Privacy Policy

Automagicae Pty Ltd

Trading as Automagicae

Effective date: [date]

Last updated: [date]

---

1. About This Policy

This Privacy Policy explains how Automagicae Pty Ltd ("Automagicae", "we", "us", or "our") collects, holds, uses, and discloses personal information. We are committed to protecting the privacy of all individuals whose information we handle.

Automagicae is an Australian Privacy Principle (APP) entity under section 6D(4) of the Privacy Act 1988 (Cth). We comply with the Australian Privacy Principles set out in Schedule 1 of the Privacy Act, as amended by the Privacy and Other Legislation Amendment Act 2024 (Cth).

This policy applies to all personal information handled by Automagicae, whether collected directly from individuals, received from clients on whose behalf we process data, or generated through our AI-assisted products.

2. What We Do

Automagicae develops AI-assisted software products for healthcare providers. Our products process personal information, including sensitive health information, on behalf of our clients. We operate as a service provider (data processor) under each client's instruction.

Our products are decision-support tools. All AI-generated outputs are subject to mandatory human review by qualified professionals before they inform any clinical, administrative, or claims decision. No AI output reaches an individual without prior human review.

3. Kinds of Personal Information We Handle

Depending on the engagement, we may handle the following kinds of personal information on behalf of our clients:

- Names, dates of birth, addresses, and contact details.
- Government-issued identification numbers (such as DVA file numbers or Medicare numbers).
- Health information, including medical records, clinical notes, pathology reports, imaging reports, and other health-related documents.
- Military service records, where relevant to the client's services.
- Information generated by our AI-assisted processing, including structured text extractions, condition assessments, and evidence summaries.

We process this information solely for the purposes specified in our agreements with the client.

4. How We Collect Personal Information

4.1 From clients

The primary way we receive personal information is from our clients, who provide records and documents for processing through our products. Automagicae does not have a direct relationship with the individuals whose information it processes. We receive personal information solely through our clients, under the terms of the Data Sharing Agreement governing each engagement.

Our clients are responsible for obtaining all necessary consents from individuals before sharing their information with Automagicae for processing. This includes consent for AI-assisted processing, as described in Section 5 below.

4.2 Generated through processing

Our AI-assisted products generate new information from the records provided (such as structured text extractions, condition assessments, and evidence summaries). Under the Australian Privacy Principles, AI-generated or inferred personal information constitutes "collection" under APP 3 (OAIC, Guidance on Privacy and Developing and Training Generative AI Models, October 2024). We treat all such information as personal information subject to the APPs.

4.3 Directly from individuals

We do not typically collect personal information directly from individuals. If we do (for example, through our website contact form or in correspondence), we will notify you at the time of collection of the purposes for which we are collecting it.

4.4 Website visitors

Our website may collect standard web analytics data (such as IP addresses, browser type, and pages visited) through cookies or similar technologies. This data is used solely for website improvement and is not linked to individual health records or client data.

5. Consent Responsibility

5.1 Client responsibility

Automagicae operates as a service provider processing personal information under the client's instruction. The responsibility for obtaining valid, informed consent from individuals whose information is processed through our products sits with the client, not with Automagicae.

Our clients are health service providers with direct relationships with their patients, veterans, or clients. They collect personal information under their own consent frameworks and provide it to Automagicae for processing. We rely on our clients having obtained appropriate consent before sharing information with us.

Under the Privacy Act 1988, consent for the collection and use of sensitive information (including health information) must be informed, voluntary, current, and specific (APP 3.3; OAIC APP Guidelines, Chapter B). Our clients are responsible for ensuring their consent processes meet these requirements in respect of the information they share with Automagicae.

5.2 How Automagicae supports client consent

Although consent is the client's responsibility, we actively support our clients in meeting their obligations:

- We provide template consent language covering AI-assisted processing, human-in-the-loop safeguards, de-identified data use, and the involvement of contracted service providers. Clients may adapt this language for their own consent forms.
- We provide descriptions of our processing activities, infrastructure, and safeguards for inclusion in client privacy policies and consent materials.
- Where a client's consent form includes an optional opt-in for the use of de-identified data in AI improvement (corresponding to the Tier 2 licence in the Data Sharing Agreement), we respect the individual's election as communicated to us by the client.

5.3 Individuals who wish to exercise their rights

Because Automagicae does not have a direct relationship with the individuals whose information it processes, individuals wishing to exercise their privacy rights (including withdrawing consent, requesting access or correction, or opting out of AI processing) should contact their healthcare provider directly. The client will communicate any relevant changes to Automagicae.

If Automagicae collects personal information directly from individuals in the future (for example, through a direct-to-consumer product), we will obtain consent directly and update this policy accordingly.

6. How We Use Personal Information

We use personal information only for the purposes for which it was collected, or for directly related purposes that the individual would reasonably expect (APP 6.1 and 6.2). In practice, this means:

- Processing records and documents on behalf of the client for the contracted service (such as medical chart review, condition identification, or evidence matching).
- Providing AI-assisted analysis and decision-support outputs to the client's qualified professionals.
- Supporting the client's clinical, administrative, or claims processes.
- Improving and maintaining our products (using de-identified data only, where a licence has been granted by the client under the Data Sharing Agreement).

We do not use identifiable personal information for marketing, profiling, or any purpose unrelated to the contracted service.

