KYC records: 7 years after relationship ends (AML/CTF Act)
- Transaction records: 7 years after transaction (AML/CTF Act)

---

[109] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), s 41 (reports to AUSTRAC) and s 123 (tipping off prohibition).
[110] Australian Privacy Principle 6.2(b), (use or disclosure required or authorised by or under an Australian law).
[111] Australian Solicitors' Conduct Rules 2012 (Qld), r 9.2.1 (disclosure compelled by law).
[112] See: 20251211_Ethics Guideline_Balancing_LPP_and_AML_Final (Law Institute Victoria).pdf
[113] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), s 107 (7-year record retention requirement).
[114] Privacy guidance for reporting entities under the Anti-Money Laundering and Counter-Terrorism Financing Act | OAIC
[115] MPR Version 6 Guidance Note #2: Verification of Identity; ARNECC Model Participation Rules Guidance Notes #5 (retention of evidence).

- Trust account records: 7 years (Legal Profession Act)
- Client files generally: 7 years recommended (longer – potentially much longer - for certain matters)
- Safe custody: potentially indefinite, subject to specific retention mandates and the Legal Profession Act (Qld)

After the applicable retention period, information should be securely destroyed in accordance with APP 11.2 and your retainer.

Note that components of the file which are the client's property cannot be destroyed without Client's consent or the procedure in S. 713A of the Legal Profession Act (Qld) followed.[116]

Key Takeaways — Chapters 7, 8 and 9

- The 13 APPs govern the complete lifecycle of personal information: governance, collection, use/disclosure, quality/security, and individual rights.
- 'Reasonable steps' is a flexible standard — what is reasonable depends on the circumstances, including the sensitivity of information held.
- APP 1 (privacy policy), APP 3 (collection limits), APP 5 (notification), APP 6 (use/disclosure), APP 11 (security), and APPs 12-13 (access/correction) are most significant for law firms.
- AML/CTF obligations and privacy obligations operate concurrently — compliance with one does not excuse non-compliance with the other.
- CDD collection is authorised by law, but notification to individuals (APP 5) is still required.
- Suspicious matter reporting is authorised under both privacy and confidentiality frameworks; the tipping off prohibition must be observed strictly.

[116] LEGAL PROFESSION ACT 2007 - SECT 713A Destruction of client documents – note that this provision is specific to Queensland, arising – in part – from the different legislative mechanisms by which they are created in this state as compared to the Uniform Law jurisdictions.

PART D

BUILDING YOUR COMPLIANCE FRAMEWORK

Chapter 10: Your Privacy Policy

The privacy policy is the public face of your privacy compliance program.

APP 1 requires every APP entity to have a clearly expressed and up-to-date privacy policy that explains how it manages personal information.[117] This chapter explains how to develop and maintain your privacy policy using Document 01: Privacy Policy Template.

10.1. Purpose and mandatory elements

The privacy policy serves two key functions: it informs individuals about how you handle their personal information, and it informs internal procedures. The policy must be made available free of charge in an appropriate form. For most law firms, this means publishing it on your website. Drafting hint: don't conflate information better contained in a Retainer Agreement.

APP 1.4 specifies six mandatory content requirements for privacy policies:[118]

#	Required Content (APP 1.4)
(a)	Kinds of personal information collected and held
(b)	How personal information is collected and held
(c)	Purposes of collection, holding, use and disclosure
(d)	How to access personal information and seek correction
(e)	How to complain and how complaints will be handled
(f)	Likely overseas disclosures and countries involved

From 10 December 2026, an additional requirement will apply: if the entity uses substantially automated systems to make decisions that could significantly affect individuals' rights or interests, this must be disclosed in the privacy policy.[119]

[117] Australian Privacy Principle 1.3,
[118] Australian Privacy Principle 1.4,
[119] *Privacy and Other Legislation Amendment Act 2024* (Cth), Schedule 1, item 17, inserting new APP 1.4(fa), commencing 10 December 2026.

10.2. Using the Privacy Policy Template

Document 01: Privacy Policy Template provides a privacy policy drafted specifically for small law firms providing designated services. Drafting notes are contained in blue boxes. These should be deleted prior to publication. To customise the template for your firm:

Step 1: Insert firm details

Replace all placeholders marked with [square brackets] throughout the document. Key placeholders include:

- [Firm Name] — your firm's legal name
- [Address] — your principal place of business
- [Phone] — your main contact number
- [Email] — your main contact email (or dedicated privacy email): consider concealing that so that it can't be harvested by spam-bots.
- [Privacy Officer name/position] — the designated privacy contact
- [Website URL] — your firm's website address

Step 2: Review and adjust content

The template includes content relevant to most small law firms providing designated services. However, the Privacy Policy must be a living document. It must reflect actual practice and be the starting point for how your firm actually deals with regulated information.

It must be drafted with clarity in mind. For that reason it is "layered", with the initial paragraph containing a simple overview with room for more specifics below. Ideally, it is published (on the website) in a format where the reader primarily sees the simple content but has the ability to expand for more detail if they want it.

Review each section to ensure it accurately reflects your firm's practices:

- **Types of information:** Confirm the categories of personal information listed are those your firm actually collects.
- **Disclosure recipients:** Review the list of typical disclosure recipients. Add categories relevant to your practice (e.g., specific regulators, experts you commonly engage – by category not name).
- **Overseas disclosure:** If your firm uses cloud services with data processed or stored overseas, a virtual assistant hosted offshore or routinely corresponds with overseas parties identify the relevant countries.

The template provided contains a basic description under each compulsory heading with expansion fields that can be used to give more detail or lists of relevant information collected. This design is intended to improve readability by providing essential information as default with the opportunity to read further if desired.

10.3. Publication and Accessibility

Once finalised, your privacy policy must be made available in an appropriate form, free of charge.[120] The OAIC recommends:[121]

- Publish the full policy on your website, with a clear link from the homepage;
- Make a copy available at your office for anyone who requests it;
- Be prepared to provide the policy in alternative formats (e.g., large print) if requested;
- Reference the policy in engagement letters and collection notices.

[120]OAIC, *Guide to developing an APP privacy policy* (September 2024), Part 3: Making your APP privacy policy available.
[121]Australian Privacy Principle 1.5, (policy must be available free of charge and in appropriate form).

10.4. Keeping the Policy Current

The privacy policy must be 'up to date'. This requires periodic review and updating whenever there are material changes to your information handling practices.[122]

Events that might trigger a policy review include:

- Changes to the types of personal information collected;
- Changes to the purposes for which information is used;
- Engagement of new service providers who will access personal information;
- Changes to overseas disclosure practices (new countries, new service providers);
- Introduction of new technologies (AI tools, new software systems);
- Changes to privacy legislation or OAIC guidance;
- Annual review (as a minimum).

Practical Tip: Version Control

Include a version number and date on your privacy policy (the template includes a placeholder for this). When you update the policy, increment the version number and update the date. Keep a copy of superseded versions for your records — they may be relevant if a complaint is made about historical practices.

[122]OAIC, *Chapter 1: APP 1 — Open and transparent management of personal information*, APP Guidelines (October 2025), [1.50]-[1.55] (keeping the policy up to date).

Chapter 11: Collection Notices

While the privacy policy provides general information about your firm's privacy practices, collection notices provide specific information to individuals at the point of collection. APP 5 requires notification at or before the time personal information is collected, or as soon as practicable afterwards.[123] This chapter explains how to use the collection notice template in Document 02.

