



Privacy Statement

Last updated 21 September 2018

This statement applies across all websites that we own and operate and all services we provide, including our online and mobile apps, and any other apps or services we may offer e.g. training and deployment. For the purpose of this statement, we will call them our 'services'.

When we say 'personal data' we mean identifiable information about you, like your name, email, address, telephone number, bank account details, payment information, support queries, community comments and so on. If you can't be identified (for example, when personal data has been aggregated and anonymised) then this statement doesn't apply. Check out our terms of use for more information on how we treat your other data.

From time to time we may need to update this statement. Where a change is significant, we will inform you – usually by sending you an email.

You can read the whole statement below, or if you haven't got much time, you can jump to the section you need using the navigation menu.

1. Who are 'we'?

When we refer to 'we' (or 'our' or 'us'), that means Trans-Tasman Software Pty Ltd trading as SafetyMinder and all its wholly owned subsidiaries. Our address details can be found on our websites About Page.

2. Our principles of data protection

Our approach to data protection is built around four key principles. They're at the heart of everything we do relating to personal data.

a. Transparency:

We take a human approach to how we process personal data by being open, honest and transparent.

b. Enablement:

We enable connections and efficient use of personal data to empower productivity and growth.

c. Security:

We champion industry leading approaches to securing the personal data entrusted to us.

d. Stewardship:

We accept the responsibility that comes with processing personal data.

3. How we collect your data

When you use our websites or use our services, we collect personal data. The ways we collect it can be broadly categorised into the following:

a. Information you provide to us directly:

When you visit or use some parts of our websites and/or services we might ask you to provide personal data to us. For example, we ask for your contact information when you sign up for a free trial, respond to an email offer, participate in community forums, join us on social media, take part in training, contact us with questions or request support. If you don't want to provide us with personal data, you don't have to, but it might mean you can't use some parts of our websites or services.

b. Information we collect automatically:

We do not use cookies and similar tracking technologies to collect personal information however you enter data into an online service which is stored for your use.

4. Information we get from third parties:

The majority of information we collect, we collect directly from you. Sometimes we might collect personal data about you from other sources, such as publicly available materials or trusted third parties like our preferred dealers or partners. We use this information to supplement the personal data we already hold about you, in order to better inform, personalise and improve our services, and to validate the personal data you provide.

Where we collect personal data, we'll only process it:

- to perform a contract with you, or
- where we have legitimate interests to process the personal data and they're not overridden by your rights, or
- in accordance with a legal obligation, or
- where we have your consent.

If we don't collect your personal data, we may be unable to provide you with all our services, and some functions and features on our websites may not be available to you.

If you're someone who doesn't have a relationship with us, but believe that a Safetyfinder dealer or partner has entered your personal data into our websites or services, you'll need to contact that Safetyfinder dealer or partner for any questions you have about your personal data (including where you want to access, correct, amend, or request that the user delete, your personal data).

5. How we use your data

First and foremost, we use your personal data to operate our websites and provide you with any services you've requested, and to manage our relationship with you. We also use your personal data for other purposes, which may include the following:

a. To communicate with you. This may include:

- providing you with information you've requested from us (like training or product materials) or information we are required to send to you
- operational communications, like changes to our websites and services, security updates, or assistance with using our websites and services
- marketing communications (about Safetyminder or another product or service we think you might be interested in) in accordance with your marketing preferences
- asking you for feedback or to take part in any research we are conducting (which we may engage a third party to assist with).

b. To support you:

This may include assisting with the resolution of technical support issues or other issues relating to the websites or services, whether by email, in-app support or otherwise.

c. To protect:

So that we can detect and prevent any fraudulent or malicious activity, and make sure that everyone is using our websites and services fairly and in accordance with our terms of use.

d. To market to you:

In addition to sending you marketing communications, we may also use your personal data to display targeted advertising to you online – through our own websites and services or through third party websites and their platforms.

6. How we can share your data

There will be times when we need to share your personal data with third parties. We will only disclose your personal data to:

- other companies in the Safetyminder group of companies
- third party service providers and partners who assist and enable us to use the personal data to, for example, support and SMS and mail services
- delivery of or provide functionality on the website or services, or to market or promote our goods and services to you
- regulators, law enforcement bodies, government agencies, courts or other third parties where we think it's necessary to comply with applicable laws or regulations, or to exercise, establish or defend our legal rights. Where possible and appropriate, we will notify you of this type of disclosure
- an actual or potential buyer (and its agents and advisers) in connection with an actual or proposed purchase, merger or acquisition of any part of our business
- other people where we have your consent.

7. International Data Transfers

When we share data, it may be transferred to, and processed in, countries other than the country you live in. This may be for services like data storage, backup, sms service providers and the likes. These countries may have laws different to what you're used to. Rest assured, where we disclose personal data to a third party in another country, we put safeguards in place to ensure your personal data remains protected.

For individuals in the European Economic Area (EEA), this means that your data may be transferred outside of the EEA. Where your personal data is transferred outside the EEA, it will only be transferred to countries that have been identified as providing adequate protection for EEA data (like Australia or New Zealand), or to a third party where we have approved transfer mechanisms in place to protect your personal data – i.e., by entering into the European Commission’s Standard Contractual Clauses, or by ensuring the entity is Privacy Shield certified (for transfers to US-based third parties). For further information, please contact us using the details set out in the Contact us section below.

8. Security

Security is a priority for us when it comes to your personal data. We’re committed to protecting your personal data and have appropriate technical and organisational measures in place to make sure that happens.

9. Retention

The length of time we keep your personal data depends on what it is and whether we have an ongoing business need to retain it (for example, to provide you with a service you’ve requested or to comply with applicable legal, tax or accounting requirements). We’ll retain your personal data for as long as we have a relationship with you and for a period of time afterwards where we have an ongoing business need to retain it, in accordance with our data retention policies and practices. Following that period, we’ll make sure it’s deleted or anonymised.

10. Your rights

It’s your personal data and you have certain rights relating to it. When it comes to marketing communications, you can ask us not to send you these at any time – just follow the unsubscribe instructions contained in the marketing communication, or send your request to support@Safetyinder.com.au .

You also have rights to:

- know what personal data we hold about you, and to make sure it’s correct and up to date
- request a copy of your personal data, or ask us to restrict processing your personal data or delete it
- object to our continued processing of your personal data

You can exercise these rights at any time by sending an email to support@Safetyinder.com.au

If you’re not happy with how we are processing your personal data, please let us know by sending an email to support@Safetyinder.com.au . We will review and investigate your complaint, and try to get back to you within a reasonable time frame. You can also complain to your local data protection authority. They will be able to advise you how to submit a complaint.

How to contact us:

We're always keen to hear from you. If you're curious about what personal data we hold about you or you have a question or feedback for us on this statement, our websites or services, please get in touch.

As a technology company, we prefer to communicate with you by email – this ensures that you're put in contact with the right person, in the right location, and in accordance with any regulatory time frames.

Our email is support@Safetyminder.com.au