7. AI-Assisted Processing

7.1 How our AI works

Our products use a two-layer processing architecture designed to protect personal information:

In the first layer, scanned documents are read by self-hosted AI models running on controlled infrastructure. The models extract text from scanned pages, including handwritten and printed content. An automated de-identification step then removes personal identifiers from the extracted text.

In the second layer, de-identified text is analysed by AI models for the contracted purpose. Because reasonable de-identification steps have been taken, the data processed in this layer is no longer reasonably identifiable.

Identifiable data is never sent to a third-party API. De-identified data may be processed via third-party services that operate under zero-data-retention terms.

7.2 De-identification

We take reasonable steps to de-identify personal information before it is processed in the second layer. Given the variety of document formats we process (including handwritten clinical notes), complete de-identification cannot be guaranteed in all cases. Residual identifiers may occasionally survive automated stripping. This residual risk is mitigated by the zero-data-retention and contractual protections required of any third-party provider.

7.3 Human oversight

All AI-generated outputs are reviewed by qualified human professionals before they inform any decision. Our products are decision-support tools, not autonomous decision-making systems. Individuals retain the right to request human review of any AI-assisted decision through their healthcare provider.

8. Automated Decision-Making Transparency

From 10 December 2026, the Privacy Act requires APP entities to include information about automated decision-making in their privacy policies (APPs 1.7 to 1.9, introduced by the Privacy and Other Legislation Amendment Act 2024).

Automagicae's products:

- Use AI to assist in the analysis of health records and related documents. This includes text extraction from scanned documents, condition identification, evidence matching, and generation of structured summaries.
- Support decisions that may significantly affect individuals' rights or interests, including in relation to healthcare and compensation claims.
- Do not make decisions autonomously. All AI outputs are subject to mandatory review by qualified human professionals before they inform any decision affecting an individual.

The personal information used in AI-assisted processing includes health records, clinical notes, and other documents provided by the client. The specific types of information processed depend on the engagement.

We work with our clients to ensure their privacy policies accurately describe the AI-assisted processing performed on their behalf. This section will be updated as the regulatory requirements take effect.

9. Disclosure of Personal Information

We do not sell, rent, or trade personal information. We may disclose personal information in the following limited circumstances:

- To the client on whose behalf we are processing the information (this is a return of the client's own data, not a disclosure to a third party).
- To infrastructure providers who supply computing resources under an infrastructure-as-a-service

model, where the provider does not access data content. Under the OAIC's effective control test (APP Guidelines, Chapter B: Key Concepts), this constitutes "use" rather than "disclosure" because the provider supplies hardware while Automagicae controls the data.
- To third-party API providers, but only after de-identification and only under zero-data-retention terms.
- Where required or authorised by law, including in response to a court order or lawful request by a regulatory body.

10. Cross-Border Disclosure

Identifiable personal information is processed exclusively on infrastructure located in Australia or the Oceania region (APP 8). We do not disclose identifiable personal information overseas.

De-identified data may be processed via third-party API providers located outside Australia, under zero-data-retention terms. Because reasonable de-identification steps have been taken, this data is no longer reasonably identifiable, and the APP 8 obligations applicable to personal information are substantially mitigated.

Automagicae's own operational infrastructure is hosted entirely within Australia (BinaryLane, Brisbane, in ISO 27001-certified NextDC data centre facilities).

11. Security

We take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification, or disclosure, consistent with APP 11 (as amended by APP 11.3 under the Tranche 1 reforms). Our measures include:

- Encryption in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent) for all identifiable data.
- Container isolation for all AI processing workloads.
- Role-based access control limiting access to authorised personnel for specified purposes.
- Selection of infrastructure providers with SOC 2 Type II certification or equivalent independent security audits.
- Automated de-identification at the boundary between identifiable and de-identified processing.
- Regular review of provider compliance and security certifications.

12. Data Retention

We retain personal information only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. Specific retention terms are set out in the Data Sharing Agreement with each client. In general:

- Identifiable data is held for the duration of the client engagement and returned or securely destroyed on termination at the client's direction.
- De-identified derivatives may be retained by Automagicae under a licence from the client, for product improvement, model evaluation, and quality assurance purposes. This licence is revocable by the client.
- Operational data (processing metrics, system logs) that contains no personal information is retained at our discretion.

13. Access and Correction

Under the Australian Privacy Principles, individuals have the right to request access to their personal information (APP 12) and to request correction of inaccurate information (APP 13).

Because Automagicae processes personal information on behalf of clients, access and correction requests should be directed to the relevant client (your healthcare provider). We will cooperate with clients to respond to access and correction requests.

If you believe we hold personal information about you directly (for example, from correspondence with us), you may contact us using the details in Section 17 to request access or correction.

14. Complaints

If you believe we have handled your personal information in a way that breaches the Australian Privacy Principles, you may lodge a complaint with us using the contact details in Section 17. We will acknowledge your complaint within five business days and aim to resolve it within 30 days.

If you are not satisfied with our response, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au or by calling 1300 363 992.

15. Data Breach Notification

In the event of a data breach involving personal information, we will comply with Part IIIC of the Privacy Act (Notifiable Data Breaches scheme). We will notify the affected client as soon as practicable, cooperate with the client's breach assessment, and support the client in meeting its notification obligations to the OAIC and affected individuals.

16. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, products, or legal obligations. Material changes will be published on our website. We encourage you to review this policy periodically.

17. Contact Us

If you have questions about this Privacy Policy, wish to make a complaint, or want to exercise your privacy rights, please contact us:

Privacy contact: privacy@automagicae.com

Website: automagicae.com