The template also explains the background of the AML regime and why your firm is required to collect the information you are requesting.

11.1. When Collection Notices Are Required

Collection notices are required whenever you collect personal information, unless the individual has already been made aware of the relevant matters. The trigger is collection, not the commencement of a formal retainer.

Given that many firms will conduct Client Due Diligence prior to costs disclosure and formal acceptance of the client and matter a separate notice may be required rather than leaving it to the retainers.

We may also need to give Collection notices if information is obtained from / about parties who are not clients.

For law firms, collection typically occurs when:

- A new client provides their details (initial enquiry or engagement);
- Identity documents are collected for AML/CTF purposes;
- Information about third parties (beneficial owners, witnesses, other parties) is collected;
- Someone completes a contact form on your website;
- Employee or job applicant information is collected. (Only some applicant information is regulated, typically that collected for staff due diligence and background checks.)

[123] Australian Privacy Principle 5.1.

11.2. Required Content of Collection Notices

APP 5.2 specifies nine matters that must be notified at or before the time of collection:[124]

Required Matter (APP 5.2)	What This Means for Law Firms
(a) Entity's identity and contact details	Your firm's name, address, and contact information
(b) Collection from third party: fact and circumstances	If information is obtained from someone other than the individual (e.g., beneficial owner info from company director), explain this
(c) Collection required by law: the law and fact of requirement	For AML/CTF collection, identify the AML/CTF Act as requiring the collection
(d) Purposes of collection	Explain why you are collecting the information (legal services, AML/CTF compliance, etc.)
(e) Consequences if not collected	Explain what happens if information is not provided (e.g., cannot provide services, cannot proceed with transaction)
(f) Usual disclosure recipients	Categories of third parties who typically receive the information (courts, regulators, other parties, etc.)
(g) Privacy policy contains access/correction information	Direct individuals to your privacy policy for information about access and correction rights
(h) Privacy policy contains complaints information	Direct individuals to your privacy policy for information about making complaints
(i) Overseas disclosure: countries if known	If information may be disclosed overseas, identify the countries (or state that countries are not known)

11.3. Using the Collection Notice Template

The OAIC has a generic Collection Notice available: Template privacy collection notice for reporting entities under the Anti-Money Laundering and Counter-Terrorism Financing Act | OAIC

QLS has adapted a version of this in the form of a client focused brochure. It also provides more context for clients why your firm is collecting certain information. (Document 2)

11.4. Timing and Delivery

Collection notices should be provided *at or before* the time of collection, or as soon as practicable afterwards.[125]

Practical delivery methods include:

- Include in first letter
- Include in engagement letter/costs agreement
- Provide with identity document request
- Display on website forms;
- Send by email when requesting

[124]Australian Privacy Principle 5.2, lists the nine matters that must be notified.
[125]OAIC, *Chapter 5: APP 5 — Notification of the collection of personal information*, APP Guidelines (October 2025), [5.1]-[5.5] (timing of notification).

- Provide to corporate client for distribution to beneficial owners

Chapter 12: Information Management

Effective privacy compliance requires knowing what personal information you hold, where it is stored, how long it must be retained, and when it should be destroyed. This chapter explains how to use Document 03 (Personal Information Inventory) and Document 04 (Data Retention Schedule) to establish systematic information management.

12.1. Personal Information Inventory (Document 03)

A personal information inventory is a register of the categories of personal information your firm holds, including where it is stored, how it is collected, and who has access to it. While not explicitly required by the APPs, maintaining an inventory is recognised by the OAIC as a foundational element of good privacy management.[126]

Why maintain an inventory?

An inventory improves protection and – in the longer term – minimizes cost. It ensures that you don't have multiple copies and sources of data breach in existence, and that you can focus protection effectively on where it is needed most.

Organizing your archive storage to quickly and easily manage destruction will also save a lot of work and expense in the longer term. While we tend to think of electronic storage as essentially free it is not once you factor in the cost of sorting through it prior to destruction.

Using the inventory template

The more complete this audit is, the better your overall outcome. However, for the purposes of initial compliance a general overview of what you hold, where and why and where you hold it may be sufficient.

Document 03 provides a template with the following columns:

Column	Description
Information Category	Type of personal information (e.g., 'Client identity documents', 'Beneficial owner information', 'Staff records')
Data Elements	Specific data items within the category (e.g., name, DOB, address, passport number)
Source	How information is collected (e.g., directly from client, from company searches, from third parties)
Storage Location	Where information is stored (e.g., practice management system, physical files, cloud storage)
Access	Who has access to this information (e.g., all staff, principals only, specific staff members)
Retention Period	How long information is retained (cross-reference to retention schedule)
Sensitivity	Whether the category includes particularly sensitive information (health, criminal record, etc.) If information is especially sensitive – both in the sense

[126]OAIC, Privacy management framework: enabling compliance and encouraging good practice (May 2025), Step 2: Establish a personal information inventory.

	that it falls within the Privacy Act definition or you anticipate especial risk of harm - this should be flagged for special protection in motion and at rest.
Overseas Disclosure	Whether information is disclosed overseas (and to which countries)

The template includes pre-populated entries for common categories of personal information held by law firms. These are only examples, not intended as a comprehensive list.

Review and adjust these entries to reflect your firm's actual information holdings.

12.2. Data Retention Schedule (Document 04)

APP 11.2 requires that personal information be destroyed or de-identified when it is no longer needed for any purpose for which it may be "used or disclosed under the APPs".[127]

Retention for risk management or to assist in the administration of justice can be justify the decision to keep information beyond the minimum period. You should consider the kinds of work you do and decide how long specific files will be kept and be prepared to defend the decision if called upon to do so.

It is much cheaper to store physical files with a specific destruction period together. This permits the entire box to be destroyed simultaneously rather than record-by-record. A destruction certificate should be requested if available. If being destroyed in-house keep a record of what was destroyed, by whom and by what method.

Key retention requirements for law firms

The seven-year period for AML/CTF designated service records[128] aligns with the trust account retention requirement under the Legal Profession Act[129] and general file retention obligation under the ASCR.

Note that a **separate retention requirement** relating to Client Due Diligence records exists. While it is also seven years, the start date for the time clock is the end of the relationship, not the date the file is closed.[130]

[127]Australian Privacy Principle 11. See: Chapter 11: Australian Privacy Principle 11 — Security of personal information paragraphs 11.29 et seq.
[128]Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), s 107 (7-year record retention requirement).
[129]Legal Profession Act 2007 (Qld), s 261(2)(d) (retention of trust records) and Legal Profession Regulation 2017 (Qld), Reg 59 2(a) (See also s 44(3)(d)) – from finalisation of the matter.
[130]Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), s 111

Minimum vs prudent retention periods.

The general recommendation of seven years for client files reflects the six-year limitation period for most civil claims[131] plus a buffer.

Longer retention is appropriate for some types of matters, although only certain elements of the file might be relevant for long term storage.[132]

Record Type	Minimum Period	Source
AML/CTF CDD records (Also e-conveyancing VOI Data)	7 years after **relationship ends (*)**	AML/CTF Act s 111 ARNECC MPR 2 – VOI
Designated service transaction records	7 years after transaction	AML/CTF Act s 107, 108
Trust account records	7 years	Legal Profession Act 2007 (Qld)
General client files	7 years mandatory	ASCR
Wills and estate planning	For as long as the will may be valid, plus additional time if a subsequent will is disputed	Not all of the file required – client instructions & testamentary capacity evidence is especially important.
Special files, such as establishing Trusts, acting for children, criminal files where long term imprisonment is the outcome	Various	See QLS Guidance.
Employment/HR records	7 years after employment ends	Various employment legislation

Client Due Diligence records – when does the clock start to run?

