FOREMIND PRIVACY POLICY AND COLLECTION NOTICE

Last updated 29 January 2026

Foremind is committed to respecting and protecting your privacy. This Privacy Policy and Collection Notice ("**Privacy Policy**") describes the types of Personal Information (as defined below) we collect, which, given the nature of our Services, is likely to be 'health information', the purposes for which we collect and use it, who we may share it with, the measures we take to protect it. It also provides information about your rights in relation to your Personal Information and how you can contact us.

This document should be read in conjunction with the *'Your Counselling and Mandatory Disclosures'*, which outlines the specific circumstances under which a Foremind-appointed Counsellor may be legally or ethically obligated to report or disclose your confidential information. Please read it carefully before commencing your first counselling session.

This Privacy Policy may be changed from time to time. All changes will be communicated by publishing a copy of the updated Privacy Policy on our Platform.

1 **Introduction and scope**

1.1 We are Foremind Pty Ltd (ABN 38 615 400 612), together with our related entities and affiliates (collectively, "**Foremind**"). In this Privacy Policy, references to "**we**", "**us**", and "**our**" mean one or more members of the Foremind group of companies.

1.2 Foremind partners with employers to deliver workplace wellbeing and support services through an Employee Assistance Program (EAP). Foremind maintains a website and platform (together, the "**Platform**") which provides employees access to these services, including confidential counselling and coaching sessions with qualified mental health professionals, risk assessments and management, and access to digital wellbeing resources and learning materials, and related or additional services made available from time to time ("**Services**"). **If you are directed to this privacy policy, it is likely your employer is a partner in this program ("Employer Partner") and may be involved in facilitating access to these services for you.**

1.3 Our services are not directed to or intended for children. We do not knowingly collect Personal Information relating to children under 16, and we do not facilitate counselling sessions for those aged 16 or 17 without parental or guardian consent, although we won't share information with them without your consent.

2 **What we collect**

2.1 The "**Personal Information**" (as that term is defined in the *Privacy Act 1988* (Cth) ("**Privacy Act**")) we collect from you, and how we collect it, will depend on the service your Employer Partner is purchasing and the way you interact with us. We only collect personal, sensitive, or health information about you to the extent reasonably necessary to provide our Services or otherwise reasonably necessary to perform our functions.

2.2 We may collect, use, store and transfer different kinds of Personal Information about you which we have grouped together as follows:

2.2.1 **'Identity Data'** includes your name, marital status, job title, employer/sponsoring organisation, employer business unit, next of kin details, location, residential address, sex, race or ethnic origin, date of birth, whether you are Aboriginal or Torres Strait Islander, driver's license, medicare number and other government identifiers;

2.2.2 **'Contact Data'** includes billing address, email address and telephone numbers;

2.2.3 **'Financial Data'** includes bank account and payment card details (of payees within an Employer Partner organisation only);

2.2.4 **'Administrative Data'** includes details about payments to and from you, and other details of products and services in the relevant transaction;

2.2.5 **'Technical Data'** includes internet protocol (IP) address, your login data for our Services, statistics on page views and sessions, acquisition sources, search queries and/or browsing behaviour, browser session data, webpage from which you came, webpage(s) or content you accessed, navigational and log data, information about your access and use of our Platform and services, including through the use of internet cookies, time zone settings and geolocation, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access the Platform, data contained with documents or files that you otherwise share with us, and other meta data;

2.2.6 **'Profile Data'** includes your username or similar identifier, password, your interests, preferences, feedback;

2.2.7 '**Health Data**' includes health information and sensitive personal information about you, including your reason for requesting EAP assistance, EAP participation records, questionnaires and reports that you have provided such as wellbeing surveys and psychosocial hazard reports, counselling scheduling and session data, health or personal history, family physical and mental health history, counselling session notes and briefs, mental health assessments and diagnoses, crisis intervention records, risk assessment responses, and legal and accounting notes ;and information received from other professionals;

2.2.8 **'Marketing Data'** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

3 **How we collect**

3.1 We generally collect Personal Information:

3.1.1 from you directly when you provide your details to us, via face-to-face discussion, teleconference, phone call, or registration form (offline or online);

3.1.2 when you interact with us via our Platform, or social media channels; or

3.1.3 from your employer (our 'Employer Partner').

