The Australian Website Compliance Checklist

14 things every Australian small-business website needs in 2026 — in plain English

Australian websites sit under more law than most owners realise: the Privacy Act 1988, the Australian Consumer Law, the Spam Act 2003, the Corporations Act 2001 and the Disability Discrimination Act 1992 all reach into an ordinary business website. None of it requires a lawyer on staff — but it does require knowing what to check. That's this list.

A note on who each law covers: the Australian Consumer Law, Spam Act and Corporations Act apply to essentially every business, no matter how small. The Privacy Act currently applies if your turnover is over $3 million OR you're a health service provider, trade in personal information, handle tax file numbers — or, since 1 July 2026, you're in an AML/CTF-regulated profession (accounting, legal, conveyancing, real estate, high-value dealing). The Government has agreed in principle to remove the $3M exemption entirely, so even currently-exempt businesses are wise to treat the privacy items below as 'when', not 'if'.

> *This checklist is general information, not legal advice. Laws change (several of these did in the last 12 months). For advice on your specific situation, speak to a qualified professional.*

Part 1 — Legal must-haves

☐ 1. An SSL certificate (the padlock / https://)

What it is: A digital certificate that encrypts everything travelling between your visitor's browser and your website — form entries, passwords, payment details. Your address shows https:// instead of http:// and browsers display a padlock.

Why you need it: If you collect any personal information, the Privacy Act's APP 11 requires you to take 'reasonable steps' to protect it — and encrypting data in transit is the floor of reasonable. Beyond the law: Chrome and Safari brand non-SSL sites 'Not secure' in red, and Google ranks them lower.

If you don't: Browsers actively warn your customers away, forms submit customer data readably to anyone on the same network, and if that leads to a breach you've failed the most basic 'reasonable step' a regulator or court would look for. SSL certificates are free (Let's Encrypt) — there is no good excuse.

☐ 2. A privacy policy that actually covers the 13 APPs

What it is: A page explaining what personal information you collect, why, how you store and protect it, who you share it with (including overseas — think Mailchimp, Google, US-hosted tools), how people can access or correct their data, and how to complain. APP 1 of the Privacy Act requires it to be 'clearly expressed and up-to-date' and freely available.

Why you need it: If the Privacy Act covers you (see the note on page 1), this is a direct legal obligation — not a nice-to-have. Even if you're currently exempt, customers, payment providers, insurers and big-business clients increasingly demand one, and every mainstream ad platform (Google, Meta) requires one as a condition of advertising.

If you don't: For covered entities, penalties for serious or repeated privacy interferences now reach the greater of $50 million, three times the benefit gained, or 30% of adjusted turnover. Since June 2025 individuals can also sue directly under the new statutory tort for serious invasions of privacy. For everyone else: no privacy policy means no Google Ads, no Meta ads, and a trust problem on every form you publish.

☐ 3. Collection notices at the point you collect data

What it is: A short notice at or near every form — contact, quote, newsletter, checkout — telling people what you're collecting and why, at the moment you collect it (APP 5). Usually one line plus a link: 'We use your details to respond to your enquiry — see our Privacy Policy.'

Why you need it: The privacy policy is the reference document; APP 5 says people must be notified when collection actually happens. It also just works: forms with a clear one-line explanation convert better because people can see there's no funny business.

If you don't: A privacy policy nobody is pointed to doesn't satisfy notification obligations, and it's one of the first gaps a complaint to the OAIC would surface. Cheap to fix — one sentence per form.

☐ 4. Cookie and tracking disclosure

What it is: Disclosure of the cookies, analytics and advertising pixels running on your site (Google Analytics, Meta Pixel, etc.) — normally a section in your privacy policy, plus a banner if you serve overseas visitors.

Why you need it: Australia has no dedicated cookie-consent law, but tracking data can be personal information, and the Privacy Act's transparency principles (APP 1 and 5) require you to disclose it. If EU or UK residents use your site, the GDPR's consent rules can apply to you regardless of where you're based. Regulator guidance increasingly expects tracking to be spelled out.

If you don't: Undisclosed tracking is exactly the kind of 'unfair' data practice the current wave of Privacy Act reform is aimed at, and it features in OAIC complaints. If you sell to overseas visitors without a consent banner, you're exposed under their rules too.

☐ 5. Website terms and conditions — fair ones

What it is: The rules of using your site and buying from you: what you deliver, payment terms, liability limits, dispute handling, IP ownership. For online stores, also delivery and cancellation terms.

Why you need it: Terms are your contract with every customer — without them, disputes default to whatever a tribunal reconstructs. But they must be fair: the unfair contract terms regime in the Australian Consumer Law now carries direct penalties (it's been illegal — not just void — to include unfair terms in standard-form small-business and consumer contracts since November 2023). One-sided terms copied from a US template are a liability, not protection.