S.111 of the AML/CTF act requires retention for 7 years after the "business relationship ends" or the firm "completes the provision of the occasional transaction".

This not necessarily the same as "matter closing".

Where you reasonably expect the client to provide ongoing instructions the relevant destruction date is 7 years after the final designated service you provide for them. This is difficult given that you may have no real way of knowing whether the client will return or not.

[131]Limitation of Actions Act 1974 (Qld), ss 10, 10A (6-year limitation period for contract and tort claims); s 11 (12-year limitation period for claims on deeds).
[132]Queensland Law Society, qls.com.au/content-collections/guides/document-retention-guide

Using the retention schedule

Document 04 provides a comprehensive retention schedule that integrates AML/CTF, Legal Profession Act, limitation period, and privacy requirements. For each record category, the schedule specifies:

- The minimum retention period;
- The trigger date (e.g., matter completion, relationship end);
- The legal basis for the retention period;
- Action required after the retention period (destroy, review, archive).

12.3. Secure Destruction

When the retention period expires and there is no other reason to retain the information, it should be destroyed securely.[133] Secure destruction means ensuring that information cannot be recovered or reconstructed.

Methods for secure destruction include:

- **Physical documents:** Cross-cut shredding (strip shredding is not sufficient for confidential documents) or secure destruction service with certificate of destruction.
- **Electronic files:** Secure deletion using appropriate software (simple deletion does not remove data); for highly sensitive data, overwriting or physical destruction of storage media.
- **Cloud/hosted data:** Request deletion from service provider and obtain confirmation; understand the provider's data deletion practices.

Maintain a destruction register recording what was destroyed, when, and how. This provides evidence of compliance with APP 11.2 and may be relevant if questions arise about historical information holdings.

If an original was in hard-copy format a destruction record may be important for ensuring admissibility of any electronic copy.

12.4. Data Quality

APP 10 requires entities to take reasonable steps to ensure that personal information collected is accurate, up-to-date, complete and relevant, having regard to the *purpose of use or disclosure*.[134] If your purpose is to record a transaction, it is not necessary to update personal contact details, although that can be very helpful when seeking to communicate with clients about proposed destruction of historical records.

[133]OAIC, *Guide to securing personal information* (June 2025), Part F: Destruction and de-identification.
[134]Australian Privacy Principle 10.1.

12.5. Cross-Border Considerations

APP 8 imposes requirements before disclosing personal information to overseas recipients.[135] The most common ways overseas disclosure takes place for law firms are:

- Cloud services with overseas data storage (practice management systems, email, document storage);
- Correspondence with overseas parties or lawyers in cross-border matters;
- Electronic identity verification services that access overseas databases.

Ideally, cross-border transmission, processing or dissemination of information should be avoided. Careful consideration of software provider's terms of service are an important risk control measure.

Before disclosing personal information overseas, the firm must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.[136] If disclosure occurs and the overseas recipient breaches the APPs, the disclosing entity is accountable as if it had committed the breach itself.[137]

Key Takeaways — Chapters 10, 11 and 12

- Your privacy policy must address six mandatory matters under APP 1.4; use Document 01 template and customise for your firm.
- Collection notices are required at or before the time of collection; use the five templates in Document 02 for different collection scenarios.
- The personal information inventory (Document 03) helps you know what you hold and where — essential for security, access requests, and breach response.
- The retention schedule (Document 04) integrates AML/CTF, Legal Profession Act, and limitation period requirements — generally 7 years for most records.
- Destroy information securely when no longer needed; maintain a destruction register.
- Before disclosing overseas, take reasonable steps to ensure the recipient will handle information in accordance with the APPs.

[135] Australian Privacy Principle 8.1.
[136] OAIC, Chapter 8: APP 8 — Cross-border disclosure of personal information, APP Guidelines (October 2025), [8.1]-[8.10].
[137] Privacy Act 1988 (Cth), s 16C (accountability for acts of overseas recipients).

Chapter 13: Implementation Roadmap

Privacy compliance is not achieved overnight. It requires a systematic approach to developing documentation, implementing procedures, training staff, and embedding privacy into firm culture. This chapter provides a roadmap for implementation, designed to ensure your firm is compliant before privacy obligations commence on 1 July 2026.[138]

13.1. Phased Implementation Timeline Overview

If your firm has not spent a lot of time on cybersecurity previously more resources might be needed than currently mapped out in phase 3.

Phase	Timeframe	Key Activities
Phase 1: Foundation	Week 1	• Designate Privacy Officer • Complete gap assessment (Chapter 6) • Map designated services and the records that might be generated • Review this manual • Brief principals and key staff
Phase 2: Documentation	Week 2	• Customise privacy policy (Doc 01) • Customise collection notice(s) (Doc 02) • Complete PI inventory (Doc 03) – set aside a bit more time for this • Finalise retention schedule (Doc 04) • Develop breach response plan (Doc 05) • Conduct threshold PIA (Doc 06)
Phase 3: Implementation	Weeks 3	• Publish privacy policy on website • Update engagement letter templates • Implement security measures • Train all staff (Doc 07) • Update website forms
Phase 4: Readiness	Week 4	• Final review of all documentation • Address any gaps identified • Confirm staff understand procedures • Principal sign-off on readiness

13.2. Phase 1: Foundation

Designate a Privacy Officer

Identify the individual who will be responsible for privacy compliance.[139] In a small firm, this is typically a Principal. The Privacy Officer should have authority to make decisions about privacy matters and allocate resources to compliance activities. Document this appointment.

Complete the gap assessment

Using the checklists in Chapter 6, assess your firm's current practices against privacy requirements. This identifies what you already have in place and where work is needed. The results inform the prioritisation of Phase 2 activities.

Map designated services

Review Chapter 9.1 and determine which of your firm's services are 'designated services' under the AML/CTF Act. This confirms the scope of your AML/CTF obligations and consequently your privacy obligations. Consider what “personal information” will be collected for AML purposes.

---

[138]Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024 (Cth), Schedule 1, commencing 1 July 2026.
[139]OAIC, Privacy management framework: enabling compliance and encouraging good practice (May 2025), Step 1: Embed a culture of privacy.

13.3. Phase 2: Documentation

The documentation phase involves customising and finalising the core compliance documents.[140] Work through each toolkit document systematically:

Document	Key Actions
Doc 03: PI Inventory	Map all personal information holdings; identify storage locations, access, sensitivity
Doc 04: Retention Schedule	Review retention requirements; map to information categories; document trigger dates
Doc 01: Privacy Policy	Customise template; review for accuracy; obtain principal approval
Doc 02: Collection Notices	Customise all five templates; integrate with engagement processes
Doc 05: Breach Response Plan	Customise plan; identify response team; document contact lists
Doc 06: PIA Framework	Complete threshold assessment; identify high-risk processes; plan any full PIAs
Doc 07: Training Framework	Develop training content; schedule training sessions; prepare materials

13.4. Phase 3: Implementation

The implementation phase puts your documentation into practice.[141] Key activities:

- **Publish privacy policy:** Upload to website with clear link from homepage (typically footer). Consider a launch communication to existing clients.
- **Update templates:** Integrate collection notices into engagement letter templates, costs agreements, and other client-facing documents.