3.2 We generally collect Health Information from you directly or otherwise with your consent, which may be implied, before or at the time of collection, unless an exception applies under applicable law — such as in an emergency, there is a serious threat to life or for other 'permitted health situations'.

3.3 We may also collect Personal Information from a person responsible for you/your appointments, such as a guardian or next of kin, or from third parties where the law allows including other members of your treating team diagnostic centres, specialists, hospitals, Healthlink, the NDIA, Medicare, your health insurer.

3.4 When you first make contact with us (including if your employer gives us your Personal Information), we create a unique digital record for you. We, and our contracted professionals and counsellors, may also keep physical records in relation to the service we provide. Each time a service is provided to you, new information is added to your record. Our clinicians, counsellors or other contracted professionals may create clinical notes, briefs and records as part of the services provided to you, and these form part of your health record.

3.5 We take reasonable technological and organisational steps to protect the Personal Information we hold from misuse, interference and loss, and unauthorised access, modification and disclosure — see *'Security measures'* below for more information.

4 Why we collect

4.1 We collect, hold, use, and disclose Personal Information for the following purposes:

Purpose for collection	Type of Personal Information
• To provide our Platform and Services to you (through secure online portals, via the telephone or in person) and to support continuity of care and professional supervision, including to assist the professionals involved in the provision of services with managing and improving the services provided to you	• Identity Data • Contact Data • Profile Data • Health Data
• To comply with our contractual obligations and provide Services to Employer Partners, including providing anonymised and/or aggregated reports and analytics.	• Identity Data • Contact Data • Health Data
• To comply with our legal obligations (including our obligations to maintain records of all health-related services or child protection legislation, under Mandatory Disclosure reporting obligations or if we are subpoenaed by a Court) or if otherwise required or authorised by law (including disclosing such information where we reasonably believe that the failure to disclose the information would place you or another person at serious risk to life, health or safety, or where a 'permitted general situation' exists such as lessening or preventing a serious threat to life, health or safety, taking appropriate action in relation to suspected unlawful activity or serious misconduct)	• Identity Data • Contact Data • Financial Data • Administrative Data • Technical Data • Profile Data • Health Data • Marketing Data
• To enable outside contractors to carry out activities on our behalf	• Identity Data • Contact Data • Financial Data • Administrative Data • Technical Data • Profile Data • Health Data • Marketing Data
• To manage our accounts and obtain payment for the services we provide, to meet our contractual obligations to partners (including Employer Partners), and other internal record-keeping and administrative purposes	• Identity Data • Contact Data • Financial Data • Administrative Data • Technical Data • Profile Data • Marketing Data

Purpose for collection	Type of Personal Information
• To contact and communicate with you, including managing our relationship, providing technical support, responding to technical enquiries, recording your preferences, and keeping you informed about changes, updates, events, and other relevant matters	• Identity Data • Contact Data • Administrative Data • Technical Data • Profile Data • Marketing Data
• To manage your account and subscription or access to our Services, to personalise our website for you, to enable logging in to our Platform, and customize your use of our Services	• Identity Data • Contact Data • Administrative Data • Technical Data • Profile Data • Marketing Data
• To administer and protect our business and our Platform (including troubleshooting, data analysis, testing, system maintenance, validating against fraudulent transactions, support, reporting and hosting of data)	• Identity Data • Contact Data • Technical Data • Profile Data • Marketing Data
• For consultations with other doctors or allied health professionals involved in your healthcare, where you would reasonably expect such information to be disclosed (e.g. your GP) and the disclosure of that information is for a purpose directly related to the primary purpose for which your personal information was collected	• Identity Data • Contact Data • Health Data
• To connect you with non-counselling/health related professional service providers (such as legal and tax) where you request us to do so	• Identity Data • Contact Data

