

Privacy Policy

M2 Technology Group Pty Ltd (ABN 24 061 357 373)

Effective: 1 July 2026

M2 Technology Group Pty Ltd (“M2 Technology”, “we”, “us”, “our”) is committed to protecting your privacy and safeguarding the information we hold. This policy explains what Personal Information we collect, how we collect, use, disclose, store, secure and dispose of it, and how you can access or correct your information or make a complaint.

We are bound by the Commonwealth Privacy Act 1988 (Cth) (“Privacy Act”), including the Australian Privacy Principles (“APPs”) contained in it. A copy of the APPs is available from the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.

This policy applies to Personal Information collected through our own business activities, our website, and through our CommTrak platform. Section 6 below deals specifically with CommTrak, which involves an additional layer of responsibility because our customers use CommTrak to store information about their own clients.

This policy is a public document, published in accordance with APP 1 (open and transparent management of Personal Information).

1.0 Definitions

- **“Collect”** means gather, acquire or obtain, by any means, information about an individual who is identified or reasonably identifiable.
- **“CommTrak”** means M2 Technology’s cloud-based customer relationship management (CRM) software-as-a-service product.
- **“CommTrak Customer”** means a business or organisation that has a subscription to use CommTrak.
- **“Direct Marketing”** means the marketing of goods or services by written, verbal, electronic (including email and SMS) or other means of communication.
- **“Disclose”, “Disclosure” and “Disclosed”** generally mean the release of information outside M2 Technology.
- **“Individual”** means a natural person. Where this policy refers to information about a company or other legal entity, different obligations under the Privacy Act may apply; we nonetheless aim to handle that information consistently with this policy.
- **“Opt Out”** means an individual’s expressed request not to receive further Direct Marketing.
- **“Personal Information”** means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether it is recorded in a material form or not.
- **“Primary Purpose”** is the main reason information is collected in a particular transaction.
- **“Privacy Act”** means the Commonwealth Privacy Act 1988 (Cth), including the Australian Privacy Principles.
- **“Sensitive Information”** has the meaning given in the Privacy Act and includes information such as health information, racial or ethnic origin, and criminal record.

- **“Use” and “Used”** mean the handling of Personal Information within M2 Technology.

Note: Providing us with Personal Information does not, by itself, amount to blanket consent to any and all uses of that information. We only use and disclose Personal Information for the purposes described in this policy, for a directly related secondary purpose you would reasonably expect, with your consent, or where otherwise required or authorised by law.

2.0 What Personal Information We Collect

The type of information we collect depends on the nature of our dealings with you. It may include:

- Name, contact details (address, email, phone number) and job title
- Billing, invoicing and payment details
- CRM records we hold about you as our customer or contact, including correspondence and notes
- Emails and email attachments sent to or received by us
- Support tickets and related communications
- Electronic signature records, including signed documents, timestamps and audit trails (see section 7)
- IP addresses, login credentials and authentication data, and usage or activity logs
- Website analytics data (such as pages visited and general browsing behaviour)
- Information provided when you contact us, subscribe to communications, or interact with our website or products

Where you are a CommTrak Customer, or a user acting on behalf of a CommTrak Customer, we also collect the information described in section 6 below.

2.1 How we collect it

We collect Personal Information only by lawful and fair means. Where practicable, we collect Personal Information directly from you — for example, when you complete a form, correspond with us by email or phone, or use our website or products, or otherwise deal with us directly.

Separately, CommTrak Customers enter information about their own clients and contacts into CommTrak. In that situation, it is the CommTrak Customer — not M2 Technology — who collects that information and who is responsible for telling those individuals how their information will be handled. M2 Technology’s role in relation to that data is described in section 4 below.

Where it is not practicable to notify you of the matters below before collecting your Personal Information, we will notify you as soon as practicable afterwards. Those matters are:

- The purpose for which we are collecting the information;
- Our identity and how to contact us;
- That you can access and seek correction of the Personal Information we hold about you;
- The types of organisations to which we usually disclose that kind of Personal Information;

- Any law that requires the particular information to be collected; and
- The consequences, if any, if the information is not provided.

3.0 Use and Disclosure of Personal Information

We use Personal Information primarily to provide our products and services to you, including CommTrak and related support, and to manage our agreements with you (including electronic signing of those agreements — see section 5). We also use it for:

- billing and account management;
- business planning and product development;
- direct marketing (see section 8); and
- providing information about our promotions, products and services, and those of related M2 Technology businesses.

We may disclose Personal Information:

- to our service providers who help us deliver our products (for example, cloud hosting, email, electronic signature and SMS providers — see section 9);
- to third parties where you have consented to the disclosure;
- where required or authorised by law; or
- to avoid an imminent threat to a person's life, health or safety, or in connection with a suspected unlawful activity or investigation.