Implement security measures: Address any cybersecurity security gaps

[140] Australian Privacy Principle 1.2.
[141] OAIC, *Privacy management framework* (May 2025), Step 3: Develop internal handling practices.

identified; document security practices. (Assumes that a cybersecurity program is already established. If not, start planning earlier as it might take more time than expected – see PART E

- Security Measures)
- **Train all staff:** Conduct training sessions using the framework in Document 07. Record attendance.

13.5. Phase 4: Readiness

By the end of Phase 4, you should be able to confirm:

- ☐ Privacy policy published and accessible
- ☐ Collection notice integrated into client engagement processes
- ☐ Personal information inventory complete and current
- ☐ Retention schedule documented and communicated
- ☐ Breach response plan in place with trained response team
- ☐ Security measures documented and implemented
- ☐ All staff trained on privacy obligations
- ☐ Procedures for handling access/correction requests documented

PART E

OPERATIONALISING PRIVACY

Chapter 14: Security Measures

APP 11 (and our general professional duty of competence) requires entities to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.[142] This chapter outlines key security measures that contribute to APP 11 compliance.

14.1. The 'Reasonable Steps' Standard for Security

What constitutes 'reasonable steps' for security depends on the circumstances, including the nature and amount of information held, the possible consequences of a breach, and the practicability of implementing security measures having regard to firm size and resources.[143]

For law firms, the sensitivity of legal information and value of identity documents, financial details, and confidential client communications to criminals warrants robust security.

14.2. Governance and Accountability

Effective security begins with clear governance.[144] Key elements include:

- **Designated responsibility:** A specific person should have responsibility for overseeing security measures. This is a management function, not an IT function although someone with both skill sets is ideal.
- **Documented policies:** Security practices should be documented so staff understand their obligations. Even in small firms, simple infographics and checklists are important.
- **Regular review:** Security measures should be reviewed periodically (at least annually) and when significant changes occur.
- **Training:** there is no point having policies and technical measures to protect data if nobody knows what they are or how to use them. Staff must be trained on induction and regularly reminded how to keep the firm safe.
- **Incident reporting culture:** Staff should be encouraged to report security incidents and near-misses without fear of blame.

[142]Australian Privacy Principle 11.1, ASCR R 4.1
[143]OAIC, *Guide to securing personal information* (June 2025), Part A: Understanding reasonable steps to protect personal information.
[144]OAIC, *Guide to securing personal information* (June 2025), Part C: Governance — establish clear responsibility.

14.3. Technical Security Measures

Technical measures protect against cyber threats and unauthorised access.

The Australian Cyber Security Centre's Essential Eight provides a useful baseline framework for mid-tier practices, but smaller firms may struggle with some of the technical steps and the resources required to implement them.[145]

Key QLS recommendations may be found here Cybersecurity - Queensland Law Society, with more information from the ACSC website:[146]

Measure	Implementation Guidance
Access controls	Unique user accounts for each staff member; access based on role (principle of least privilege); disable accounts promptly when staff leave
Strong authentication	Complex passwords (12+ characters); multi-factor authentication (MFA) for remote access and sensitive systems; password manager recommended See QLS resources[147] on password selection. Note that other authentication technologies (eg, pass-keys loaded onto secure devices, Single Sign On systems, biometrics) may be more secure and convenient that passwords. However, most firm networks will still retain passwords as secondary access options or for devices such as printers and routers, so they must be secure and used appropriately.
Encryption	Encrypt sensitive data in transit (TLS/HTTPS); consider additional encryption at rest for highly sensitive information; encrypted email for sensitive attachments
Network security	Firewall protection; secure Wi-Fi (WPA3 or WPA2 with strong password); separate guest network; VPN for remote access
Software updates	Enable automatic updates for operating systems and applications; patch critical vulnerabilities promptly; maintain supported software version. See QLS resources here: Basic cyber steps can block most attacks – Proctor
Malware protection	Antivirus/antimalware software on all devices; regular scans; email filtering for malicious attachments
Backup and recovery	Regular backups (at least daily for critical data); offsite or cloud backup; test restoration periodically; maintain offline backup copy

[145]Australian Cyber Security Centre, *Essential Eight Maturity Model* (November 2023), available at <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight>.
[146]OAIC, *Guide to securing personal information* (June 2025), Part D: ICT security; See also Small business cyber security guide | Cyber.gov.au
[147](Password selection and use) : qls.com.au/content-collections/template/qls-password-protection-policy-template, (multi factor authentication) qls.com.au/content-collections/guides/multi-factor-authentication-guide

14.4. Physical Security Measures

Physical security protects against unauthorised physical access to information and systems.[148] Key measures include:

- **Premises security:** Locked premises; alarm system; visitor management (sign-in, escorting in sensitive areas).
- **Document security:** Lockable filing cabinets for sensitive files, fire / flood resistance for safe custody; clear desk policy; secure storage for identity documents. Archive files should not be stored in insecure sheds or under-house storage areas.
- **Device security:** Screen locks when unattended; secure laptop storage; mobile device management for firm devices.
- **Secure disposal:** Cross-cut shredding for confidential documents; secure destruction of storage media; secure disposal service with certificate.

14.5. Personnel Security Measures

People are both the greatest security asset and the greatest security risk. Personnel measures include:

- **Pre-employment checks:** Reference checks; verification of qualifications; consider police checks for roles with access to sensitive information. (See ARNECC model participation rules for mandatory pre-employment police & other checks)
- **Confidentiality agreements:** Employment contracts should include confidentiality and privacy obligations.
- **Training:** Regular security awareness training covering phishing, social engineering, password security, and incident reporting.
- **Offboarding:** Prompt access revocation when staff leave; return of firm devices and documents; exit reminders of ongoing confidentiality obligations.

[148]OAIC, *Guide to securing personal information* (June 2025), Part E: Physical security and personnel security.

Chapter 15: Breach Response

The Notifiable Data Breaches (NDB) scheme requires entities to notify the OAIC and affected individuals when an 'eligible data breach' occurs.[149]

Effective breach response requires preparation before a breach occurs. This chapter explains the NDB scheme and how to use Document 05: Data Breach Response Plan.

15.1. What is an Eligible Data Breach?

An eligible data breach occurs when:[150]

1. There is unauthorised access to, unauthorised disclosure of, or loss of personal information held by the entity; AND
2. A reasonable person would conclude that the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

'Serious harm' includes serious physical, psychological, emotional, financial, or reputational harm. Factors relevant to assessing serious harm include:

- the kind and sensitivity of the information (identity documents, financial information);
- whether the information is protected by security measures (encryption);
- the persons who have obtained or could obtain the information;
- whether the information could be used for identity fraud, financial fraud, or other harm.

The OAIC website has some useful decision trees and checklists to assist in this decision. One of the services available under the QLS Cyber Essentials cyber insurance policy is forensic analysis and expert advice to determine how serious a breach is and whether you have a notification obligation.

Remember: if your firm has a turnover below $3M, the NDB scheme only applies if information collected for AML / CTF purposes is suspected to have been lost – however, our fiduciary and ethical obligations will usually require modified disclosure to affected parties even if the NDB scheme does not.

Law Firm Context: Risk of Serious Harm

Given the sensitivity of information typically held by law firms — including identity documents, financial details, and confidential legal communications — many data breaches affecting client information are likely to meet the 'serious harm' threshold. Err on the side of treating breaches as notifiable unless clearly low-risk.

An example of a low-risk event: an email containing confidential client information is sent to another firm accidentally. The firm agrees to delete the information. You inform your client of the event but may reasonably conclude that no serious harm is likely.

