Personal Data Protection Notice

1. Introduction

In order to conduct our business, The Simpro Group Pty Ltd, a company established in Australia with company number 131 893 573 and its related bodies corporate which includes its offices in Australia, New Zealand, United Kingdom, United States of America and Canada (collectively referred to in this Notice as "Simpro", "we", "our" or "us") need to process Personal Data of individuals that interact with us.

We process Personal Data when we perform (whether or not by automated means) any operation or set of operations on it. For example, we process Personal Data when we collect, record, organise, structure, store, alter, retrieve, consult, use, disclose, disseminate, restrict, erase or destruct such Personal Data.

We consider the protection of your Personal Data a paramount corporate responsibility and we will always process Personal Data lawfully, fairly and in a transparent manner. This Personal Data Protection Notice ("Notice") sets out the Personal Data we collect from you, why we collect it, how it is used and shared and your choices and rights regarding the use of Personal Data we collect.

2. Scope

This Notice describes how we process Personal Data of:

- our suppliers, customers, business partners and their representatives;
- users of Simpro's websites, web applications, mobile applications and desktop applications ("Products and/or Services"); and
- Simpro's shareholders and their representatives;

This Notice does not cover the processing of Personal Data belonging to Simpro's employees, contractors and job applicants. If you are one of these individuals, please see our separate Privacy Notice here.

3. What is Personal Data?

Personal Data is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4. How do we collect your Personal Data?

We will primarily collect Personal Data from you either directly or indirectly from your interactions with us and our Products and/or Services. In some cases, we may also collect Personal Data about you from third parties who provide services to us (for example, credit information agencies)

Our Products and/or Services may use cookies. Cookies are small pieces of data stored on the web browser of your device. These are used by us for site administration and analysis purposes and to deliver tailored content. If you wish not to take advantage of cookies, you may configure your browser not to accept them (although this may disable or render unusable some of the features of our Products and/or Services).

5. What Type of Personal Data do we Collect?

We collect and process different types of Personal Data depending on who you are and why you interact with us.

We may process the following types of your Personal Data:

- Identification data – such as your name, gender, job title, photograph, date of birth and bank account details.
- Contact details – such as your home and business address, email address and telephone number.
- Sales-related information – which may include identification data and contact details along with business and industry information such as your business name, the industry your business is in and the size of your business and financial billing information that we require to process payment for our Products and/or Services.
- Usage information – this includes server log information (such as login information, IP addresses, device type, browser type, operating system, browser language, time zone, access times, network/connection type, location) and records of your use of our Products and/or Services.
- Location data – such as precise or approximate location information derived from GPS, Wi-Fi, Bluetooth, IP address, device settings, or other signals, including where used to enable location-based features, attendance verification, job-site check-in/check-out, route or proximity-based workflows, security controls, and geo-fencing functionality within our Products and/or Services.
- AI interaction data – such as prompts, instructions, queries, attachments, inputs, outputs, feedback, and related usage metadata where you use AI-enabled or machine learning-enabled features made available through our Products and/or Services.
- Other information – this includes information about access and attendance to our premises and physical assets, details about your use of our assets, communications with you (including complaints or concerns raised by you or any feedback or survey responses that you provide to us) and other information you voluntarily provide us.
- In respect of Shareholders, shareholder information – this includes contact details, number/quantity of shares and share numbers and details (including Identity and Contact details of any proxy who you may nominate to attend a Shareholders' Meeting.

Sensitive Personal Data

Our policy (which is reflected in our terms and conditions applicable to our Products and/or Services is not to collect or otherwise process your 'Special Category Data' and/or 'Criminal Offence Data' (both as defined in The General Data Protection Regulation 2016/679 ("**EU GDPR**") or EU GDPR as retained in the Data Protection Act 2018 or other applicable national legislation of the United Kingdom ("**UK GDPR**")) and/or other data which is treated differently by law due to its sensitive nature. If we need to collect or otherwise process this category of Personal Data, we will do so only where permitted under applicable law, including by obtaining explicit consent where required, and will provide you with further details of the processing, including the measures we take to keep such data secure, at the point of collection.

While our general policy is not to collect or otherwise process Special Category Data, certain features within our Products and/or Services may involve the processing of biometric data, such as facial images or face-matching data, for the purpose of identity verification, authentication, security, or access control. Where such features are used, we will only process biometric data where:

- it is necessary to provide the relevant functionality requested by you or your organisation; and
- we have obtained your explicit consent or otherwise have a valid lawful basis under applicable law.