5 **Anonymised and aggregated data**

5.1 We may anonymise the Personal Information we collect (so it can no longer identify you) and may then combine it with other anonymous information so it becomes aggregated data. Aggregated data helps us produce wellbeing insights and program-level statistics (for example, the percentage of employees accessing counselling services, completing wellbeing check-ins), which helps us evaluate and improve our Services, support research and quality-assurance activities, and provide anonymous reports to our Employer Partners in accordance with our contractual obligations.

5.2 Data protection and privacy laws do not govern the use of aggregated data.

6 **Use of cookies**

6.1 A cookie is a text file or a packet of information that is placed on your hard disk by a web page server to identify and interact more effectively with your computer. There are two types of cookies that may be used at our website: a persistent cookie and a session cookie. A persistent cookie is entered by your web browser into the "Cookies" folder on your computer and remains in that folder after you close your browser, and may be used by your browser on subsequent visits to Our website. A session cookie is held temporarily in your computer's memory and disappears after you close your browser or shut down your computer.

6.2 Cookies are uniquely assigned to you and can only be read by a web server in the domain that issued the cookie to you. In some cases, cookies may collect and store Personal Information about you.

6.3 You can configure your internet browser to accept all cookies, reject all cookies or notify you when a cookie is sent. Please refer to your internet browser's instructions to learn more about these functions. Most web browsers automatically accept cookies, but you can usually modify your browser settings to decline cookies if you prefer. If you choose to decline cookies, you may not be able to fully experience the features of our Platform.

6.4 We use our own cookies to keep track of your use of our Platform, designed to provide a better user experience for you. We also use third party cookies. The following cookies are used on our Platform:

6.4.1 **Necessary cookies**. These are cookies that are required for the operation of the Platform. These essential cookies are always enabled because the Platform will not work properly without them. They include, for example, cookies that enable certain security functions.

6.4.2 **Preference cookies**. These enable us to recognise you when you return to the Platform, to personalise our content for you and remember your preferences.

6.4.3 **Statistics cookies**. These help us to understand how visitors interact with the Platform. They include cookies that tell us how long people spend on the Platform and the number of times they visit.

6.4.4 **Marketing cookies**. These are used to record your visit to the Platform, to make the Platform more relevant to your interests.

7 **Security measures**

7.1 We hold Personal Information electronically in the cloud, on secure servers in and outside of Australia, and may also hold Personal Information locally, including but not limited to on desktop computers, laptops and back-up hard drives. [All systems used to store clinical records are protected by strong encryption, access controls and audit logging.]

7.2 We take all reasonable steps to ensure that your Personal Information is secure from any unauthorised access, misuse or disclosure. However, no transmission or storage system can be guaranteed to be completely secure, and we do not guarantee that unauthorised access will never occur.

7.3 Our security measures include:

7.3.1 role-based access controls and user authentication (including multi-factor authentication);

7.3.2 storing your information in secure, Australian-based cloud infrastructure protected by controls such as encryption in transit and at rest;

7.3.3 endpoint antivirus and malware protection;

7.3.4 unified threat-management traffic scanning;

7.3.5 segregated data backups;

7.3.6 hardened security policies;

7.3.7 automated server patching;

7.3.8 multi-factor authentication;

7.3.9 role-based and least-privilege access controls;

7.3.10 continuous security monitoring and audit logging;

7.3.11 regular testing and review of our cybersecurity measures;

7.3.12 documented staff policies and security-awareness training;

7.3.13 documented incident and breach reporting processes;

7.3.14 documented business continuity and disaster recovery processes; and

7.3.15 other industry standard safeguards.