An example of a high-risk event: a conveyancer's email account is compromised and attempts to divert funds were unsuccessful. On forensic analysis it appears that several months' worth of email have been copied. Despite the fact that the attacker's primary objective seems to be funds diversion, it is quite possible that confidential data will be sold. It is likely that this is an NDB event.

[149]Privacy Act 1988 (Cth), Part IIIC (Notification of eligible data breaches), ss 26WE-26WK.
[150]Privacy Act 1988 (Cth), s 26WE (meaning of eligible data breach).

15.2. The Four-Step Response Process

The OAIC recommends a four-step approach to breach response.[151] Document 05 provides a basic plan following this framework: (See also the QLS Data Breach Checklist)

Step	Action	Key Activities
Step 1	Contain	Stop the breach; limit damage; preserve evidence; secure systems; isolate affected data or accounts
Step 2	Assess	Investigate what happened; identify affected information and individuals; assess likelihood of serious harm; document findings (within 30 days if breach suspected)
Step 3	Notify	If eligible data breach: notify OAIC using online form; notify affected individuals
Step 4	Review	Conduct post-incident review; identify root cause; implement improvements; update breach response plan; document lessons learned

15.3. The 30-Day Assessment Period

When an entity has reasonable grounds to suspect an eligible data breach may have occurred, it must complete an assessment within 30 days.[152] That is a maximum period. The 30-day period begins when the suspicion arises.

The assessment must determine whether the breach is an 'eligible data breach', that is, whether serious harm is likely. If the assessment is not completed within 30 days, the breach is deemed to be an eligible data breach and notification is required.[153]

[151] OAIC, *Data breach preparation and response* (February 2025), Part 2: Responding to data breaches — four key steps.
[152] Privacy Act 1988 (Cth), s 26WH (assessment of suspected eligible data breach — 30 day period).
[153] Part 4: Notifiable Data Breach (NDB) Scheme | OAIC

15.4. Notification Requirements

If a breach is an eligible data breach, notification must be provided as soon as practicable.

Notification to the OAIC

The statement to the OAIC must include:[154]

- your firm name, trading entity and contact details;
- a description of the breach;
- the kinds of information involved;
- recommendations about steps individuals should take.

Notification is made via the OAIC's online Notifiable Data Breach form.

Notification to individuals

Affected individuals must be notified with:[155]

- a description of the breach;
- the kinds of information involved;
- recommendations about steps they should take (e.g., monitor accounts, change passwords, contact IDCARE);
- If a client, a recommendation that they seek appropriate legal and other advice. If direct notification is not practicable (e.g., contact details not available), substitute notification may be appropriate — such as publishing a notice on the firm's website and taking other reasonable steps to publicise the breach.

You should speak to your insurer to review policy obligations as part of this disclosure and notification process.

15.5. Professional and Confidentiality Considerations

A data breach at a law firm raises additional considerations beyond the NDB scheme:

Professional obligations: A breach involving client data is likely to engage obligations under the Australian Solicitors' Conduct Rules and fiduciary duties to clients. As a general proposition, a solicitor who has made an error adversely affecting client interests must disclose this client promptly, frankly and in sufficient detail for the client to make informed decisions.[156]

Affected clients should be notified as a matter of professional conduct (regardless of NDB requirements) once it has been established that client data has been lost.

Insurance: Professional indemnity insurance may be triggered by a data breach. Notify your insurer promptly. QLS Member firms may be eligible for assistance from the Cyber Essentials cybersecurity group policy.

Suspicious matter reports: If the breach relates to AML/CTF records, be mindful of the tipping off prohibition — do not disclose the existence of any suspicious matter reports in breach notifications.[157] Similarly, client details and especially privileged content must be protected. It would be unusual for the OAIC to need access to material which would disclose either of these things.

Other stakeholders: opposing parties must be advised if their client's confidentiality has been compromised.

Access undertakings that may have been given to gain access to family court or other restricted subpoena material, and a term of this undertaking usually requires notification to the Court as soon as possible.

---

[154]Privacy Act 1988 (Cth), s 26WK (contents of statement to Commissioner about eligible data breach).
[155]Privacy Act 1988 (Cth), s 26WL (notification to individuals about eligible data breach).
[156]Australian Solicitors' Conduct Rules 2012 (Qld), r 9.1 (confidentiality) and r 13.1 (competence and diligence).
[157]Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), s 123 (offence — tipping off about suspicious matter reports).

Similarly, participation rules/subscriber agreements for electronic conveyancing or other e-commerce providers such as Court portals or banking may require notification of incidents.

15.6. Using the Breach Response Plan

Document 05: Data Breach Response Plan provides a summary overview of what is needed.

In case of a more serious incident it is strongly encouraged that you obtain expert advice (using the Cyber Essentials QLS Member Insurance if available.)

Customise the plan by inserting your firm's details, designating response team members, and reviewing the procedures to ensure they reflect your firm's systems and processes.

Having a plan is the foundation requirement for Privacy regulated entities. However, there are also number of key things to work through that can greatly reduce the cost and impact of a cybersecurity incident. For example:

- What should staff do if the Principal is not available?
- Who will you turn to for assistance?
- How will you triage urgent work and critical dates if your system is down?
- How will you communicate with clients?
- Does your system create logs that can be used to quickly establish what happened and whether data has been accessed?
- When did you last test that your backups are working? (Not just that it seems to be working, but that you are getting usable copies that can be restored quickly.)

Chapter 16: Handling Access and Correction Requests

APPs 12 and 13 give individuals rights to access personal information held about them and to request correction of inaccurate information. This chapter provides practical guidance on handling these requests, including the exceptions that are particularly relevant to law firms.

16.1. Recognising Access Requests

An access request does not require any particular form. It need not use specific language or even refer to the Privacy Act.[158] Any request from an individual to see information you hold about them should be treated as a potential access request.

Examples of requests that may constitute access requests:

- "You act for my ex-wife. I want to see what information you have about my business"
- "I'd like a copy of my file."
- "What identity documents do you have on record for me?"

Important note: If a client / former client requests a copy of their file they are entitled to elements of this as of right.[159] Not everything on the file is the client's property.

Train staff to recognise access requests and escalate them to the Privacy Officer for handling.

16.2. Process for Handling Access Requests

Step	Action
1	Acknowledge receipt: Confirm receipt of the request and provide an expected timeframe for response (30 days is the OAIC benchmark[160]).
2	Verify identity: Before providing access, verify that the requester is the individual to whom the information relates (or their authorised representative).
3	Locate information: Search relevant systems and files to identify all personal information held about the individual.
4	Review for exceptions: Assess whether any exceptions to access apply (see section 16.3). If exceptions apply, consider whether partial access can be provided.
5	Prepare response: Compile the information for disclosure, redacting any information subject to exceptions or relating to other individuals.
6	Provide access: Provide access in the manner requested (if reasonable) or an alternative manner. If refusing access, provide written reasons.
7	Document: Record the request, your assessment, and the response for compliance purposes.

[158]Australian Privacy Principle 12.1.
[159]ASCR, rule 16.
[160]OAIC, *Chapter 12: APP 12 — Access to personal information*, APP Guidelines (October 2025), [12.25]-[12.30] (reasonable period for response).

