

Privacy Act changes for law firms

STARTING: 1 JUL 2026

New privacy requirements apply to law firms with **an annual turnover under \$3 million** that provide **designated services** under the AML/CTF Act. Personal information collected for AML/CTF purposes will now be regulated under the Privacy Act. Fines up to \$50 Million apply for noncompliance.

At a glance

The small-business exemption to Privacy Act regulation has been partially withdrawn.

If your firm supplies AML/CTF designated services (conveyancing, business sales, company/trust structuring + more) you need to implement a privacy program.

A basic privacy program requires:

- **A Privacy Officer:** Responsible (together with the Principal) for the firm's compliance
- **Documentation:** A Privacy Policy, Collection Notice(s), Document Retention Schedule and a Data Breach response plan
- **Training:** You will need to be able to demonstrate that staff have been trained and shown what to do
- **Ongoing compliance:** New obligations relating to privacy will sit beside your existing confidentiality obligations
- **Cybersecurity:** Firms must take "reasonable steps" to protect regulated personal information. Take this opportunity to improve information security

Where to start?

1 Foundation

Week 1

Know your scope. Pick your person. Map what data you actually touch.

- Threshold check.** Do you provide "designated services"?
- Appoint a Privacy Officer** (usually a Principal or Practice Manager)
- List what **regulated personal information** you are likely to collect.
- Schedule time** to ensure you can get the basics in place by 1 July 2026

2 Documentation & policies

Week 2

Customise the template documents needed for basic compliance.

- Privacy Policy**
- Regulated Data Inventory**
- Breach Response Plan**
- Collection Notice**
- Data Retention Schedule**
- Privacy Impact Checklist**

3 Implementation

Week 3

Put paper into practice. People, systems, website.

- Publish Privacy Policy** on website
- Roll out collection notices** via engagement letters & ID requests
- Cybersecurity review** – assess your current security and what you need to improve
- Update firm procedures** (eg, onboarding forms, file destruction protocols)
- A short training program** – record attendance
- Create complaints process** & access/correction handling

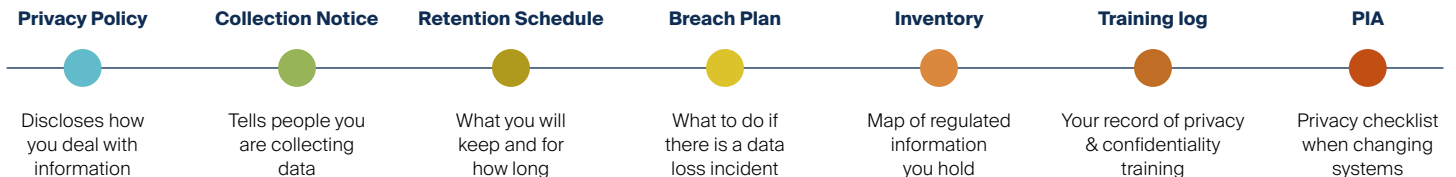
4 Readiness & Sign-off

Week 4

Verify, fix gaps, document. Then keep improving.

- Start cybersecurity program.** Consider SMB-1001 certification as a starting point
- List** anything that still needs to be done; diarise
- Principal sign-off** on readiness; diarise review
- With IT support; schedule cyber improvement

Core Features



Is all my data regulated?

No. Only data collected for or in relation to an AML purpose is regulated if a small business.

What about confidentiality & privilege?

These remain unaffected. A solicitor's professional duties and a client's right to claim privilege sit side by side with Privacy Act measures.

What about larger firms?

Firms with turnover above \$3 Million are already Privacy Act regulated, and obligations extend to all personal information held.

For more information and template documents visit the QLS website [here](#).