Queensland Law Society

Privacy Program Starter Guide

For small law firms preparing for Privacy Act changes commencing 1 July 2026

June 2026

Privacy Program Starter Guide

for small law firms preparing for Privacy Act changes commencing 1 July 2026

From **1 July 2026**, the small-business exemption in the Privacy Act 1988 (Cth) will be **partially withdrawn** for firms that provide 'designated services' under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (the AML/CTF Act). Many small firms (turnover less than $3 Million) that have never had to think about the Australian Privacy Principles (APPs) will now need to comply with them — at least for some of the information they hold.

This Starter Guide is a short companion to the QLS Privacy Compendium (the 'Compendium'). The Compendium summarises guidance from the Office of the Australian Information Commissioner (OAIC), AUSTRAC and other sources in enough detail to understand basic obligations. For most purposes you won't need to read the entire compendium, just the chapters which relate to your specific task.

AT A GLANCE

- **Who is affected?** Law firms with annual turnover under $3 million that provide AML/CTF designated services (typically conveyancing, business sales, company or trust structuring, managing client money + other). Firms above $3 million are already fully regulated.
- **What is regulated?** Personal information collected or held for the purposes of or in connection with AML/CTF activities (Privacy Act, s.6E)— for example, client identity documents, beneficial owner records, AML risk assessment notes.
- **What is the deadline?** 1 July 2026 (AML/CTF Tranche 2 commencement). Additional automated-decision-making disclosures commence 10 December 2026.
- **What are the penalties?** OAIC have significant enforcement powers, including fines up to $50 million dollars.

Where do I start? Read this guide, then work through the four step roadmap on page 4. Information available in the Compendium and associated template documents & policies should provide most of what you need.

Compendium reference: Chapter 1 'Purpose and Scope of This Manual' (pp. 5-9); Chapter 2 'Privacy Act changes in 2026' (pp. 10-14);

What is changing?

Until 1 July 2026, the Privacy Act has largely left small law firms alone. Most firms operate within the small-business exemption, principally governed by turnover. The Privacy Act always regulated AML reporting entities, but until 2026 most law firms did not fall into that category. Now many will.

For a firm under the turnover threshold, the practical effect is a **partial withdrawal of the exemption**: some of your information is in scope, the rest is not. A firm over the threshold is Privacy Act regulated and has been for some time.

The Privacy Act does not regulate all of an organisation's data holdings, only "personal information". For firms otherwise within the small business exemption only the AML-related subset of personal information will be regulated. While the term "regulated personal information" does not appear in the Act, in practical terms that is what we are concerned with and references to personal information should be read accordingly. Personal information collected for a dual purpose (Identity documents to comply with ARNECC/PEXA rules and *also* AML/CTF, for example) is regulated.

Regulated personal information must be collected and managed in accordance with the Australian Privacy Principles ("APPs").

In one sense the entirety of a solicitor's file is relevant to AML activity – we must monitor the whole transaction as it unfolds to watch for money laundering red flags. On current indications the OAIC does not appear to regard this broader use as falling within the definition.

Compendium reference: Chapter 2.1 'The AML/CTF & Privacy Act interaction' (p. 10); OAIC guidance: Privacy guidance for reporting entities under the Anti-Money Laundering and Counter-Terrorism Financing Act | OAIC

Designated services — the trigger

Whether your small firm is AML regulated and therefore Privacy regulated depends on whether you provide any 'designated services'. Designated services are set out in Table 6 of the AML/CTF Act1. The broad categories are:

- Assisting in the planning or execution of a transaction to buy or sell real estate (conveyancing).
- Assisting in the planning or execution of a transaction to buy, sell or transfer a business or shares.
- Managing a client's money, securities or other property.
- 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.

Several common legal activities are **excluded**: providing legal advice only, representing a client in court or tribunal proceedings, and trust account disbursements made on client instructions in connection with legal services. A firm that does only family-law litigation, for example, might escape providing designated services — but a single activity in scope can change that. There is no *de minimis* exemption: providing even one designated service on one occasion brings the firm into both regulatory systems.

While the core designated service classes and exemptions are clearly defined, there are many uncertainties in the edge cases. A quick analysis of the basics and assumption that your firm is not regulated may prove to be an expensive mistake.

Compendium reference: Chapter 2.3 'What are designated services?' (p. 11); Chapter 2.4 'Consequences of Non-Compliance' (p. 12).