16.3. Exceptions to Access — Key Exceptions for Law Firms

APP 12.3 sets out exceptions that permit refusal of access.[161] The following exceptions are particularly relevant to law firms:

Exception	Application to Law Firms
Legal professional privilege (APP 12.3(b))	Access may be refused where giving access would reveal information to which a claim of legal professional privilege applies. The privilege belongs to the client — if the individual requesting access is the client, questions of privilege do not arise; if the individual is a third party, privilege may protect the information.
Enforcement activities (APP 12.3(c))	Access may be refused where giving access would prejudice enforcement-related activities conducted by an enforcement body. This may be relevant where information relates to suspected fraud or criminal conduct that has been reported to police or regulators.
Privacy of others (APP 12.3(g))	Access may be refused where giving access would have an unreasonable impact on the privacy of other individuals.
Legal proceedings (APP 12.3(d)-(e))	Access may be refused where information relates to existing or anticipated legal proceedings and would not be accessible by way of discovery, or where giving access would prejudice negotiations with the individual.
Commercially sensitive decision-making (APP 12.3(h))	Access may be refused where giving access would reveal evaluative information in connection with a commercially sensitive decision-making process.

Where an exception applies to part of the information, consider whether partial access can be provided — that is, access to the information not subject to the exception.[162]

16.4. Refusing Access

If access is refused (in whole or in part), the firm must give the individual a written notice that:[163]

- states the reasons for the refusal (except where stating reasons would itself undermine the exception);
- sets out the mechanisms available to complain about the refusal (internal complaint process and the OAIC).

[161]Australian Privacy Principle 12.3 (exceptions to the access requirement).
[162]OAIC, *Chapter 12: APP 12 — Access to personal information*, APP Guidelines (October 2025), [12.55]-[12.65] (refusal and partial access).
[163]Australian Privacy Principle 12.8, (refusal to give access — written notice with reasons).

16.5. Handling Correction Requests

APP 13 requires entities to take reasonable steps to correct personal information that is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to the purpose for which it is held.[164]

When handling correction requests:

1. **Assess the request:** Is the current information actually inaccurate, out-of-date, incomplete, irrelevant or misleading? Consider the purpose for which the information is held.[165]
2. **If satisfied correction is needed:** Take reasonable steps to correct the information.[166] This usually means updating records, adding additional information, or noting that information is disputed.
3. **If refusing to correct:** Give written notice of the refusal with reasons. Offer to associate a statement with the information noting the individual's view that it is inaccurate, out-of-date, incomplete, irrelevant or misleading.[167]
4. **Notify third parties:** If correction is made and you have previously disclosed the information to third parties, consider whether to notify them of the correction.[168]

Special Consideration: Legal Records

Care must be taken with correction requests relating to legal records. File notes, attendance records, and other contemporaneous documents form part of the legal record of a matter and may be relevant to future disputes or claims.

Rather than altering such records, it may be more appropriate to add a note indicating that the information is disputed or should be read in context with more up to date information.

16.6. Fees and Timeframes

Fees: APP 12.5 permits charging a fee for access, but the fee must not be excessive.[169] Where the request comes from a client or former client no charge can be made for giving them access to the file in most circumstances.[170] The OAIC indicates that fees should reflect the actual cost of providing access and should not be used to discourage access requests.[171] Correction requests must be handled free of charge.

Timeframes: Respond to access and correction requests within a reasonable period. The OAIC suggests 30 calendar days as a benchmark for access requests. If more time is needed, communicate this to the requester. A client's file must be supplied "as soon as reasonably practicable". 30 days would be longer than usual for most client file uplifts.

Complaints: If an individual is dissatisfied with how an access or correction request was handled, they may complain to the OAIC.[172] Ensure your privacy policy explains the complaint process.

---

[164]Australian Privacy Principle 13.1.
[165]OAIC, *Chapter 13: APP 13 — Correction of personal information*, APP Guidelines (October 2025), [13.20]-[13.30] (considerations when assessing correction requests).
[166]Australian Privacy Principle 13.2,(obligation to correct if satisfied information is inaccurate).
[167]Australian Privacy Principle 13.3,(if refuse to correct, must give written notice and offer to associate a statement).
[168]Australian Privacy Principle 13.4,(notification of correction to third parties).
[169]Australian Privacy Principle 12.5,(fees for access).
[170] See: Charging for document storage - Queensland Law Society
[171]OAIC, *Chapter 12: APP 12 — Access to personal information*, APP Guidelines (October 2025), [12.40]-[12.50] (charges for access).
[172]Privacy Act 1988 (Cth), s 36 (making a privacy complaint to the Commissioner).

Chapter 17: Staff Training

Effective privacy compliance depends on staff understanding their obligations and knowing how to apply privacy principles in their daily work.

APP 1.2 requires entities to take reasonable steps to implement practices, procedures and systems — and staff training is a critical component of this.[173] This chapter explains how to develop and deliver privacy training using Document 07: Staff Training Framework.

17.1. Who Needs Training

All staff who handle personal information need privacy training.[174] In a law firm, this typically includes:

Role	Training Focus
Principals	Overall compliance responsibility; governance; breach response decision-making; regulatory interaction
Solicitors	Confidentiality reminder, Collection and use of client information; collection notices; handling access/correction requests; privilege considerations; client communication about privacy
Paralegals/Legal assistants	Confidentiality training, Collection procedures; document handling; recognising access requests; secure document management
Administrative staff	Confidentiality training, Reception of enquiries; client identification; secure document handling; recognising and escalating privacy requests
IT/Systems staff	Which technical security measures have been selected; access controls; incident response; security policies and their role in maintaining and enforcing them.
New staff (all roles)	Induction training covering legal confidentiality rules, firm privacy policy, key procedures (such as system use and access, password policy, personal device policies, use of external systems – including AI – and internal incident escalation.)

[173]Australian Privacy Principle 1.2(d), (staff training as part of reasonable steps to implement practices, procedures and systems).
[174]OAIC, *Chapter 1: APP 1 — Open and transparent management of personal information*, APP Guidelines (October 2025), [1.35]-[1.40] (staff awareness and training).

17.2. Core Training Content

Document 07: Staff Training Framework provides a comprehensive training curriculum. Core topics that all staff should understand include:[175]

- **Why privacy matters:** Privacy vs confidentiality intersection, what information the firm holds is privacy regulated vs confidential, connection to professional obligations; consequences of non-compliance.
- **Key concepts:** Personal information; sensitive information; confidential information, privileged information, collection, use and disclosure.
- **Firm's privacy policy:** Overview of the policy; where to find it; how it applies to daily work.
- **Security practices:** Password security; physical security; secure document handling; email security.
- **Collection notices:** When and how to provide collection notices; which template to use.
- **Recognising requests:** How to recognise access requests, correction requests, and complaints; escalation procedures.
- **Data protection measures and policies:** what they are and how to use them;
- **Incident reporting:** How to recognise a potential data breach; reporting procedures; importance of prompt reporting.
- **AML/CTF integration:** The connection between AML/CTF and privacy; CDD procedures; tipping off prohibition.

17.3. Training Delivery and Documentation

Document training delivery: Maintain a training register recording training sessions delivered, attendees, and topics covered.

This provides evidence of compliance with APP 1.2 and AML/CTF training requirements. It will also be of great assistance if a staff member makes an error and the firm needs to establish what steps it took to prevent this happening.

[175]OAIC, *Privacy management framework* (May 2025), Step 4: Train staff — training should be role-appropriate.