7.4 If there is an incident that has affected your Personal Information, we will notify the regulator and keep you informed (where required under applicable privacy law).

8 How long we keep your Personal Information

8.1 We will only retain your Personal Information for as long as necessary to fulfil the purposes we collected it for, or otherwise as required or authorised by law.

8.2 To decide how long to keep Personal Information (also known as its retention period), we consider the volume, nature, and sensitivity of the Personal Information (particularly where it constitutes Health Information), the potential risk of harm to you if an incident were to happen, whether we require the Personal Information to achieve the purposes we have identified or to maintain accurate business and clinical records, or whether we can achieve those purposes through other means (e.g. by using aggregated data instead), and any applicable legal or professional requirements (e.g. minimum retention periods under State health records legislation).

8.3 We may keep identity data and certain other data (including any exchanges between us by email or any other means) for up to seven years after the end of our contractual relationship with you.

8.4 If you have asked for information from us or you have subscribed to our mail-out list, we keep your details until you ask us to stop contacting you.

9 **Who we share your Personal Information with**

9.1 We may share your Personal Information with the organisations listed below (together with our employees and related bodies corporate, our "**Affiliates**"), for the specified reasons.

Category of third party	Reason for sharing your Personal Information
Service providers such as hosting providers, IT security providers and auditors, payment processors and billing providers, and marketing agencies	To host our Platform, manage cloud storage, process payments or manage invoicing, comply with our data security obligations, or otherwise to conduct our business
Counsellors, clinicians and other contracted service providers	To provide counselling, coaching, and wellbeing services to employees under the EAP; for clinical supervision and quality assurance
Employer Partners	To provide anonymised utilisation reports, program-level wellbeing insights, and other information we are contractually obligated to provide; never your Health Information unless a specific exception permits otherwise (such as with your consent)
Any authorised government or regulatory or self-regulatory authority or enforcement agency	If we are under a duty to disclose your Personal Information in order to comply with any legal obligation, or to protect the rights, property or safety of Foremind, its Employer Partners or others
Professional advisers or contractors, such as our auditors, accountants, or lawyers or other professional consultants and insurers	To obtain relevant advice in running and insuring our business
As part of or in connection with a sale of our business, or a merger, reorganisation, investment, change in control, transfer of substantial corporate assets, liquidation or similar transaction	For the purposes of the relevant transaction

10 **Mandatory Disclosure Reporting**

10.1 We may use or disclose your Personal Information or Health information where required by applicable mandatory disclosure reporting laws or where we reasonably believe the disclosure is necessary to prevent or lessen a serious threat to life, health or safety. You can read more about our mandatory disclosures here.

11 **Direct marketing and service communications**

11.1 Where your active consent to receive marketing messages is required by applicable privacy laws, we will obtain such consent for this purpose. Otherwise, by providing us with your Personal Information, you consent to us using it to make contact with you on an ongoing basis to provide you with current information about our products and services, special offers you may find of interest, or new products or services being offered by us or one of our associated companies. This may be by telephone, mail, email, SMS and social media.

11.2 Where the communication involves or is based on Health Information or other "Sensitive Information" (as the term is defined in the Privacy Act), we will first obtain your express consent before using that information for any direct marketing purposes.

11.3 If you are using our Services as an employee under one of our Employer Partners, we may send you:

11.3.1 service-related messages such as appointment confirmations and reminders, wellbeing check-in reminders, or resource links; and

11.3.2 with your consent, information about new or expanded wellbeing programs available through your employer.

11.4 You may opt out of marketing communications at any time by:

11.4.1 clicking the "unsubscribe" link in our marketing emails;

11.4.2 replying "STOP" to our marketing SMS; or

11.4.3 emailing us at privacy@foremind.com.au.

11.5 Even if you opt out of marketing communications, you will still continue to receive essential service notifications such as appointment details, and other information required for us to deliver our Services.