6. How we Process your Personal Data – Lawful basis and purpose

We will only process your personal information when the law allows us to. Unless otherwise stated in this Notice, we process Personal Data for our Legitimate Interests. In particular, we process Personal Data in order that we may conduct our business operations and transactions smoothly and efficiently and continue to provide and develop our Products and/or Services. More specific examples of how our Legitimate Interests operate as the basis for our processing are listed below. In some cases, including where we provide AI-enabled features, we also process your Personal Data to perform a contract we have entered into with you, to take steps at your request before entering into a contract, or based on your instructions when using those features. We may process your Personal Data for any other purposes for which you have provided your consent or if there is another lawful basis for doing so and the new purpose is compatible with the original purpose. We may also process Personal Data where we are required to by law.

In some cases, we process Personal Data on behalf of our customers in connection with their use of our Products and/or Services. In those circumstances, we act as a processor (or service provider, as applicable) and process Personal Data in accordance with our contractual arrangements with those customers and their documented instructions.

We process your Personal Data for the following specific purposes:

- managing our relationship with you – this includes providing you with information about our Products and/or Services, improving our Products and/or Services and communicating with you including to evaluate your satisfaction and seeking feedback regarding our Products and/or Services;
- business-related purposes – this includes negotiating, managing, and fulfilling our contracts with customers, suppliers and third parties, managing business relationships, managing accounts and records, supporting corporate social

responsibility activities, resource planning and workforce management, activities and operations, internal investigations and debt administration;

- Products and/or Services-related purposes – this includes preparing a proposal (quote document) for you or sending you a demonstration, determining which or if any of our Products and/or Services are suitable for you, establishing your account, account integration or providing you with the Products and/or Services you have elected to purchase, notifying you of new features to our Products and/or Services or providing you with training, performing internal operations necessary to provide our Products and/or Services to you such as troubleshooting software, processing or facilitating payment for the Products and/or Services, including internal accounting or administration, providing your Personal Data to our related bodies corporate for the purposes of administration, storage, advisory or technical services. This also includes using Personal Data and AI interaction data to provide, maintain, test, improve, monitor, secure, and support AI-enabled, generative AI, machine learning, and large language model features within our Products and/or Services, including generating responses, summarising content, extracting information, classifying content, powering assistants or automations, improving the performance and functionality of those features within our Products and/or Services, and preventing misuse. You are responsible for the content you submit when using such features and should not include Personal Data unless you have appropriate authority to do so. We implement reasonable measures designed to minimise the amount of Personal Data processed through such features and to limit processing to what is reasonably necessary for the purposes described above. This also includes using location data to provide, enable, support, verify, secure, improve, and administer location-based features within our Products and/or Services, including geo-fencing, attendance and time tracking, job-site verification, dispatching, route-related workflows, fraud prevention, and related reporting and analytics;
- communications and messaging purposes – this includes contacting you by phone call or text message where permitted by law and, where required, with your consent, to provide service, support, operational, transactional, account, security, reminder, and other communications relating to our business, Products and/or Services;
- marketing and public relation purposes – this includes analysing the characteristics of visitors to our website, to prepare analytics and profiling for business intelligence purposes, to personalise your experience on our website and managing our newsletters and communications;
- managing safety and security risks – this includes managing and monitoring access and use of our premises and sites, safety and security at our sites and our IT environment (including monitoring electronic communications);
- internal operations – this includes troubleshooting, data analysis, testing, research, statistical and survey purposes; and
- managing shareholder relationships and complying with any legal requirements in relation to maintaining the shareholder register.

We may also (upon obtaining your express permission) collect and otherwise process your Personal Data for secondary purposes, such as sending you targeted marketing activities (including email mail outs or electronic marketing materials) in relation to events and/or our Products and/or Services.

7. Children and Minor Users

Our Products and/or Services are business and workforce-management tools and are not directed to children under 13. Children under 13 must not use our Products and/or

Services. Individuals aged 13 to 17 may use them only as authorised users of a customer organisation and subject to any parental or guardian approval required by applicable law or the relevant app marketplace. The customer is responsible for ensuring that such use is lawful and for obtaining any consent or authorisation that it is required to obtain.