Sensitive Information is only used or disclosed for the primary purpose it was collected, a directly related secondary purpose you would reasonably expect, with your consent, or where required or authorised by law.

We do not sell or share our customer lists on a commercial basis with third parties. If this were ever to occur, we would only do so with the appropriate consent of the individuals involved.

4.0 CommTrak — How We Handle Customer Data

CommTrak is our cloud-based CRM product. CommTrak Customers use it to store and manage information about their own clients and contacts ("CommTrak Data"). This section explains how M2 Technology handles CommTrak Data. It applies in addition to, and alongside, our arrangements with individual CommTrak Customers (including any subscription or data-processing terms agreed between us).

Who is responsible for what: CommTrak Customers decide what information to enter into CommTrak about their own clients and contacts, and are responsible for collecting it lawfully and telling those individuals how their information will be handled (including that it is stored in CommTrak). M2 Technology hosts and processes CommTrak Data on behalf of CommTrak Customers, to provide and support the CommTrak platform, and does not independently collect, use or disclose CommTrak Data for its own separate purposes.

If you are an individual who believes your information has been entered into CommTrak and want to know more about how it is being used, please contact the relevant CommTrak Customer directly — see section 4.4 below for how access, correction and deletion requests are handled.

4.1 Hosting

CommTrak is hosted on Amazon Web Services (AWS) infrastructure located in Australia. We also maintain a backup copy of CommTrak Data on our own servers located at a NextDC data centre in Australia.

4.2 Access by M2 Technology staff

M2 Technology staff may access CommTrak Data where reasonably necessary to provide technical support, troubleshoot issues, maintain or improve the CommTrak platform, or ensure the security of the service. Access is restricted to authorised personnel and is limited to what is necessary for these purposes. We do not access CommTrak Data to view, use or disclose it for any other purpose.

4.3 Security

We apply technical and organisational security measures to protect CommTrak Data from misuse, loss, and unauthorised access, modification or disclosure. These measures include restricted access controls, secure hosting infrastructure, and regular backups. Further detail is set out in section 10 (Data Security and Data Breaches).

4.4 Retention and deletion of CommTrak Data

While a CommTrak Customer's subscription is active, CommTrak Data is retained to enable the ongoing operation of the service.

When a CommTrak Customer's subscription ends or is cancelled, they are given the opportunity to export and download their CommTrak Data. After that point, CommTrak Data is deleted. Backup copies are kept in accordance with our Retention Policy and then removed in the ordinary course of our backup cycle following deletion of the primary data.

If you are an individual whose information has been entered into CommTrak by a CommTrak Customer (rather than a CommTrak Customer yourself), requests to access, correct or delete that information should generally be directed to the relevant CommTrak Customer in the first instance, as they control the collection and content of that data. We will assist CommTrak Customers to respond to such requests where reasonably required.

5.0 Electronic Signatures

Electronic signatures are used in two different ways in our business, described separately below.

5.1 Agreements between M2 Technology and our customers

When we ask you to sign an agreement with M2 Technology (for example, a services agreement), we use a third-party electronic signature provider — currently **PandaDoc** (having previously used DocuSign) — to manage that signing process.

In doing so, we collect and hold signature-related information, including signature images and signed documents, date and time stamps, the signer's name, email address and IP address, and authentication and audit trail records confirming how and when the document was signed. This information is used to create a reliable record of the signing process, verify the authenticity of the signed document, and meet our legal and contractual obligations. It is retained for as long as reasonably necessary to preserve the integrity and enforceability of the document (see section 11).

5.2 CommTrak's built-in signing feature

CommTrak includes a built-in electronic signature feature, developed by M2 Technology, which CommTrak Customers can use to send documents such as quotes to their own clients for signing. This is a feature of the CommTrak platform, not a separate signing service offered by M2 Technology directly to those clients.

Signature-related information generated through this feature (signature images, signed documents, timestamps, IP addresses and audit trail records) forms part of CommTrak Data. It is collected by the CommTrak Customer sending the document, and is hosted and processed by M2 Technology on the CommTrak Customer's behalf, consistent with section 4 above.

6.0 Direct Marketing

If we conduct Direct Marketing (by email, SMS or telephone), we will:

- only do so where you would reasonably expect it, where you have consented, or as otherwise permitted under the Privacy Act;
- clearly notify you of a simple way to Opt Out (for example, an unsubscribe link in emails, or by contacting us directly);
- process Opt Out requests promptly; and
- not contact you for Direct Marketing purposes after you have Opted Out, unless you later ask us to resume.

You may unsubscribe from our marketing communications at any time by using the unsubscribe function in the relevant communication, or by contacting us using the details in section 15.