The changes are modest but important

Privacy compliance does not fundamentally change anything you currently do. It **sits alongside** a solicitor's established duties of confidentiality and the rules protecting legal professional privilege. A firm that has always maintained strict confidentiality is **not automatically** privacy-compliant: privacy law has a different focus and imposes proactive duties (notification, security, individual access rights) that confidentiality does not. It also involves duties to non-clients. It is likely that existing policies (how long you keep files, for example) may need to be updated.

Compendium reference: Chapter 4 'Confidentiality vs Privacy — Key Distinctions' (pp. 11-14); Chapter 5 'What Changes for Your Firm' (pp. 25-31).

The seven core documents and policies

A basic compliance program is built around seven template documents in the Privacy Toolkit. Each is keyed to a specific obligation under the APPs or the Notifiable Data Breaches scheme, and each is explained in detail in the corresponding chapter of the Compendium.

It is important to note that simply putting your firm's name on a template policy is not sufficient. The policy must reflect and guide your actual real world data collection and handling practices. This requires both establishing the compliance program and maintaining it over time. A system for dealing with access requests and privacy complaints is mandatory, for example.

Doc	Document	Purpose	Compendium ref.
01	**Privacy Policy**	Reflects and explains how the firm handles regulated personal information.	Ch. 10, p. 49
02	**Collection Notice**	Tells individuals what you collect and why.	Ch. 11, p. 52

[1] See Subsection 6(5B), Table 6.

Doc	Document	Purpose	Compendium ref.
03	**PI Inventory**	Register of regulated information you hold.	Ch. 12.1, p. 55
04	**Retention Schedule**	What you keep, and for how long.	Ch. 12.2, p. 56
05	**Breach Response Plan**	Four-step procedure under the NDB scheme.	Ch. 15, p. 68
06	**PIA Framework**	Checklist to assess the privacy impact of new systems or processes.	Ch. 5.2, p. 26
07	**Training Framework**	Staff training program and records.	Ch. 17, p. 76

*The templates are **starting points*** — each contains bracketed placeholders that must be replaced, and each will need at least some firm-specific tailoring. Drafting notes included in the documents should be deleted once appropriate selections are made.

The Privacy Policy in particular needs careful review. It must both guide and reflect your actual processes, and it should not bind your firm to deal with all personal information as if it were *regulated* personal information. A poorly drafted policy can extend your regulatory obligations beyond what the law requires by making general promises you will then be held to.

Compendium reference: Chapter 1.4 ‘The Compliance Toolkit — Documents at a glance’ (p. 8); OAIC : Privacy Essentials Checklist for AML/CTF reporting entities.

What are APPs and what do they require us to do?

The Australian Privacy Principles are thirteen rules in Schedule 1 of the *Privacy Act 1988* (Cth) that cover the complete lifecycle of personal information — from how it is collected, through how it is used, stored and destroyed, to how individuals can access and correct it. All thirteen apply to an APP entity, but six will do *most* of the day-to-day work in a small or medium law firm context:

APP	What it asks the firm to do
APP 1 — Open and transparent management	Have a clearly expressed, up-to-date privacy policy and documented practices, procedures and systems to ensure compliance.
APP 3 — Collection	Collect personal information only where reasonably necessary for the firm's functions; sensitive information requires consent or a specific exception.
APP 5 — Notification	Tell individuals what you are collecting, why, who you might disclose it to, and how to access or complain — at or before the time of collection.
APP 6 — Use and disclosure	Use the information only for the primary purpose for which it was collected, unless an exception applies.
APP 11 — Security	Take reasonable steps to protect information from misuse, loss and unauthorised access; destroy or de-identify it when it is no longer needed.
APPs 12 & 13 — Access and correction	On request, give individuals (including non-clients) access to their personal information, and correct it where it is inaccurate, out of date, incomplete or misleading. (Subject to important exceptions)

Honourable mention: APP 8 requires disclosure where regulated personal information will be sent overseas. (If you use a Virtual Assistant or software which processes data outside of Australia, for example.)

Some of these obligations are framed in terms of ‘reasonable steps’ — a proportionate standard that takes into account the size of the firm, the sensitivity of the information held, and the practicability of the measure. A

small firm is not expected to operate like a major institution, but it is expected to take steps that **are genuine and proportionate to the risks** posed and the resources available.

Compendium reference: Chapter 7 'Introduction to the APPs' (pp. 34-37); Chapter 8 'APPs Most Relevant to Law Firms' (pp. 38-44); Chapter 7.4 'The "Reasonable Steps" Standard' (p. 36).

The four step roadmap

If you set aside time to give the issue your undivided attention, a few hours a week for four weeks should be enough provided you have an existing reasonable standard of cybersecurity.

