Privacy policy

Effective from 11 November 2026

1. About this policy

This policy explains how Automagicae Pty Ltd (ACN 672 194 884, ABN 74 672 194 884), trading as Quantyr ("Quantyr", "we", "us"), handles personal information.

It covers:

- people who visit www.quantyr.com.au, send us an enquiry or book a call with us
- the people we deal with at our clients, suppliers and partners
- personal information we process for our clients when we build, host and support software for them, including our products

In this policy, "our products" means the products that we provide ourselves, such as chartreview.

Some of our products have their own privacy policy. When you use one of those products, its policy applies. If that policy does not deal with something, this policy applies.

PSYCHFINDER is provided by a separate company, Psychfinder Pty Ltd (ACN 680 668 624). We grant Psychfinder Pty Ltd an exclusive licence to provide the PSYCHFINDER software in Australia. We also build, host and support PSYCHFINDER for Psychfinder Pty Ltd as its service provider (section 3.5). Psychfinder Pty Ltd is responsible for how PSYCHFINDER handles personal information. Its privacy policy is at www.psychfinder.com.au/privacy.

Our website and services are for businesses and other organisations. They are not directed at children.

We handle personal information in line with the Australian Privacy Principles (APPs) in Schedule 1 to the Privacy Act 1988 (Cth).

Personal information is information or an opinion about an individual who is identified, or who is reasonably identifiable.

2. The short version

- We collect only what we need to reply to you, hold a call with you or deliver work for a client.
- This website uses no analytics, advertising or tracking cookies.
- We do not sell personal information or use it for advertising.
- We do not use client data for our own purposes, including to train AI models.
- Enquiries, bookings and emails are stored by our service providers, mainly in the United States (section 7). Client project data is stored in Australia by default (section 5).
- We do not use computer programs to make decisions that significantly affect people. When a client uses our software in its own decisions, the client's privacy policy covers this (section 8).
- You can ask to see, correct or delete the personal information we hold about you (section 11).

3. What we collect and how

You can ask us a general question without giving your name, or by using a different name. To reply to an enquiry, hold a call or work with you, we need your name and contact details.

3.1 When you visit our website

- We do not use analytics, advertising, tracking pixels or tracking cookies.
- Our host, Cloudflare, processes technical information to deliver the website and protect it from attacks. This includes your IP address, browser and device details and the pages you request.

- Cloudflare may place a short-lived security cookie on your device to detect automated traffic. This cookie is strictly necessary. It does not track you across websites.
- If you choose a light or dark theme, your browser stores that choice on your device. It is not sent to us.
- So you can book a call, every page loads a booking script from Cal.com, our booking service. Your browser then contacts Cal.com, which receives your IP address and browser and device details (Cal.com privacy policy). When you open the booking calendar, Cal.com also receives the address of the page you are on, including anything after the "?" in it, such as a campaign name. The script stores nothing on your device for our website. Cal.com's own security service may set a short-lived security cookie (`__cf_bm`) for cal.com. We do not receive it.
- Our website code records the outcome of each enquiry and booking it handles, so we can fix problems. These logs are deleted within 7 days.

3.2 When you send an enquiry

Our enquiry form collects your name and email address. It also collects your organisation, phone number and sector if you give them, your message and the product or service you asked about. We use this information to reply to you. We record your enquiry in our customer relationship system, Attio.

Before a form is sent, Cloudflare Turnstile checks that it comes from a person and not an automated program. Cloudflare says Turnstile uses technical signals such as your IP address, browser details, connection details and the website you are on. Turnstile does not receive what you type into the form. Cloudflare also uses these signals to improve Turnstile, as its Turnstile Privacy Addendum explains. We have not turned on the Turnstile setting that places a cookie.

If the check fails, the form is not sent. We then show you how to email us or book a call instead.

Please do not put health information, or details about your patients or clients, in the form. If you do, we use it only to reply to you. We delete it when you ask or when we no longer need it.

3.3 When you book a call

Calls are booked through Cal.com. Cal.com collects your name, email address and the time you choose. It sends you a confirmation and adds the call to our calendar, which is hosted by Fastmail. Calls take place on Cal Video, which runs on Daily. We do not record or transcribe calls.

When you book, reschedule, cancel or miss a call, Cal.com tells our website. Our website records this in Attio. After a call we may add notes, such as your organisation and what we discussed.

3.4 When you email us or work with us

Our email is hosted by Fastmail. For clients, suppliers and partners, we keep names, business contact details, roles, correspondence, proposals, contracts and invoices. We keep invoices and payment records in our accounting system, Xero.

3.5 Information we process for our clients

When we build, host or support software for a client, or a client uses one of our products, we may handle personal information that the client is responsible for. Depending on the work, this can include customer, patient or claim records. It can also include sensitive information such as health information.

In this work we act as a service provider to the client:

- We use the information only to deliver the services the client engaged us for. We follow our agreement with the client and its instructions.
- We do not use it for our own purposes, including to train AI models, unless the client agrees in writing.
- We protect it as section 9 describes and as our agreement with the client sets out.
- The client decides what is collected and why. The client's own privacy policy explains this.
- If you want to see, correct or ask about information that one of our clients holds, contact that organisation. We help them respond.

4. How we use personal information

We use personal information to:

- reply to enquiries, hold calls and prepare proposals
- deliver, host and support client work and our products
- run our business, including invoicing, record keeping and meeting our legal obligations
- keep our website and systems secure, including checking for spam

We use personal information for another purpose only if you agree or the law allows it.

We send marketing emails only to people who ask to receive them. Each marketing email tells you how to unsubscribe. We do not sell personal information or share it for advertising.

