Privacy and consent checklist for marketing

A 28-point check of how your website, tracking, email and ads handle customer information, in line with the Australian Privacy Act and Spam Act.

Marketing runs on customer information: who visited your website, who opened your emails, who bought. Australian privacy law has been tightening, customers expect more control, and browsers are blocking more tracking every year. Getting this right protects your customers and your reputation, and it keeps your marketing numbers accurate.

This checklist is a starting point, not legal advice. If you handle sensitive information or have specific obligations, talk to a privacy lawyer.

How to use it

Tick an item only if you've checked it and it's true. Every unticked item is something to fix or ask your agency or web developer about.

1. Your privacy policy

- [ ] **You have one, and it's easy to find** from every page of your website.
- [ ] **It's in plain English** and explains what you collect, why, and who you share it with.
- [ ] **It names your tools.** It mentions analytics, advertising and email platforms you use, and that some may store information outside Australia.
- [ ] **It says how to ask for access or correction,** and how to complain.
- [ ] **It's up to date.** It was reviewed in the last 12 months, and after any new tool was added.

2. Website tracking and cookies

- [ ] **You know what's on your website.** You have a list of every tracking tag, pixel and script, and who added each one.
- [ ] **Nothing is there by accident.** Old tags from past agencies, tools and campaigns have been removed.
- [ ] **Visitors get a choice** where it matters. If you use a cookie banner, declining is as easy as accepting.
- [ ] **Choices are respected.** When someone declines, the tags that shouldn't run actually stop. You've tested it.

- [ ] **Google and Meta know about consent.** Consent settings are passed to Google (consent mode) and Meta, so their tools behave correctly.
- [ ] **No personal details leak into tracking.** Names, emails and phone numbers don't appear in page addresses or get sent to analytics.
- [ ] **Server-side tracking is set up carefully,** if you use it, so it only sends what you've decided to send.

3. Forms and data collection

- [ ] **You only ask for what you need.** Every form field has a reason.
- [ ] **People know why you're asking.** Forms say what you'll do with the details, with a link to your privacy policy.
- [ ] **Marketing permission is separate.** Agreeing to marketing emails is a separate, unticked box, not bundled into an enquiry or purchase.
- [ ] **Sensitive details are handled with care.** If you collect health, financial or similar information, it's protected and limited to those who need it.

4. Email and SMS

- [ ] **You have permission to send.** Every contact on your list has agreed to hear from you, or there's a clear existing business relationship, as required by the *Spam Act 2003*.
- [ ] **Every message identifies you** and includes a working unsubscribe link.
- [ ] **Unsubscribes are actioned promptly,** within five business days, and across every tool you send from.
- [ ] **Bought or scraped lists aren't used.**

5. Advertising audiences

- [ ] **Customer lists are uploaded securely.** When you upload customer lists to Google, Meta or LinkedIn, the details are encrypted (hashed) first, and only people who've agreed to marketing are included.
- [ ] **Old audiences are cleared out.** Lists and remarketing audiences you no longer use are deleted.
- [ ] **You've thought about sensitive targeting.** You don't target or exclude people based on health, religion, sexuality or similar, even indirectly.

6. Access and suppliers

- [ ] **You know who can see customer data,** in your shop, customer database, email platform, ad accounts and analytics.
- [ ] **Agencies and contractors have only the access they need,** ideally view-only, and it's removed when the work ends.

- [ ] **Two-step sign-in is turned on** for every system that holds customer information.
- [ ] **Suppliers have agreed how they'll handle your data,** in writing.
- [ ] **You know what to do if something goes wrong.** You have a simple plan for a data breach, including when you'd need to notify the Office of the Australian Information Commissioner.

Your score

Count your ticks out of 28.

- **24 or more:** You're well organised. Review this list each year and whenever you add a new tool.
- **15 to 23:** The basics are there, with gaps worth closing soon. Start with sections 2 and 4.
- **Under 15:** There's real risk to your customers and your reputation. Start with sections 1 and 6, then tracking.

Free help

- The Office of the Australian Information Commissioner explains your obligations under the Australian Privacy Principles.
- The ACMA explains the Spam Act rules for email and SMS.
- Our staff cyber security checklist covers the habits your team needs.

Where Blend can help

Our tracking and consent rebuild cleans up your website tracking, sets up consent properly with Google and Meta, and makes sure your marketing numbers stay accurate while respecting your visitors' choices.

This guide is general information, not professional advice for your situation. Read it online and find more free guides at www.blend-datastrategy.com/tools.