If you do not, expand Phase 3 and start the cybersecurity workstream in Phase 1. The Compendium sets out the same roadmap in more detail at Chapter 13 (p. 60).

PHASE 1 | Week 1	PHASE 2 | Week 2	PHASE 3 | Week 3	PHASE 4 | Week 4
Foundation	**Documentation**	**Implementation**	**Readiness & sign-off**
• Confirm whether the firm provides designated services. • Appoint a Privacy Officer (usually a Principal). • List the regulated personal information you collect (start of Doc 03). • Block calendar time to get the basics in place by 1 July 2026.	• Customise Privacy Policy (Doc 01). • Customise Collection Notice(s) (Doc 02). • Finalise the PI Inventory (Doc 03) and Retention Schedule (Doc 04). • Develop the Breach Response Plan (Doc 05) and run the threshold PIA (Doc 06).	• Publish the Privacy Policy to the firm website. • Roll out collection notices via engagement letters and ID requests. • Update intake forms, file-destruction protocols and onboarding. • Deliver a short training session — record attendance (Doc 07). • Review cybersecurity; consider SMB1001 certification.	• Identify and diarise any residual gaps. • Principal sign-off on readiness. • Schedule cybersecurity improvement work and an IT review. • Diarise an annual privacy review.

A LAW FIRM's ACHILLES HEEL — CYBERSECURITY

APP 11 requires reasonable steps to protect regulated personal information. For a law firm holding identity documents2 and highly sensitive information, 'reasonable' sets a high bar.

The cost and damage of a cyber attack also makes an investment in information security a very good idea irrespective of regulatory obligations.

Most firms benefit from working towards SMB1001 certification, or using recognized frameworks such as NIST or the ACSC Essential Eight. Obtaining certification not only allows firm Principals to be satisfied that their firm is moving the right direction but demonstrates objective proof of your cyber-readiness to clients and regulators if called upon to do so.

Compendium reference: Chapter 14 'Security Measures' (pp. 65–67).

[2] Ideally, you should not keep full copies of ID documents. Only if your safe harbour obligations for ARNECC/PEXA VOI require it should you do so.

Common questions

I don't think I will be providing Designated Services. Is that OK?

No. A general intention not to do so must be backed by a strong guardrail ensuring that your firm does not accidentally move into the AML sphere. This requires both firm Principals and all staff to have a very good understanding of what is and is not regulated, and a comprehensive onboarding system to screen out provision of designated services. Also ensure that a request to expand your scope of work in a matter is carefully considered. (Signing a Guarantor's Certificate, for example)

What about firms with turnover above $3 million?

Larger firms are already Privacy Act–regulated and have been since the Act came into force. For those firms, all personal information is in scope (not only AML/CTF information), and the templates in this toolkit are not appropriate. The structure of the implementation roadmap is the same; but the scope of what each document covers is wider and the "reasonable steps" required to comply with obligations will be higher.

Should I just treat all data I hold as regulated, to keep life simple?

Possibly — but the decision should be deliberate. Running parallel regimes for 'regulated' and 'unregulated' personal information can be administratively painful, and some firms will sensibly apply privacy-grade security and retention practices to everything.

What you must avoid is accidentally opting in by publishing a Privacy Policy or Collection Notice that does not make the scope clear. The template Privacy Policy is drafted with the partial exemption in mind; do not strike out the scope clause without thinking about the consequences. (See Compendium Chapter 2.1, p. 10.)

What does document retention have to do with it?

A particular focus of the OAIC is that businesses (in particular professional firms) do not collect potentially damaging data they don't need and don't keep it any longer than they have to. This is hard to reconcile with the expectations on solicitors to collect and retain evidence that might be needed later, potentially much longer than the usual minimum mandatory retention period of 7 years. For this reason, a balance must be struck, your decision documented and system to get rid of excess information implemented.

Further OAIC and QLS resources

QLS Privacy Compendium and template documents: <<Link>>

Guide to privacy for reporting entities under the AML/CTF Act (February 2026): oaic.gov.au — Privacy guidance for reporting entities with associated resources: (available on the OAIC website here)

OAIC template AML/CTF collection notice: oaic.gov.au — Template AML/CTF collection notice

OAIC Notifiable Data Breaches scheme — decision trees and checklists: oaic.gov.au/privacy/notifiable-data-breaches

QLS Cybersecurity hub (member resources, password template, checklists): qls.com.au — Cybersecurity

ACSC Essential Eight maturity model: cyber.gov.au — Essential Eight