7.0 Overseas Disclosure of Personal Information

Some of the third-party service providers we use to run our business and deliver CommTrak store or process Personal Information overseas, or are part of international groups even where the immediate service is based in Australia. These currently include:

- **Amazon Web Services (AWS)** — CommTrak is hosted on AWS infrastructure located in Australia (Sydney region).
- **Microsoft 365** — used for our business email and related productivity tools. Microsoft is a United States-based provider and may store or process some data overseas as part of its global infrastructure.
- **PandaDoc** — our current electronic signature provider for agreements between M2 Technology and our customers (see section 5.1), headquartered in San Francisco, California, USA.
- **SMS Central** — our SMS provider, based in Melbourne, Australia, and owned by 26 Engage, an international messaging group.
- **Dricko Ltd, trading as Symberity** — our search engine optimisation (SEO) provider, based in Cork, Ireland.

We only disclose Personal Information to an overseas recipient where: you have consented to the disclosure; the disclosure is necessary for the performance of a contract with you; the disclosure is necessary for a contract in your interest between us and a third party; or the

disclosure is for your benefit and it is impracticable to obtain your consent beforehand (and you would be likely to give it if asked). Where practicable, we take reasonable steps to ensure our overseas providers handle Personal Information consistently with the Australian Privacy Principles, including through the provider's own privacy and security terms.

8.0 Data Security and Data Breaches

We take reasonable technical and organisational steps to protect the Personal Information we hold from misuse, interference, loss, and unauthorised access, modification or disclosure. These steps include:

- restricting access to Personal Information to personnel who need it to perform their role;
- secure storage of electronic records, including cloud hosting with access controls and regular backups;
- requiring staff and contractors to handle Personal Information consistently with our privacy obligations; and
- regularly reviewing our information security practices.

If we experience a data breach that is likely to result in serious harm to affected individuals (an "eligible data breach"), we will comply with our obligations under the Notifiable Data Breaches scheme in the Privacy Act. This includes investigating the breach, taking steps to contain and remediate it, and notifying affected individuals and the OAIC where required.

We take reasonable steps to destroy or permanently de-identify Personal Information once it is no longer needed for any purpose for which it may be used or disclosed under this policy, unless we are otherwise required or authorised by law to retain it.

9.0 Retention and Deletion

Unless a longer period applies by law or is otherwise stated in this policy, we generally retain information as follows:

- **Tax records** — retained for at least 5 years, consistent with Australian Taxation Office record-keeping requirements.
- **Other financial records (e.g. billing and invoicing records)** — retained for at least 7 years.
- **CRM records, correspondence and support tickets** — retained for the duration of our relationship with you, and for a reasonable period afterwards (for example, up to 7 years) to meet legal, accounting or dispute-resolution needs.
- **Electronic signature records and signed documents** — retained for as long as reasonably necessary to preserve the enforceability of the relevant document, and consistent with our obligations under any applicable electronic transactions legislation.
- **CommTrak Data** — see section 4.4 above.
- **Website analytics data** — retained in accordance with the relevant analytics provider's standard retention settings.

Where Personal Information is no longer needed for any authorised purpose, we take reasonable steps to securely destroy or permanently de-identify it, including in backup systems as part of our normal backup cycle.

10.0 Information Quality

We take reasonable steps to ensure that the Personal Information we collect, use and disclose is accurate, complete and up to date, having regard to the purpose for which it is used.

11.0 Access and Correction

You may request access to the Personal Information we hold about you, or ask us to correct it, at any time. Requests should be made in writing to our Privacy Officer using the contact details in section 15.

We will respond to access and correction requests in accordance with the Privacy Act. We may charge a reasonable administrative fee for providing a copy of your Personal Information (but not for making the request itself). If we refuse a request for access or correction, we will provide our reasons and explain how you may complain about the refusal.

12.0 Anonymous Transactions and Pseudonymity

Where it is lawful and practicable to do so, we will give you the option of not identifying yourself, or of using a pseudonym, when dealing with us. We do not require visitors to our website to provide Personal Information simply to browse it.

13.0 Complaints

If you have a concern or complaint about how we have handled your Personal Information, please contact our Privacy Officer in writing at privacy@m2technology.com.au, or using the other contact details in section 15.

We will acknowledge your complaint, investigate it, and aim to respond within a reasonable time. If you are not satisfied with our response, you have the right to lodge a complaint with the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.

14.0 Changes to This Policy

We may update this policy from time to time to reflect changes in our practices, technology, legal requirements, or the products and services we offer. The current version will always be available on our website. We encourage you to review it periodically.

15.0 Contact Us

If you have any questions about this Privacy Policy, or wish to make an access, correction or complaint request, please contact our Privacy Officer:

- **Email:** privacy@m2technology.com.au
- **Telephone:** +61 8 9315 0000
- **Post:** PO Box 588, Applecross WA 6953

- **Website:** www.m2technology.com.au