Where supported by the relevant app marketplace or device platform, our mobile applications may receive and use general age-category and consent-status signals made available by providers such as Apple or Google to apply age-appropriate access controls and comply with applicable law. These signals do not include a user's exact date of birth. We use the signals transiently when the application is launched and do not store or locally cache the age-signal data.

A user identified as under 13 will be prevented from using the mobile application. Users aged 13 to 17 may proceed where any parental or guardian approval required by the relevant app marketplace has been provided. Where an age signal is unavailable or has not been shared, we do not treat that fact alone as indicating that the user is under 13, unless applicable law or platform requirements require a different result.

8. Why our processing of your personal data is necessary

We only process Personal Data when this is necessary, including where this is for our Legitimate Interests as detailed above. Our ability to perform the functions listed above (for example, our ability to perform any contract entered into with you) may be adversely affected if we do not process your Personal Data. It may also prevent us from complying with our legal obligations.

9. Consent

Except to the extent set out in this Notice or unless you are advised to the contrary, we do not use Consent as the lawful basis upon which we process your Personal Data.

10. Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We will only subject your Personal Data to automated decision making where:

- we have notified you of the decision and given you 21 days to request a reconsideration.
- it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- you give your explicit written consent to such automated decision making and where appropriate measures are in place to safeguard your rights.

11. With whom do we share your Personal Data?

We may disclose your Personal Data (which may sometimes include Special Category, Criminal Offence, or other sensitive Personal Data but only where you have consented to the processing of such Personal Data) to related bodies corporate as well as with third parties involved in the running of our business where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing. We might also be required to disclose your Personal Data to a third party:

- to respond to a legal process such as a court order or subpoena or to comply with the requirements of applicable law
- to protect the safety of any person; or
- to address fraud, security or technical issues.

In particular, we may disclose your Personal Data to the following parties:

Related Bodies Corporate

Where necessary, for the internal and/or external operations of the Simpro group of companies, including in order to provide you with our Products and/or Services, to perform a contract we may have entered into with you and/or so that we can best fulfil any of the purposes set out in section 6, we may disclose your Personal Data between our related bodies corporate, meaning our offices across the world. See a list of our current locations listed here. This may result in your Personal Data being transferred to countries other than your country of residence, including countries which may be subject to reduced privacy laws. We can confirm that Simpro entities are subject to the same corporate policies and procedures (including this Notice) and we will only transfer data in accordance with the provisions of section 11 of this Notice.

Third Parties

We may also need to disclose your Personal Data to:

- third parties who provide services we use to run our business (such as external service providers that assist Simpro to perform information technology and security services functions);
- prospective purchasers of all or part of our business or of any shares in Simpro;
- our professional advisors (such as our lawyers and accountants); and
- government authorities or other persons where obliged to do so by an applicable law.

We may also disclose your Personal Data to third parties who provide services we use to run our business and deliver our Products and/or Services, such as hosting, infrastructure, analytics, customer support, security, telecommunications, messaging, and information technology service providers.

This may include service providers that provide artificial intelligence, machine learning, or large language model capabilities on our behalf. Where we use such providers, they may process Personal Data, including AI interaction data, solely for the purpose of providing services to us and in accordance with our instructions.

We only permit our third-party service providers to process your Personal Data, including AI interaction data, for specified purposes and in accordance with our instructions. They must not use your Personal Data for their own independent purposes or to train or improve their own or any third-party artificial intelligence or machine-learning models.

12. Use of Telephone Numbers and Messaging Data

We may collect and use your mobile telephone number to communicate with you, including via voice calls or text messages where permitted by law and, where required, with your consent.

We may share your mobile telephone number, messaging data, and related communication records with our service providers, including telecommunications and messaging providers, solely for the purpose of delivering communications to you on our behalf and in accordance with our instructions. These providers are not permitted to use such information for their own purposes, except as necessary to provide their

services or comply with applicable law.

We do not sell, rent, or share mobile telephone numbers or related messaging consent data with third parties or affiliates for their own marketing or promotional purposes.

We do not share records of your consent to receive communications, including opt-in data, with third parties or affiliates except as necessary to provide messaging services, to comply with applicable law, or to protect our legal rights.

Where you have expressly requested or consented to be contacted by a third party or affiliate, we may share your contact details with that third party or affiliate for that purpose.

