EQUAL TIME

Equal Time (Equalicert Inc) takes your privacy and security seriously. We are proud to use the highest standards of security and privacy in our software development practices and data storage.

How does the Equal Time technology work?

- For users who use Equal Time's Zoom App, we use "active speaker detection" which is part of the API from Zoom. This essentially is like a timestamp that shows when speakers start speaking and stop. In Google Meets, we use active speaker detection as well, which comes from the front-end user interface.
- Equal Time's Zoom App is limited to reading information. It does not modify, add or delete meeting information or user information. Our app uses the following three scopes: *zoomapp:inmeeting, meeting:read, and user:read*.
    - The *zoomapp:inmeeting* scope makes our app available for use in Meetings.
    - The *meeting:read* scope allows our app to view a user's meeting information. This includes meeting reports, participants, polls, and registrant information.
    - The *user:read* scope allows our app to view a user's profile information. This includes information such as user settings, the user's permissions, user tokens that allow the user to join a Meeting SDK meeting, and the user's scheduling privileges.

- For users who use Equal Time with a Calendar Connection, a bot notetaker joins calls and automatically records audio from the meeting. We use a transcription service (from AssemblyAI) to generate a transcript. We then run AI data analysis on the transcript, leveraging OpenAI's GPT API. This allows us to detect the frequency of questions, and to generate a useful summary of the meeting.
- Meeting data is NOT used to train OpenAI's model. Read more here. We use the API, and this data is private and secure.
- The audio file of the meeting is automatically deleted after 7 days. Equalicert Inc maintains the only copy of the meeting transcript on our secure servers, which users can request to be deleted at any time.
- We do not create or store a video file of any meetings.
- Any meeting participant, even if they are not an Equal Time user, can request that the meeting recording be halted at any time during the meeting by clicking on a link sent in the Zoom and Google Meet chat, or to the user by email at the start of the meeting.
- Meeting participants, even if they are not Equal Time users, can request that meetings where they were in attendance be deleted in compliance with GDPR by emailing legal@equaltime.io.
- Equal Time users may edit or delete meeting transcripts from their own dashboard at any time. They can also email a deletion request for single meetings, several meetings, or their full account and meeting history by emailing legal@equaltime.io.

What data is visible to whom?

- Individuals who are Equal Time users have access to transcription, and full data analytics detail of all meetings they hosted or participated in.
- If an organization has adopted Equal Time, company leaders have access to aggregate meeting data and group trends. Company leaders can review inclusion KPIs in order to track progress and take appropriate action. Aggregate data may include (but may not be limited to): speaking time by gender, monologues, frequency and level of severity of inappropriate language, sentiment, and number of questions asked.
- Organizations on an Enterprise license have the opportunity to send Equal Time a CSV containing employee data and request that we customize their "Company Dashboard". This enables leaders to track aggregate speaking time by seniority level, geographic location, native language, or other dimensions.
- Company leaders with Admin privileges may read the meeting transcripts and AI-analysis for users within their organization.

Privacy. We safeguard privacy by design.

- We are 100% GDPR and CCPA compliant.
- We collect only the minimum data necessary for clients to use the application. We collect email addresses and screen names from users, which are considered to be PII and are stored with utmost caution. As this is sensitive data, by request, we can store it in the correct region and country based on the customer's location (US, Europe, etc)
- We will never sell or share personal information with a 3rd party.
- Published privacy policy (link)
- Please inquire if you require SSO in your organization.

EQUAL TIME

Security. We protect your data and defend against cybersecurity threats.

- All customer data is encrypted at rest with AES-256 and in transit via TLS.
- Sensitive information like access tokens and keys are encrypted at the application level before they are stored in the database.
- Our database is SOC2 compliant.
- We have row-level security to protect each user's data.
- We restrict access to production resources and log all changes and access to production data.
- Our infrastructure is built on Microsoft Azure and Supabase, and leverages their built-in security protocols and best practices.
- We backup our data every day to protect user data from unauthorized deletion.
- We use a secure software development process, also known as SSDLC (link)
- We enforce secure coding practices based on industry standards like OWASP. We use DeepSource to automatically review code for bug risks, anti-patterns, performance issues, and security vulnerabilities.
- Our application uses SAST (Static Application Security Test) and/or DAST (Dynamic Application Security Test).
- Our database undergoes regular penetration tests.
- We monitor performance and reliability 24/7.
- Equal Time's Vulnerability Management Policy (link)
- Infrastructure Management Policy for Patching Systems (link)
- Equal TIme's Incident Management Process (link)

Training. All employees with access to customer data have had Privacy and Security training.

EQUAL TIME

Disclosure Policy

- If you believe you've discovered a potential vulnerability, please let us know by emailing us at support@equalicert.com. We will acknowledge your email within 24 hours.
- Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within one week of disclosure.
- Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the Equal Time service. Please only interact with accounts you own or for which you have explicit permission from the account holder.

Please email us if you have any questions.

Sincerely,

Rachel Dowling CEO (rachel@equaltime.io)
Kim LaRocca CTO (kim@equaltime.io)