Chapter 18: Handling Privacy Complaints

Individuals have the right to complain if they believe their privacy has been breached. Your privacy policy must explain how individuals can complain and how complaints will be handled.[176]

18.1. Establishing a Complaint Process

A good complaint process should be:[177]

- **Accessible:** Easy to find (in privacy policy) and easy to use.
- **Transparent:** Clear about what will happen with complaints and expected timeframes.
- **Fair:** Complaints investigated impartially with opportunity for complainant to respond.
- **Confidential:** Complainant's information handled appropriately.

Designate who is responsible for handling privacy complaints (typically the Privacy Officer). Ensure that person has authority to investigate and resolve complaints.

18.2. Receiving and Assessing Complaints

A privacy complaint does not require any particular form. Any expression of dissatisfaction about how the firm has handled personal information should be treated as a potential complaint.[178]

Step	Action	Detail
1	Receive	Record the complaint; acknowledge receipt within 5 business days; provide expected timeframe for response
2	Assess	Clarify the complaint if needed; identify the APP or privacy issue raised; determine if complaint is within scope
3	Investigate	Gather relevant information; review records; consider the facts against privacy obligations; document findings
4	Respond	Communicate outcome to complainant; explain findings; if breach occurred, explain remediation steps
5	Resolve	Implement any agreed remediation; if complainant remains dissatisfied, advise of right to complain to OAIC
6	Record	Document the complaint, investigation, and outcome; identify any systemic issues for follow-up

18.3. Timeframes

While the Privacy Act does not specify timeframes for complaint handling, the OAIC expects complaints to be handled promptly. Good practice timeframes include:[179]

- **Acknowledgement:** Within 5 business days of receiving the complaint.
- **Initial response:** Within 30 days for most complaints.
- **Complex matters:** If more time is needed, communicate this to the complainant with an updated timeframe.

---

[176] Australian Privacy Principle 1.4(e), (privacy policy must explain how to complain).
[177] OAIC, *Privacy complaint handling* (March 2025), Part 1: Setting up a complaint handling process.
[178] OAIC, *Privacy complaint handling* (March 2025), Part 2: Receiving and assessing complaints.
[179]

18.4. Escalation to the OAIC

If a complainant is dissatisfied with how their complaint is handled, they may complain to the OAIC.[180] The OAIC generally expects complainants to first raise the matter with the entity before escalating.[181]

If the OAIC investigates:[182]

- Cooperate fully with the investigation, bearing in mind that information from a client file may not be automatically handed over;
- Provide requested information within timeframes;
- Consider engaging legal advice, particularly for significant complaints;
- Notify professional indemnity insurer if the complaint may give rise to a claim.

The OAIC may make a determination if it finds an interference with privacy occurred.[183] Determinations can include declarations that conduct was an interference with privacy, requirements to take specified steps, and requirements to pay compensation.

[180]Privacy Act 1988 (Cth), s 36 (individuals may complain to the Commissioner about an act or practice that may be an interference with privacy).
[181]Privacy Act 1988 (Cth), s 40(1A) (Commissioner may decline to investigate if complaint not first made to the respondent).
[182]Privacy Act 1988 (Cth), Part V (investigations by the Commissioner), ss 36-52.
[183]Privacy Act 1988 (Cth), s 52 (determinations by the Commissioner following investigation).

PART F

REFERENCE MATERIALS

Chapter 19: Resources and References

19.1. OAIC Guidance and Resources

Resource	Description / Use
Australian Privacy Principles Guidelines	Comprehensive guidance on interpreting and applying each APP. Essential reference for understanding APP requirements.
Guide to developing an APP privacy policy	Detailed guidance on privacy policy content and drafting. Use when developing or reviewing your privacy policy.
Guide to securing personal information	Guidance on reasonable security measures under APP 11. Reference for security implementation.
Data breach preparation and response	Guidance on NDB scheme compliance. Essential for breach response planning.
Privacy management framework	Framework for establishing and maintaining privacy compliance. Useful for governance and implementation.
Guide to undertaking privacy impact assessments	Guidance on when and how to conduct PIAs. Reference for PIA process.
Privacy complaint handling	Guidance on internal complaint handling processes. Reference for complaint process design.
Notifiable Data Breach form	Online form for notifying eligible data breaches. Bookmark for breach response.
Privacy guidance for reporting entities under the Anti-Money Laundering and Counter-Terrorism Financing Act	Summary of the intersection between AML obligations and Privacy, with specific reference to the implications for Small Businesses.

OAIC webs ite: www.oaic.gov.au[184]

Specific references used as the basis for information in this toolkit include:

[184]OAIC, *Australian Privacy Principles Guidelines* (October 2025), available at <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines>.

19.2. Key Legislation

Legislation	Key Provisions
Privacy Act 1988 (Cth)	Schedule 1 (APPs); Part IIIC (NDB scheme); Part V (enforcement)
Privacy and Other Legislation Amendment Act 2024 (Cth)	2024 amendments including automated decision-making disclosure (from Dec 2026)
Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)	Part 2 (CDD); s 84 (AML/CTF programs); s 107 (record retention); s 123 (tipping off)
Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024 (Cth)	Tranche 2 reforms extending to professional services (from 1 July 2026)
Legal Profession Act 2007 (Qld)	Part 3.3 (trust accounts); s 258 (retention of trust records)
Australian Solicitors' Conduct Rules 2012 (Qld)	Rule 9 (confidentiality); Rule 13 (competence and diligence)

Federal Register of Legislation: www.legislation.gov.au

19.3. Other Useful Resources

AUSTRAC: AML/CTF guidance for professional services sector — www.austrac.gov.au[185]

Queensland Law Society: Practice support resources including file retention guidance — www.qls.com.au[186]

Australian Cyber Security Centre: Essential Eight and cybersecurity guidance — www.cyber.gov.au

IDCARE: National identity and cyber support service for breach victims — www.idcare.org

[185]AUSTRAC, *AML/CTF Reform — Professional services sector*, available at <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/amlctf-reform>.
[186]Queensland Law Society, Practice Support resources, available at <https://www.qls.com.au/For-the-profession/Practice-support>.

Chapter 20: Glossary of Key Terms

This glossary defines key terms used throughout this manual and in privacy compliance generally.

Term	Definition
APP	Australian Privacy Principle — the 13 principles in Schedule 1 to the Privacy Act that govern handling of personal information by APP entities.
APP entity	An entity to which the APPs apply, including organisations (private sector) and agencies (government). Small businesses are generally exempt unless they fall within an exception (such as being an AML/CTF reporting entity).
AML/CTF	Anti-Money Laundering and Counter-Terrorism Financing — the regulatory regime under the AML/CTF Act designed to prevent money laundering and terrorism financing.
Collection	The gathering, acquiring, or obtaining of personal information from any source and by any means, including directly from individuals and from third parties.
Consent	Voluntary agreement to some act or practice. For privacy purposes, consent to collection, use or disclosure of personal information must be informed, voluntary, current and specific.
Customer due diligence (CDD)	The process of identifying and verifying the identity of customers, and understanding the nature of their business, as required by the AML/CTF Act.
Designated service	A service specified in the AML/CTF Act that triggers reporting entity obligations. For lawyers, this includes certain transactional services but excludes legal advice and court representation.
Disclosure	Making personal information accessible to others outside the entity, or releasing it from the entity's effective control.
Eligible data breach	A data breach that triggers notification obligations under the NDB scheme — being unauthorised access, disclosure or loss of personal information where serious harm is likely.
Interference with privacy	A breach of an APP or other contravention of the Privacy Act. The OAIC may investigate interferences with privacy and make determinations.
NDB scheme	Notifiable Data Breaches scheme — the legislative scheme under Part IIIC of the Privacy Act requiring notification of eligible data breaches.
OAIC	Office of the Australian Information Commissioner — the federal regulator for privacy matters.
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether recorded in a material form or not.
PIA	Privacy Impact Assessment — a systematic assessment of a project to identify privacy impacts and how they can be addressed.