If you don't: No terms: every dispute is decided without your rules on the table. Unfair terms: courts can now impose penalties per unfair term, and ACL penalty ceilings were doubled in March 2026 to up to $100 million for the most serious corporate contraventions. Don't copy-paste from overseas templates — they fail Australian law in predictable ways.

☐ 6. A refund policy that respects consumer guarantees

What it is: A clear statement of when customers get refunds, repairs or replacements. Under the ACL's consumer guarantees, customers are entitled to a remedy when a product or service is faulty, unfit for purpose or not as described — and that right cannot be signed away.

Why you need it: Blanket 'No refunds' statements (or 'no refunds on sale items') are unlawful because they misrepresent rights the customer has regardless of your policy. 'No refunds for change of mind' is generally fine — the distinction matters. The ACCC has prosecuted retailers (Tiger Mist, Fitbit) specifically for misstating refund rights.

If you don't: A 'no refunds' line on your website is a standing ACL breach the ACCC can act on, and any customer who screenshots it wins the argument before it starts. This is one of the most common — and most visible — compliance mistakes on Australian small-business sites.

☐ 7. Your legal identity, visible

What it is: Your legal entity name and ABN (companies: legal company name and ACN/ABN, per sections 153 and 219 of the Corporations Act) plus real contact details — ideally in the footer and on an About or Contact page. A trading name alone is not enough: 'Melbourne's Best Builders' must still show 'Blue Wren Holdings Pty Ltd ABN xx xxx xxx xxx' somewhere official.

Why you need it: Companies are legally required to show their name and ACN/ABN on public documents, and invoices need your ABN regardless of structure. Just as importantly, anonymous websites read as scams — visible identity is the cheapest trust signal you can buy.

If you don't: ASIC can act on companies that don't display required identifiers, and other businesses must withhold 47% of payments to suppliers who won't quote an ABN. Commercially: customers increasingly check ABNs before paying an unfamiliar website. No identity, no sale.

☐ 8. GST-inclusive pricing

What it is: Every price a consumer sees must be the single total price — GST and all unavoidable fees included (section 48 of the ACL). You can show a GST breakdown, but the all-in figure must be at least as prominent.

Why you need it: '$100 + GST' as the headline price to consumers is a breach, full stop (B2B-only quoting is treated differently). This includes pre-ticked extras and mandatory surcharges — the advertised number must be what the card gets charged.

If you don't: The ACCC treats component pricing as misleading conduct: Air Asia was fined $200,000 for exactly this, and ACL penalty ceilings now run to $100 million for serious cases. Practically, surprise fees at checkout are also the #1 documented cause of abandoned carts.

☐ 9. Spam Act-compliant email marketing

What it is: Three rules from the Spam Act 2003 for every marketing email or SMS: (1) consent — the person opted in, or you can genuinely infer consent from an existing relationship; (2) identification — the message clearly says who you are and how to contact you; (3) unsubscribe — a working opt-out honoured within 5 business days. Buying email lists is effectively always a breach.

Why you need it: This applies to every business, any size, from the first email you send. ACMA enforces it actively and doesn't reserve action for big companies.

If you don't: Penalties run to $220,000 per day for a first corporate breach and over $2 million per day for repeat offenders — and ACMA has fined household-name Australian brands millions in recent years, usually for the mundane failures: unsubscribe links that don't work, or emailing people who opted out.

Part 2 — Security and data protection

☐ 10. Secure payment handling

What it is: Taking card payments through a compliant processor (Stripe, Square, PayPal, Shopify Payments) so card numbers never touch your own website or database. The PCI DSS security standard applies to every merchant that accepts cards — it's enforced through your merchant agreement rather than legislation, but it is binding.

Why you need it: Using a hosted payment processor moves almost all PCI burden onto them and is the single biggest security de-risking available to a small online business. Storing card details yourself — even 'temporarily' in emails or spreadsheets — puts you in scope for requirements you cannot realistically meet.

If you don't: A card-data breach means processor fines passed down through your merchant agreement, potential loss of the ability to take card payments at all, and NDB-scheme notification duties if you're Privacy Act-covered. The ACSC puts the average cost of a small-business cyber incident at $56,600.

☐ 11. A data breach response plan

What it is: A one-page plan for the bad day: who you call (IT, lawyer, insurer), how you contain the breach, and your legal clock — Privacy Act-covered entities must assess a suspected eligible breach within 30 days at most, and notify the OAIC and affected individuals as soon as practicable if serious harm is likely.