13. Transfer of Personal Data

Where disclosure to one of the parties mentioned above results in data being transferred to another country, we will only make such disclosure where we have a lawful basis for doing so and we shall ensure that the disclosure complies with all applicable laws. This may include entering into a legally binding contract with the recipient under which they are obliged to handle your information in accordance with applicable laws of that jurisdiction or a higher standard if required (for example to meet compliance with the requirements relating to international data transfer under EU GDPR and UK GDPR).

For the purposes of this Notice, "disclose and disclosure" means to transfer, share (including verbally and in writing), send, or otherwise make available or accessible your Personal Data to another person or entity.

14. How do we keep Personal Data safe?

We have an obligation to ensure that your Personal Data is protected from unauthorised processing, accidental disclosure, access, loss, destruction or alteration. Accordingly, we have a range of technical security measures and procedures in place to ensure that your Personal Data is protected appropriately. These measures have been implemented and are reviewed regularly to protect your Personal Data from scenarios which may result in the accidental or unauthorised disclosure of your Personal Data as mentioned above.

In the unlikely event there is a data breach, we will notify the relevant data protection authority as required by applicable law.

For further information on the security measures in place you can contact us by using the contact details at section 19.

15. For how long do we keep your Personal Data?

We will only keep your Personal Data for as long as necessary to fulfil the purposes for which we are processing your Personal Data, unless the law requires us to retain it for longer. Further details on our retention policy can be obtained by contacting us in accordance with the details set out in section 19.

In accordance with our retention policy, we will ensure Personal Data is destroyed securely.

16. Third Party Links and Forums

Our Products and/or Services may contain links to other websites. We are not responsible for the privacy practices or the content of other websites. The privacy practices applicable to other websites may differ substantially from ours. Please read the privacy notice of any other websites you visit before using such websites.

Any Personal Data that you choose to submit or post on our social media pages or any other public forum ("Forums") may be read, collected, or used by others who visit these Forums and may be used to send you unsolicited messages. We are not responsible for the Personal Data you choose to submit in these Forums.

17. What are your rights in relation to the Personal Data we collect?

You have certain rights in relation to your Personal Data that we hold about you, though the details of these may vary depending on the country where you are based.

In general, it is within your rights to:

- request access to and obtain copies of any Personal Data we hold about you;
- request that your Personal Data be provided to you in a format that can be easily read; and
- request the correction of your Personal Data.

If you wish to exercise any of the above rights, please send your request to our Data Protection Officer using the contact details set out below.

18. EU GDPR/UK GDPR Specific

If you are a Data Subject of the UK or the EU, for the purposes of this Notice, Simpro is the "Controller" (as defined in EU GDPR and UK GDPR) in relation to your Personal Data and the terms "personal data", "data subject", "processing", "special category data", "criminal offence data" and "legitimate interests" used in this Notice, (whether capitalised or not), shall have the meanings given to them in EU GDPR and UK GDPR as applicable.

In addition to the rights described in section 17 (What are your rights in relation to the Personal Data we collect), you have the right, in certain circumstances to:

- request the erasure of your Personal Data (more commonly referred to as the "Right to be Forgotten") if you believe it is no longer necessary for the purposes of which it was originally collected;
- request the restriction of processing;
- withdraw consent (where processing is being undertaken on the basis of consent) previously given at any time;
- object to the processing of the Personal Data where processing is being undertaken on the basis of our (or a third party's) Legitimate Interests; and
- request the transfer of your Personal Data from Simpro to a third party.

19. Contact Us

If you:

- have any questions or complaints in relation to this Notice or our use of your Personal Data
- wish to inform us of a change or correction to your Personal Data or exercise any of the other rights available to you as a data subject; or

- would like a copy of the information we collect on you in relation to this Notice or our use of your Personal Data,

please contact our Data Protection Officer using the following details:

Name: Data Protection Officer

Email: privacy@simpro.co

Post: Attention: Data Protection Officer
Simpro Software Limited
Building 17, Garden City Office Park
2404 Logan Road
Eight Mile Plains QLD 4113
Australia

If you are not satisfied with Simpro's response the regulatory body that governs privacy in your jurisdiction may be able to help you. Please contact our Data Protection Officer for details of the regulatory body that applies to you.

We will ensure that your question, concern or complaint is dealt with as soon as practicable. We reserve the right to verify your identity before complying with the request.

20. Changes to this Personal Data Protection Notice

We will update this Notice from time to time where necessary to reflect changes in applicable laws or in our privacy compliance practices. The latest version of this Notice will always be available online through the Simpro website.

This Notice was last updated on 26 August 2026.