



PRIVACY COMPLIANCE · REAL ESTATE

The Privacy Trap: What Real Estate Agencies Must Know Before 1 July 2026

A plain-English guide to the privacy obligation almost no one is talking about

FREE GUIDE

Accessible**Risk**

enquiries@accessablerisk.com

The obligation hiding behind AML/CTF

Everyone's talking about AUSTRAC. Almost no one is talking about this.

From 1 July 2026, real estate agencies that are involved in buying or selling property for clients become reporting entities under Australia's anti-money laundering laws. That much most principals now know. What far fewer realise is what comes attached to it.

For years, most real estate agencies relied on the small business exemption in the Privacy Act — if your turnover was under \$3 million, the Act largely didn't apply to you. That exemption does not apply to reporting entities for the personal information they handle to meet their AML/CTF obligations.

So the moment your agency is captured by the AML/CTF regime, it is also brought within the Privacy Act 1988 and the Australian Privacy Principles — regardless of your size. The OAIC estimates this change will affect more than 100,000 small businesses.

Two regulators, not one

AUSTRAC oversees your AML/CTF obligations. The Office of the Australian Information Commissioner (OAIC) oversees your privacy obligations. Both apply from day one — and the OAIC can pursue penalties of up to \$50 million for serious or repeated privacy breaches, on top of anything AUSTRAC does.

What the Privacy Act actually requires

The Australian Privacy Principles, in plain English

Principle	What it means for your agency
APP 1 — Open and transparent	Have a clear, current Privacy Policy that is publicly available (for example on your website)
APP 3 & 5 — Collection	Collect only what you reasonably need, and tell people what you're collecting
APP 6 — Use & disclosure	Only use or disclose personal information for the purpose you collected it for
APP 10 & 11 — Quality & security	Keep information accurate, and protect it from loss, misuse and unauthorised access
APP 12 & 13 — Access & correction	Let individuals ask to see the information you hold about them, and correct it if it's wrong

The practical takeaway — Compliance isn't a state of mind — it's a set of documents and processes. A Privacy Policy, a collection notice, a way to handle access requests, and a plan for when something goes wrong. Good intentions don't satisfy the APPs; evidence does.

The data minimisation trap

The instinct that gets agencies into trouble

Here is the single most counter-intuitive part of the new regime — and the one the OAIC has gone out of its way to spell out.

When agencies start verifying identity, the natural instinct is to keep everything: scan the driver licence, save the passport, file it all away "just in case". That instinct is wrong, and it can itself be a privacy breach.

The OAIC's guidance is clear: the AML/CTF regime does not require you to keep full copies of identification documents. You should record only the minimum details necessary to evidence that verification was carried out — not the documents themselves — unless another law specifically requires you to retain copies.

Why this matters

Every full ID document you store is something you can lose in a data breach. Holding copies you don't need increases your risk and your exposure — without improving your AML/CTF compliance at all. Less is genuinely safer.

This is exactly the kind of detail a generic privacy template misses — and exactly the kind of thing a regulator notices.

Where the two regimes collide

The tipping-off trap — and breaches

Privacy law and AML/CTF law mostly point the same way: handle information carefully. But in two places they pull in opposite directions, and that's where agencies get caught.

The tipping-off trap

Privacy law says be transparent and give people access to their information. AML/CTF law says you must never reveal that a suspicious matter report has been, or may be, made — that's the criminal offence of "tipping off". So when someone asks to see the information you hold about them, you must respond to the privacy request without disclosing anything about a suspicion or a report.

When something goes wrong

Under the Notifiable Data Breaches scheme, if personal information is lost or accessed without authorisation and it's likely to cause serious harm, you must notify the affected individuals and the OAIC. You need a documented plan before a breach happens — not scrambled together afterwards.

Eight common mistakes

The mistake	Do this instead
Assuming the small-business exemption still applies	Recognise that becoming a reporting entity removes it for AML/CTF data
Having no Privacy Policy at all	Publish a current, plain-English policy people can find
Keeping full ID document copies "just in case"	Record only the minimum verification details needed
No collection notice on forms	Tell people what you collect and why, at the point of collection
Treating privacy as part of AML/CTF	Treat them as two regimes with two regulators
Answering access requests carelessly	Respond without ever revealing a suspicious matter report
Sharing data with portals and CRMs untracked	Keep a register of every third party you share data with
No plan for a data breach	Have a written response plan ready before you need it

Your privacy action plan

Seven steps to get your agency ready

- Appoint a Privacy Officer — the person responsible for privacy in your agency.
- Publish a current Privacy Policy that people can easily find.
- Add a Privacy Collection Notice to your forms and onboarding.
- Stop keeping full ID document copies; record only what you need.
- Put a Data Breach Response Plan in place before you need it.
- Keep a register of every third party you share data with.
- Train your staff — and have them acknowledge their obligations.

Getting it done without starting from scratch

Accessable Risk was founded by a former ASIC leader and Certified Anti-Money Laundering Specialist who understands exactly how the AML/CTF and privacy regimes intersect. Get in touch at enquiries@accessablerisk.com or visit accessablerisk.com to book a free consultation.

Important

This guide is general information, not legal advice. It does not replace the Privacy Act 1988 (Cth), the Australian Privacy Principles, the AML/CTF Act 2006, or OAIC and AUSTRAC guidance. Confirm your specific obligations against the current law and seek professional advice where required.