Primary purpose	The main reason for which personal information was collected. Information may generally be used or disclosed for the primary purpose without further justification.
Reporting entity	An entity that provides designated services under the AML/CTF Act and is therefore subject to AML/CTF obligations including CDD, reporting, and record-keeping.
Secondary purpose	A purpose other than the primary purpose for which information was collected. Use or disclosure for a secondary purpose requires an exception (such as consent or legal requirement).
Sensitive information	A subset of personal information that attracts additional protections, including health information, biometric information, racial or ethnic origin, political opinions, religious beliefs, and criminal record.
Serious harm	For NDB purposes, harm that a reasonable person would consider to be serious, including physical, psychological, emotional, financial, or reputational harm.
Use	The handling of personal information within the entity, including accessing, reading, analysing, referencing, or otherwise doing something with the information internally.

Chapter 21: Quick Reference Guides

These quick reference guides provide at-a-glance summaries for common privacy scenarios. Consider printing these for easy reference.

21.1. Quick Reference: Privacy & New Client Onboarding

NEW CLIENT PRIVACY CHECKLIST

- ☐ Determine whether a designated service is to be supplied
- ☐ If designated service: Provide AML/CTF Collection Notice (client)
- ☐ Collect identity documents (if needed, retain copy if essential but preferably note details and certify that the original documents were inspected)
- ☐ Verify identity (Following firm policy, may depend on whether ARNECC Safe Harbour is relevant)
- ☐ If corporate client: Identify beneficial owners (they may require a Collection Notice)
- ☐ Confirm client has access to privacy policy (reference in engagement letter)
- ☐ Record in matter management system

21.2. Quick Reference: Access Request Handling

ACCESS REQUEST QUICK GUIDE

1. ACKNOWLEDGE within 5 days — confirm receipt, advise 30-day timeframe
2. VERIFY identity of requester before providing access
3. LOCATE all personal information about the individual
4. REVIEW for exceptions:
   - Legal professional privilege?
   - Privacy of others affected?
   - Related to legal proceedings?
   - Enforcement activities prejudiced?
5. PROVIDE access or REFUSE in writing (with reasons and complaint info)
6. DOCUMENT the request, assessment, and response

Target: Complete within 30 calendar days

21.3. Quick Reference: Data Breach Response

DATA BREACH IMMEDIATE RESPONSE (See QLS Checklist here)

STEP 1: **CONTAIN** (Immediately)

- Stop the spread —isolate systems, prevent outgoing email
- Preserve evidence — do not delete logs or data
- Ask for help from IT, insurers

STEP 2: **ESCALATE** (Same day)

- Notify Privacy Officer / Principal
- Activate breach response plan (Document 05)

Ensure clients know to contact their bank immediately if money could have been diverted. Even minutes can count.

STEP 3: **ASSESS**

- What information was affected? Is that Privacy Act Regulated information?
- Who is affected?
- Is serious harm likely? → If yes, it's an ELIGIBLE DATA BREACH

STEP 4: **NOTIFY** (If eligible — as soon as practicable)

- Notify OAIC via online form
- Notify affected individuals with recommended steps

21.4. Quick Reference: Key Contacts

Contact	Details
Firm Privacy Officer	[Insert name, phone, email]
OAIC (enquiries)	1300 363 992 / enquiries@oaic.gov.au
OAIC (NDB notification)	www.oaic.gov.au/privacy/notifiable-data-breaches
AUSTRAC	1300 021 037 / www.austrac.gov.au
IDCARE (breach support)	1800 595 160 / www.idcare.org
Queensland Law Society	(07) 3842 5943 / www.qls.com.au
Lexon	(07) 3007 1266
Professional Indemnity Insurer	[Insert insurer contact details]
IT Support / MSP	[Insert IT support contact details]

Implementation Checklist & Timeline

Implementation overview

This toolkit provides Queensland law firms with practical templates and guidance for implementing Privacy Act compliance obligations arising from AML/CTF Tranche 2. All firms providing 'designated services' under the AML/CTF Act are small business reporting entities under the Privacy Act and must comply with Australian Privacy Principles (APPs).

The toolkit includes seven practical documents designed for immediate use by small-to-medium law firms.

Toolkit contents

This implementation package includes seven practical documents:

1. **Implementation Checklist & Timeline** (this document) — Master roadmap for privacy compliance
2. **Template Privacy Policy** — APP-compliant policy with AML/CTF-specific clauses
3. **Collection Notice Template** — APP 5 compliant notice for client onboarding (KYC/CDD)
4. **Personal Information Register** — Record of personal information flows and privacy risks
5. **Data Breach Response Plan** — Notifiable Data Breaches (NDB) scheme procedures
6. **Privacy Impact Assessment** — Threshold PIA tool for new systems and processes
7. **Staff Training Framework** — Privacy awareness training outline with sample materials

Privacy project – simple implementation

Complete these tasks in sequence to establish baseline privacy compliance:

Phase 1: Foundation

- ☐ Conduct threshold assessment: Confirm firm provides 'designated services' under AML/CTF Act
- ☐ Assign Privacy Officer role (may be Principal or Practice Manager)
- ☐ Complete Personal Information Register (Document 4) to map data flows
- ☐ Undertake self education to ascertain firm’s obligations

Phase 2: Documentation

- ☐ Customize Template Privacy Policy (Document 2) for firm's specific practices
- ☐ Publish privacy policy on firm website and make available in office
- ☐ Adapt Collection Notice Template (Document 3) for client onboarding process
- ☐ Update client engagement letters to reference privacy policy and collection notice
- ☐ Create data breach response procedures using Document 5

Phase 3: Systems & Training

- ☐ Review current technology systems against APP 11 security requirements
- ☐ Conduct Privacy Impact Assessment (Document 6) for any new/planned systems
- ☐ Implement Staff Training Framework (Document 7) — deliver initial training session
- ☐ Document training attendance and maintain training records
- ☐ Establish process for privacy inquiries and complaints

Phase 4: AML/CTF Integration

- ☐ Register with AUSTRAC (deadline: 31 March 2026)
- ☐ Implement AML/CTF customer due diligence (CDD) procedures
- ☐ Determine what regulated personal information is likely to be collected during CDD and how to handle that.
- ☐ Establish record retention policy

Phase 5: Testing & Refinement

- ☐ Review data breach response procedures with IT support team.
- ☐ Schedule consideration of ongoing cybersecurity improvement.
- ☐ Schedule annual privacy compliance review date

DISCLAIMER

This toolkit provides general guidance only and is not legal advice.

Queensland Law Society — May 2026

AI Usage statement

Literature review: Claude Opus 4.6

Briefing paper: Claude Opus 4.6

Guide content drafting: Wireframe, Claude Opus 4.7, Document drafting: N/a

Page formatting, footnotes: Claude Opus 4.6, pptxgenjs

Template document drafting: Wireframe, Claude Opus 4.7, first draft Chat GPT v5, revisions: N/a

Last update: 31 May 2026

Verification and content responsibility: D Bowles, Solicitor, QLS.

Disclaimer: The content of this material is not intended as legal advice. Specific advice pertinent to your circumstances is prudent prior to acting upon it. Third party sources and resources may change without notice and should be checked for currency.