



The 10 December 2026 Privacy Act changes: what applies to you

A plain-English guide for Australian small and mid-size businesses

narwhai.com.au · September 2026

Current as at September 2026. This guide summarises law as passed and guidance as published. It is general information, not legal advice, and it is not a substitute for checking your own circumstances.

The short version

Three things are worth knowing. First, from 10 December 2026, businesses that use automated systems to make decisions significantly affecting people must say so in their privacy policy. Second, a Children's Online Privacy Code is due to be registered by the same date, and it catches services children *could* use, not just services aimed at them. Third, several changes are already in force, including a new right for individuals to sue over serious invasions of privacy.

None of this requires a large project for most small businesses. It requires knowing which parts apply to you, and having the documents to show it.

1. Automated decisions have to be disclosed

This is the change with a hard date on it. If your business uses a computer program to make, or substantially help make, a decision that significantly affects someone's rights or interests, your privacy policy must say:

- that those kinds of decisions are made using personal information;
- what kinds of decisions they are; and
- what kinds of personal information are used to make them.

The phrase that trips people up is "significantly affects". It is not about whether the software is clever. It is about the consequence for the person. Some practical examples in a small business setting:

- automated screening that rejects job applicants before a human sees them;
- an eligibility or scoring tool that decides who gets a service, a discount, or credit terms;
- automated fraud or risk checks that block a customer's transaction or account;
- tools that allocate appointments, priority or access on criteria the customer cannot see.

A newsletter tool that segments your mailing list is not this. A tool that decides whether someone is offered a service is.

What to do: list every place software makes or shapes a decision about a person, decide honestly which are significant, and write them into your privacy policy in language a customer can follow. Doing this also tends to surface tools nobody had documented.

2. The Children's Online Privacy Code

A Children's Online Privacy Code is due to be registered by 10 December 2026. It is aimed at services *likely to be accessed by children*, which is broader than services aimed at children.

That distinction matters. A tutoring service, a sports club booking page, a clinic that sees teenagers, or a shop selling to a young market may all be captured without ever marketing to a child. Expect the Code to cover matters such as minimising what you collect from young users, setting privacy-protective defaults, being careful with any tracking or advertising, and writing notices a young person can actually understand.

What to do: decide, and write down, whether children could reasonably use your service. A short documented assessment is worth having on file even where the answer is no. Check the final Code text on the OAIC website when it is registered, because the detail matters here.

3. What has already changed

- **A statutory right to sue.** Individuals can bring an action for serious invasions of privacy, including intrusion into seclusion and misuse of information. This applies regardless of the small business exemption, which makes it the single biggest practical shift for smaller operators.
- **Doxxing offences.** Maliciously publishing someone's personal data is now a criminal offence.
- **Stronger enforcement.** The OAIC has a wider range of penalties available, including tiers for less serious breaches, which makes enforcement more likely rather than less.
- **Security expectations spelled out.** The obligation to protect personal information is expressed in terms of technical and organisational measures, which is language you will recognise from insurance questionnaires.

4. Does the Privacy Act even apply to me?

Businesses with annual turnover of \$3 million or less are currently exempt from the Privacy Act, but the exemption is narrower than most people assume. You are covered regardless of turnover if you:

- provide a health service and hold health information;
- trade in personal information, meaning you buy or sell it;
- are a contracted service provider under a Commonwealth contract;
- are related to a larger entity that is covered; or
- have opted in.

The exemption has also been under review for some time, and it does not apply to the new statutory tort at all. Separately, it gives you nothing when a tender panel, an insurer or an enterprise client asks how you handle personal information. Most businesses that lose work over privacy lose it commercially, not to a regulator.

5. A ten-minute self-check

Answer honestly. Each “no” is a gap worth writing down.

1. Can you list every place your business collects personal information, including forms, bookings, email and paper?
2. Does every one of those collection points tell the person why you are collecting it?
3. Is your privacy policy accurate today, rather than accurate when it was written?
4. Does it name the third-party platforms that receive personal information from you?
5. Does it say whether information goes overseas, and where?
6. Do you have a stated retention period, and do you actually delete on it?
7. Do you know which of your tools make or shape decisions about people?
8. Could children reasonably access your service?
9. If you had a breach on Monday, do you know what you would have to do, and by when?
10. Could you show a client or insurer evidence of all of the above, rather than telling them?

If you answered no more than twice, you are in the same position as most Australian small businesses, and the work to fix it is usually measured in days rather than months.

6. Where the official information is

- Office of the Australian Information Commissioner: **oaic.gov.au**, which publishes the Australian Privacy Principles guidelines and will publish the Children’s Online Privacy Code.
- The amending legislation: *Privacy and Other Legislation Amendment Act 2024*, available at **legislation.gov.au**.
- Notifiable Data Breaches scheme guidance, also on the OAIC site.

Where this guide and the official sources differ, the official sources are right. Commencement dates and code details can change.

Want to know where you actually stand?

NarwhAI runs a free external check on your website or privacy policy and sends you what we find. No obligation.

narwhai.com.au · hello@narwhai.com.au · 0414 270 214

NarwhAI · ABN 12 126 499 242 · Canberra, ACT

This guide is general information, current as at September 2026. It is not legal advice and does not take your circumstances into account. NarwhAI identifies gaps against published standards and provides documentation to support compliance.