12 **Contacting us and complaints**

12.1 If you have questions, requests or concerns about your Personal Information or this Privacy Policy, please email us at privacy@foremind.com.au. We will take such steps as are reasonable to investigate any issues within a reasonable time of receipt. We will give you written notice of the investigations which have been carried out and the outcome.

13 **Anonymity and Pseudonyms**

13.1 Because we provide wellbeing services under an EAP, it is generally impracticable for us to deliver counselling, coaching, wellbeing check-ins or referral services anonymously or under a pseudonym. We are required to verify that you are eligible to access the EAP through your employer, and our clinicians must be able to confirm your identity to provide safe, continuous and appropriate care.

13.2 Regretfully, we cannot provide our services to you on an anonymised basis. If you do not provide your personal details to us:

13.2.1 we may not be able to communicate with you about our products and Services;

13.2.2 we may not be able to provide you with some or all aspects of our Services (for example, if you do not establish an account with us, you will not be able to use and access our Services or Platform);

13.2.3 we may not be able to provide you with information about Services that you may want, including information regarding any complaints you may have regarding our Services; and/or

13.2.4 we may be unable to tailor the content of our Services to your preferences, and your experience of our Services may not be as enjoyable or useful.

13.3 Foremind does not disclose identifiable Personal Information (including Health Information) about users to Employer Partners without express consent, unless disclosure is required or authorised by law. For more information on when disclosures are required by law, please refer to *'Your Counselling and Mandatory Disclosures'*. Foremind may provide aggregated and de-identified information to Employer Partners for the purpose of reporting on overall program utilisation, wellbeing trends, and service effectiveness. This information does not identify any individual.

14 **Transfers of Personal Information out of Australia**

14.1 Our Affiliates may be located in or outside Australia. For example, certain technology or support services we use, such as secure email or data analytics, may involve incidental disclosure of Personal Information outside your relevant state or Australia. Where this occurs, we take reasonable steps to ensure that the overseas Affiliate:

14.1.1 handles information in accordance with the Privacy Act and other applicable law;

14.1.2 is bound by contractual terms imposing equivalent privacy and security obligations; and

14.1.3 does not use or disclose the Personal Information for any purpose other than to provide the contracted services to Foremind.

14.2 We do not authorise any overseas recipient to use Health Information for its own purposes, and we do not transfer Health Information to jurisdictions without privacy protections substantially similar to those in Australia and/or relevant Australian state law.

14.3 In cases where we transfer your Personal Information (other than Health Information) to a recipient outside Australia, we will only do so in accordance with Australian Privacy Principle 8. For example, where you have given your informed consent, the disclosure is required by law, or where we reasonably believe the overseas recipient is subject to a law or binding scheme that is substantially similar to the APPs that provides accessible enforcement mechanisms.

14.4 We store and process your Health Information on secure cloud servers located in the US, EU, UK ansd Australia. By providing your Health Information to us, you consent to it being stored and handled in accordance with this Privacy Policy and applicable privacy and health records legislation. In cases where we transfer your Health Information to a recipient outside Australia, it will only occur with your consent or where authorised or required by law. For example, where it is necessary to respond to a serious threat to life or health.

15 **Notifiable Data Breach Scheme (NDBS)**

15.1 If there is a data breach and we are required to comply with the NDBS, we will take all reasonable steps to contain the suspected or known breach where possible and follow the process set out in this clause.

15.2 If we have reasonable grounds to suspect that the data breach is likely to result in serious harm to any individuals involved, then we will take all reasonable steps to ensure an assessment is completed within 30 days of the breach or sooner if possible. We will follow all guidance published by the Office of the Australian Information Commissioner ("**OAIC**") (if available) in making this assessment. If we reasonably determine that the data breach is not likely to result in serious harm to any individuals involved, or that any remedial action we take is effective in preventing serious harm from becoming likely, then we will not notify the affected individuals or the OAIC.

