<u>SecondMind Privacy Policy</u>

Privacy and the protection of personal data (or "personally identifiable information") is very important to Second Mind Labs Inc., the corporate entity that operates the APIs and voice infrastructure for the Ambient Intelligence and VoiceProtect products, as well as a website at Secondmind.ai (for purpose of this document will be referred to as "Second Mind").

This Privacy Policy applies to all Second Mind clients and partners, and whenever appropriate, to their end customers

<u>The Information Second Mind Collects</u>

The amount and type of information that Second Mind gathers depends on the nature of the interaction. There are three ways Second Mind collects information:

1. We collect information you provide to us voluntarily when you sign up as a business customer or become a registered user of our service through one of our partners. For any third party applications that you choose to integrate such as email or file services, Second Mind does not store any data except the matches that occur during conversations for purpose of maintaining a history for you, which will include number or contact that call was with.

2. All our voice biometric software products utilize a standard request-response exchange through our secure API. We act as a custodian of this data and collect the absolute minimum amount of personal data possible, which include speech samples.

3. Second Mind does not disclose personally-identifying information other than as described below.

4. We collect and store metadata from apps you choose to connect with Second Mind such as Google apps (Gmail, Google Drive, Google calendar), Dropbox, Foursquare, Microsoft Outlook, etc. This information is to maintain a history of matches that occur for each of your calls so you can view this history.

5. When you use Second Mind, we use log data and cookies to collect certain information. A cookie is a string of information that a website stores on a visitor's computer, and that the visitor's browser provides to the website each time the visitor returns. Second Mind uses cookies to help Second Mind

identify and track visitors, their usage of Second Mind website, and their website access preferences. Second Mind visitors who do not wish to have cookies placed on their computers should set their browsers to refuse cookies before using Second Mind's website, with the drawback that certain features of Second Mind's website may not function properly without the aid of cookies.

6. Second Mind will from time to time record and save calls for purposes of deep learning and mapping of your speech patterns and vocabulary. This enables Second Mind's artificial intelligence engine to improve its recognition and understanding of your speech patterns and vocabulary. This will improve our service over time and enable new capabilities.

Like most web operators, Second Mind collects non-personally-identifying information of the sort that web browsers and servers typically make available, such as the browser type, language preference, referring site, and the date and time of each visitor request.

Second Mind's purpose in collecting non-personally identifying information is to better understand how Second Mind's visitors use its service. From time to time, Second Mind may release non-personally-identifying information in the aggregate, e.g., by publishing a report on trends in the usage of its service.

Second Mind also collects potentially personally-identifying information like Internet Protocol (IP) addresses. Second Mind does not use such information to identify its visitors, however, and does not disclose such information, other than under the same circumstances that it uses and discloses personally-identifying information, as described below.

<u>How we user your information</u>

1. **Personal Information.** Depending on the application, Second Mind may require certain personal information including, but not limited to your email address. The reason Second Mind requests information is critical to the service and detailed as follows:
    A. Account Integration. This is the information used to integrate Second Mind with a third party service such as Dropbox or Google.
    B. Speech Recognition and Vocabulary Customization. With a knowledge of your industry, SecondMind can better tailor it's speech recognition to your business needs.

B. Speaker Recognition (Voiceprint / VoiceProtect). For companies or users that use VoiceProtect or any of our voice biometrics products, Second Mind will create an algorithmic representation of the voice. This will not be shared with any third party or used for any other purposes other than as designated by user or company for authentication purposes.
C. Billing and Payments. In order to process payment for our service, we may ask for your credit card number and other billing information.
D. Customer Service. Second Mind will use your personal information to respond to your inquiries or questions. If you send us a request (for example via a support email or via one of our feedback mechanisms), we reserve the right to publish it in order to help us clarify or respond to your request or to help us support other users.

2. **Third-Party App Metadata.** We store the metadata from the apps you connect such as Google apps, Dropbox, and Foursquare only in regards to matches that occur during calls. This is so we can maintain and provide you a history of matches for all your calls made using Second Mind.

3. **Aggregated Statistics.** Second Mind may collect statistics about the behavior of visitors. Second Mind may display this information publicly or provide it to others. However, Second Mind does not disclose personally-identifying information other than as described below.

<u>Sharing and protection of your personally-identifying information</u>

1. **Second Mind Customers.** When you register to Second Mind as a business or user, no one else will have access to your personal information.