Why you need it: The Notifiable Data Breaches scheme already binds all Privacy Act-covered entities (that includes every health provider and TFN recipient regardless of size, and AML-covered professions since July 2026). Written plans are the difference between a controlled 48 hours and a chaotic month — the OAIC expects assessment 'much shorter' than 30 days where possible.

If you don't: Failing to assess and notify is itself a Privacy Act breach, separate from the incident — meaning the cover-up (or just the disorganisation) gets penalised on top of the crime. Customers judge you almost entirely on how you handled it, not that it happened.

☐ 12. Software updates and basic security hygiene

What it is: The unglamorous fundamentals: CMS, themes and plugins kept current (most hacked WordPress sites fall to known, already-patched holes); unique passwords and multi-factor authentication on admin, hosting and domain accounts; security headers configured; backups that you've actually tested restoring.

Why you need it: APP 11's 'reasonable steps to protect information' is judged against what's reasonable for your size — and patching, MFA and backups are considered reasonable for everyone. They're also the controls cyber insurers now ask about at application time, and the core of the ACSC's small-business guidance.

If you don't: An unpatched site gets found by automated scanners within days — attackers don't check your revenue before probing your website. Post-breach, 'we hadn't updated since the site was built' is indefensible under APP 11, can void a cyber insurance claim, and Google blacklisting a hacked site takes weeks to undo.

Part 3 — The ones most businesses miss

☐ 13. Accessibility (WCAG)

What it is: Making your site usable by people with disability: readable colour contrast, text alternatives on images, keyboard navigation, properly labelled forms. The benchmark is WCAG 2.2 Level AA — the standard the Australian Human Rights Commission points to under section 24 of the Disability Discrimination Act 1992.

Why you need it: The DDA applies to private businesses, not just government. Providing a service through an inaccessible website can constitute unlawful discrimination — and around 1 in 5 Australians live with disability, so it's also simply a fifth of your market.

If you don't: Complaints go to the AHRC and can escalate to the Federal Court — the precedent dates back to Maguire v SOCOG (2000), and complaint volumes are rising. Accessibility fixes also overlap heavily with SEO and mobile usability, so this item quietly pays for itself.

☐ 14. Automated decision-making and AI disclosure — deadline 10 December 2026

What it is: The newest obligation: Privacy Act amendments passed in December 2024 require privacy policies to disclose any computer programs that make (or substantially assist) decisions significantly affecting individuals — automated quote approvals, AI chatbots that determine outcomes, algorithmic credit or eligibility screening. Covered entities must comply by 10 December 2026.

Why you need it: If your website uses AI or automation in decisions about customers, this needs a privacy-policy section before the deadline. Even businesses not yet covered by the Privacy Act should note it — it signals where regulation is heading as reform continues.

If you don't: Post-deadline, missing ADM disclosure is a straightforward Privacy Act transparency breach — an easy target for regulators wanting demonstrative cases, because checking a privacy policy requires no investigation at all.

Now check your site — free

Most of this list can be verified automatically. AegorIQ's free scan runs the checks — SSL certificate, security headers, privacy policy and terms pages, cookie disclosure, software fingerprint and more — and emails you a free scorecard showing how many findings are Critical, how many Need Attention, and how many pass.

Request your free scan at **aegoriq.com.au** — just your name, email and website address, and your scorecard arrives in your inbox within minutes. The full report identifies each finding and explains exactly how to fix it, in plain English.

For the items a scanner can't check for you (refund policy wording, unfair terms, Spam Act consent records), work through this list with your accountant, lawyer or adviser — or start with the ones marked as heavy penalties above.

Before you launch — and every six months after

Check before you go live: Run a full website security and compliance check before your site launches. Fixing a missing privacy policy, an insecure form or an unlawful 'no refunds' line is quick and quiet before customers and regulators can see it — and far costlier once they can. Treat it as the last item on your pre-launch list.

Re-scan every six months: A site that's compliant today drifts out of compliance. Plugins and themes fall behind, new pages skip the checklist, and the law itself keeps moving — several items on this list changed in just the last 18 months. Re-scan every six months, and after any major change to your site, so nothing quietly slips.

About this checklist: compiled July 2026 from the Privacy Act 1988 (Cth) and OAIC guidance, the Australian Consumer Law (Sch 2, Competition and Consumer Act 2010), the Spam Act 2003 and ACMA guidance, the Corporations Act 2001, the Disability Discrimination Act 1992 and AHRC guidance, and the ACSC Annual Cyber Threat Report 2024–25. It is general information, not legal advice; laws referenced were current at publication and several are amid active reform. AegorIQ — Australian-built website security scanning.