16 **Your rights**

16.1 Your privacy rights include:

16.1.1 Access to Personal Information.

(a) You can request access to your Personal Information, subject to certain exceptions. For example, we or your treating clinician or counsellor may, in accordance with applicable law, refuse to provide you with access if, for instance, granting you such access could result in serious harm to you or another individual, or if they believe the request is frivolous and vexatious.

(b) We will endeavour to provide access in the manner requested by you if it is reasonable and practicable to do so, otherwise we will take such steps as are reasonable to provide access in a way that meets both your and our needs.

(c) We may charge you for providing access to your Personal Information. You will be advised of the relevant charge and asked to make payment prior to access being provided.

(d) We may also require you to provide identification or validation to verify your identity or provide you with certain records.

(e) If we refuse your request for access on any ground permitted by law, we will give you written notice in accordance with applicable law, setting out the ground/s of the refusal (except to the extent that it would be unreasonable to do so) and the mechanisms to complain about the refusal.

16.1.2 Correction of Personal Information

(a) You can request corrections to any inaccurate, outdated, incomplete or misleading information regarding your Personal Information. If you request correction, we will address it within a reasonable timeframe and notify you of the outcome.

(b) Where Personal Information which has previously been disclosed to another organisation in accordance with applicable law and this Privacy Policy has been corrected you may ask us to notify the other organisation of the correction. We will take such steps as are reasonable to give that notification unless it is impracticable or unlawful to do so.

(c) If we refuse your request to correct your Personal Information we will give you written notice in accordance with applicable law, setting out the ground/s of the refusal (except to the extent that it would be unreasonable to do so) and the mechanisms to complain about the refusal.

(d) If we refuse your request to correct your Personal Information, you may request that we associate with your Personal Information in a statement that in your view the information is inaccurate, out of date, incomplete, irrelevant or misleading. We will take such steps as are reasonable to associate the statement with your Personal Information in such a way that the statement will be apparent to users of the information.

(e) We have an independent obligation to take reasonable steps to correct Personal Information that is inaccurate, out-of-date, incomplete, irrelevant or misleading.

16.1.3 You can ask us to delete or de-identify your Personal Information if there is no good reason for us to continue holding it.

16.1.4 You can ask to have your Personal Information, where technically feasible, sent to another organisation, where we hold this Personal Information with your consent or for the performance of a contract with you.

16.1.5 You can ask us not to send you any marketing materials. However, we may still send you newsletters and updates about your account, if you are a business contact, or otherwise send important service communications.

16.1.6 If you are unhappy with the way we collect and use your Personal Information , you can complain to the OAIC, but we would encourage you to contact us first so that we can try to address your concerns.

16.2 To submit requests in relation to any of the above, please email us on privacy@foremind.com.au. Please note that we may ask you to verify your identity before responding to such requests. If your request is particularly complex it may be necessary to book a scheduled counselling appointment in order to discuss and assess correction requests with you.

17 **Automated decision making**

17.1 Our Platform includes automated functions such as appointment reminders, wellbeing check-ins, survey delivery and anonymised usage analytics. These tools help improve the delivery of our Services but do not involve automated clinical decision-making nor do they impact contractual rights, legislative benefits, or access to essential services. These decisions do not create, alter, or deny any rights or entitlements. As such, they do not have significant effects on you, nor do they reach the threshold of significantly affecting individuals, and we do not provide additional disclosures related to automated decision-making.

18 **Secondary purposes**

18.1 The Privacy Act permits use of Personal Information for secondary purposes when those secondary purposes are related to the primary purpose of providing services to you.

18.2 Where permitted under the Privacy Act, we will use and share Personal Information we hold about you for the following secondary purposes:

18.2.1 Adding your details to our mail-out list to inform you of products and services which may affect or interest you;

18.2.2 Notifying you of any changes to our business or other news which may be relevant to your circumstances; and

18.2.3 Contacting you for sales purposes.