5. Where client project data is stored

Client project data is stored and processed in Australia by default. We store it on virtual servers in Brisbane that we rent from BinaryLane and manage ourselves, with Supabase in its Sydney region or in the client's own cloud environment in Australia.

We use a service that stores or processes client project data outside Australia, including an artificial intelligence (AI) model provider, only when the client agrees in writing. Our agreement with the client records the provider and where it operates.

Our software is designed for people at the client to review AI outputs before they act on them. Our terms of service require this.

6. Who we share personal information with

We use these service providers to run our business and the client systems we host. Each one processes personal information for us under its own terms and security commitments.

Provider	What we use it for	Where the data is stored
Attio	Customer relationship system: enquiries, bookings, client contacts	Attio Ltd is a United Kingdom company on Google Cloud; its sub-processors are in the United Kingdom, Ireland and the United States
BinaryLane	Virtual servers for the client systems we host	Australia (Brisbane)
Cal.com	Booking calls	United States
Daily	Video for calls booked through Cal.com (Cal Video)	United States; live calls may pass through servers in other countries
Cloudflare	Website hosting and security, the Turnstile spam check, website logs	United States and Europe, with servers worldwide, including in Australia
Fastmail	Email and calendar	United States
Resend	Notifications and automatic emails sent by our systems	United States
Supabase	Databases for client systems and our products	Australia (Sydney)
Xero	Accounting and invoicing	United States

We also use everyday business tools for project tracking, team chat, code hosting and AI assistants. These providers are based mainly in the United States. They may hold names and business contact details. We do not keep client project data in them.

We may also share personal information with:

- our professional advisers, such as our accountant, lawyer or insurer
- a buyer of our business or its assets, under a confidentiality agreement
- government authorities, when the law requires it

7. Disclosure outside Australia

Several providers in section 6 store enquiries, bookings, emails, business records and website data outside Australia. The main country is the United States. Some data is also stored in the United Kingdom or in European Union countries. Cloudflare processes data at servers in many countries, including Australia.

We choose providers that publish data processing terms and security commitments. We send them only what they need.

We remain accountable under the Privacy Act for how these providers handle personal information we disclose to them.

8. Decisions made by computer programs

APPs 1.7 to 1.9 apply from 10 December 2026. They require a privacy policy to explain where an organisation has arranged for a computer program to use personal information to make a decision, or to do a thing substantially and directly related to making a decision, that could reasonably be expected to significantly affect an individual's rights or interests.

8.1 Decisions in our own business

We do not arrange for computer programs to make decisions like this, or to do things substantially and directly related to making them, about the people whose information we hold for our own business.

For transparency, these are the automated steps in our own business. None of them decides anything that significantly affects anyone:

- **The spam check.** Turnstile decides whether a form submission is sent, using the technical information described in section 3.2. If it fails, you can email us or book a call instead.
- **Recording enquiries and bookings.** Our website code adds enquiries and bookings to Attio. It creates reminders for us to reply or follow up. It does not score, rank or reject anyone.

8.2 Software we provide to clients

Some of our software reads, sorts, summarises or flags information, such as medical records, claim documents or intake forms. A client may use these outputs when it makes decisions about individuals.

When a client does this, the client is the organisation that has arranged for the computer program to be used. The client's privacy policy describes those decisions. We give each client a plain description of the kinds of personal information our software uses and the outputs it produces. This helps the client describe its use accurately.

Our guide Your privacy policy now has to name your automated decisions explains the requirement in more detail.

9. How we protect personal information

We take reasonable steps to protect personal information from misuse, interference, loss and unauthorised access, change or disclosure. These include:

- encryption in transit and at rest with our service providers
- access limited to the people who need it, with multi-factor authentication on our accounts
- secrets, such as access keys, stored encrypted and never in our code
- a written process for responding to suspected data breaches
- for client systems, the access controls, audit logs and data location agreed with each client

10. How long we keep personal information

- **Enquiries and bookings that do not lead to work:** deleted from Attio and Cal.com within 2 years of our last contact.
- **Client and supplier records:** kept for 7 years after the work ends, to meet our obligations under the Corporations Act 2001 (Cth) and tax law.
- **Website logs:** deleted within 7 days. Cloudflare keeps its own network logs under its privacy policy.

- **Client project data:** kept, returned or deleted as our agreement with the client sets out.

When we no longer need personal information and the law does not require us to keep it, we delete it or de-identify it.

11. Seeing, correcting or deleting your information

You can ask for a copy of the personal information we hold about you. You can also ask us to correct it or delete it. Email privacy@quantyr.com.au. We may need to confirm who you are first.

We respond within 30 days and do not charge for this. If we cannot do what you ask, for example because the law requires us to keep a record, we tell you why in writing. We also tell you how you can complain.

If we correct information that we gave to someone else, we tell them about the correction if you ask us to.

For information we process for one of our clients, contact that organisation first (section 3.5).

12. Complaints

If you think we have mishandled your personal information, email privacy@quantyr.com.au. We acknowledge complaints within 5 business days and aim to resolve them within 30 days.

If you are not satisfied with our response, you can complain to the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au or on 1300 363 992.

13. Data breaches

We follow the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act. If we suspect a data breach, we act to contain it. We assess it promptly and within

30 days. If it is likely to result in serious harm, we notify the people affected and the OAIC as soon as practicable.

If a breach involves information we process for a client, we tell the client promptly, or within any shorter time our agreement sets. We then help the client meet its obligations.

14. Changes to this policy

We update this policy when our practices or the law change. The date at the top shows when the current version took effect. If a change materially affects how we handle client data, we tell affected clients in writing.

15. Contact us

Our privacy officer is one of our directors. For privacy questions, requests or complaints, email privacy@quantyr.com.au.