2. **Employees.** As a general rule, Second Mind's employees and service providers do not monitor, review or listen to your meeting information that is recorded and stored by our Services; however, we list below the limited circumstances in which our employees and service providers will access or review your meeting information:
   a. We need to do so to evaluate problems with the quality of our voice recognition.
   b. We need to do so for other troubleshooting purposes

3. **Compliance and Law Enforcement.** Second Mind discloses potentially personally-identifying and personally-identifying information only to those of its employees, contractors and affiliated organizations that (i) need to know

that information in order to process it on Second Mind's behalf or to provide services available at Second Mind's websites, and (ii) that have agreed not to disclose it to others. Some of those employees, contractors and affiliated organizations may be located outside of your home country; by using Second Mind's service, you consent to the transfer of such information to them. Second Mind will not rent or sell potentially personally-identifying and personally-identifying information to anyone. Other than to its employees, contractors and affiliated organizations, as described above, Second Mind discloses potentially personally-identifying and personally-identifying information only when required to do so by law, or when Second Mind believes in good faith that disclosure is reasonably necessary to protect the property or rights of Second Mind, third parties or the public at large. Second Mind takes all measures reasonably necessary to protect against the unauthorized access, use, alteration or destruction of potentially personally-identifying and personally-identifying information.

4. **Security of Billing Information.** When you enter sensitive information such as credit card number on our registration or order forms, we encrypt that information using secure socket layer technology (SSL). We follow generally accepted industry standards to protect the Personal Information submitted to us, both during transmission and once we receive it. No method of transmission over the Internet, or method of electronic storage, is 100% secure, however. Therefore, we cannot guarantee its absolute security. We will make any legally required disclosures of any breach of the security, confidentiality, or integrity of your unencrypted electronically stored "personal data" (as defined in applicable state statutes on security breach notification) to you via email or conspicuous posting on our website and mobile application in the most expedient time possible and without unreasonable delay, insofar as consistent with (i) the legitimate needs of law enforcement or (ii) any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

5. **Phishing**. Identity theft and the practice currently known as "phishing" are of great concern to Second Mind. Safeguarding information to help protect you from identity theft is a top priority. We do not and will not, at any time, request your credit card information, your login information, or national identification numbers in a non-secure or unsolicited e-mail or telephone communication. For more information about phishing, visit the Federal Trade Commission's website at http://www.ftc.gov.

6. **International Transfer.** Your information may be transferred to and maintained on computers located outside of your state, province, country or other governmental jurisdiction where the privacy laws may not be as protective as those in your jurisdiction. If you are located outside the United States and choose to provide information to us, Second Mind transfers Personal Information to the United States and processes it there. Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

Application Security

Second Mind's products have multiple built-in features to help further secure our customer and partner data. These occur at the data model, voiceprint, and application level.

Data Model. Our data model has been specifically designed to not support the storage and transfer of any personally identifiable information, other than what is considered bare minimum.

Voiceprints. Our voiceprints are natively secure. Voiceprints are not voice recordings. They are mathematical models of the unique elements of a person's speech which are derived from a "feature extraction" process. Voiceprints can't be listened to and cannot be reverse-engineered into speech. We use a proprietary voiceprint data storage format that is not published and which can only be interpreted by Second Mind's voice biometric engine. So, in the highly unlikely event that someone ever obtained a Second Mind voiceprint, there is nothing they could do with it. Also all personally identifiable information in Second Mind's system is fully encrypted at the application level.

Data Retention

Any of the personal data captured by any of our applications are only retained as long as a customer or partners is engaged with Second Mind's services.

Policy towards children

Second Mind's website application are not directed to individuals under 18. We do not knowingly collect personally identifiable information from children under 13. If a parent or guardian becomes aware that his or her child has provided us with Personal Information without their consent, he or she should contact us. If we become aware that a child under 13 has provided us with Personal Information, we will delete such information from our files.

Privacy policy changes

Although most changes are likely to be minor, Second Mind may change its Privacy Policy from time to time, and in Second Mind's sole discretion. Second Mind encourages visitors to frequently check this page for any changes to its Privacy Policy. Your continued use of this site after any change in this Privacy Policy will constitute your acceptance of such change.

Contact us

If you have any questions about this policy, please contact us at contact@SecondMind.ai.