

Privacy Policy

Initial Effective Date: Jun 1, 2026

Latest Revised Date: Jun 1, 2026

This Privacy Policy outlines the scope of processed data and the ways we treat your data received through our Service. Together with the Terms of Use, this Policy stands for the foundation of our binding relationship.

Before we start, here is the list of the crucial considerations about our Services and your data:

1. The main interaction with our Services is you having conversations with our AI chatbot. We designed the AI chatbot to provide a conversational experience, different coping techniques tailored to your requests and needs.
2. We may process sensitive information like information about your health, emotions, feelings, or well-being, but we collect it to the extent necessary for the Services functionality and the delivery of the personalized content. Such type of content is visible to you only. It remains private unless you decide to share this information outside the Services.
3. We follow industry best practices for data protection and are HIPAA-compliant, ensuring the privacy and security of your health-related information. Our security infrastructure is designed to safeguard your data throughout its lifecycle. We process your information solely for the purpose of delivering and improving our Services. If we ever intend to use your data for any other purpose, we will first request your explicit consent.
4. We do not share or sell your personal data to any advertisers.

We hope you find all necessary details to be assured your personal data is safe.

What Data Do We Process?

First let's break it down: what is personal data (or information) and what is processing in general, and how are we handling it all in the CSS Sidekick App.

What is Personal Data?

Personal data or personal information is any information relating to you that, alone or in combination with other pieces of information, could reasonably be linked, directly or indirectly, with you.

For example, other servicers may collect your name, alias, email address, ID identifiers, audio, electronic, visual, or similar information, etc. Personal data could also include internet and other electronic network activity information such as IMEI (International Mobile Equipment Identity) or MAC addresses, IP addresses, time zone, browser type, or system information. There are also some types of personal information, like data collected and analyzed concerning a consumer's health, sex life, or sexual orientation; mental or physical health condition or diagnosis; religious beliefs; personal data of a known child; or precise geolocation data. Such data should be

treated with special caution, as, depending on the context, it mostly constitutes sensitive information or personal health information (PHI).

What is Processing?

Personal data processing means any action with it, for example, collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and even turning it into anonymized data.

How Do We Process Your Personal Data?

The CSS Sidekick App collects only data necessary for Services functionality.

However, there are different situations when you may decide to share more data, or we are requesting some information from you. Find the data types, the justification, and the ways of such processing cases below:

Type of data	Processing reasons	Lawful Basis	Notes to Processing
Email address	To set up an account	Execution of the contract	Occurs during registration
User ID	User IDs are used to perform A/B testing	Controller interest	We do not tie your email to our internal processes. We generate a unique identifier for you, as such use enhances your email privacy
Information related to your mood, general well-being, feelings, or any other thoughts	To process inbound messages, analyze them and deliver personalized content	Execution of the contract	Occurs during conversations with the AI chatbot while we deliver conversation output or personalized content to you
Sensitive personal information, or personal health information, including about mental health	To process inbound messages, analyze them and deliver personalized content	Consent	Occurs during conversations with the AI chatbot while we deliver conversation output or personalized content to you
Email address, full	To process feedback,	Execution of the	We process this data

name or nickname, the content of the email	or feature suggestion, received from you via email	contract	if you are reaching out to us via email for solution suggestion, complaints, or claims
Email address, results of the interviews	To run in-depth interviews, questionnaires	Controller interest (when we make a list of users whom to question), consent (when we directly ask you to participate in the interview/fill in questionnaire)	We may use such data to improve our Services. If you agree to such an interview, we may offer you discounts or other benefits
Postal code, address, signature, full name. or nickname	To enable refunds or any inquiries received at our physical address	Execution of the contract	We may process it either for refund purposes or any Services-related mail if you decide to send it by post
Email address	To inform you about technical updates and new features	Controller interest	Once we launch new features, significantly update our Services, or solve technical inaccuracies
Log data of your usage of the Services	To analyze how you interact with our Services	Controller interest	We may analyze how you tap, for how long and how often you interact with the content, and your usage frequency and preferences
Email address	To send you newsletters to promote our products and services	Consent	Once you opt in to the newsletter in the Settings section of the Services
(Only anonymized to the maximum extent possible) conversational data about your mood, preferences, worries, reflections, or symptoms alongside language preferences, time of	To train our model for improving existing models, delivering more tailored result	We do not need a legal basis for processing the anonymized data	We run the AI trainings once we delete all possible identifiers of your personal data. Please note , that once anonymized, data that cannot be attributed to the user is no longer

the conversation			“personal”
------------------	--	--	------------

Data Disclosure to Third Parties

We want to reassure you that we do not sell or share data with third parties for commercial purposes, such as advertising. However, we work with some third party service providers under the respective contracts to deliver and improve our Services. We only share the minimum amount of data necessary for each Service to function properly. See the breakdown below:

Service provider	Type of provider	Purpose of disclosure	Data shared
OpenAI (USA)	AI Services	AI content generation	Messages, preferences, age group, and onboarding information.
Anthropic (Claude) (USA)	AI Services	AI content generation	Messages, preferences, age group, and onboarding information.
Google Cloud (USA)	Infrastructure	Server hosting and data storage	All processed data, messages, and account information (email).
Sentry (USA)	Technical	System stability monitoring and error reporting	Device information, language preferences, app version, error logs, location (city/country), timezone, hours format, device information, and IP address.
RevenueCat (USA)	Payment	Subscription management (App Store/Google Play)	User ID, country location, history of logs to the Services (last opened, first used), timezone, subscription status, and purchase history.
Mixpanel (USA)	Analytics	App usage analytics	User ID, age group, IP address, city, usage patterns.
AppsFlyer (USA)	Analytics	Deep link generation	No personal data (link clicks information only).
Flagsmith (UK)	Optimization	Conducting A/B testing	User ID only.

SendGrid (USA)	Communication	Email notifications	Email address only.
Firebase (USA)	Communication	Push notifications and analytics	Device information, notification preferences, usage data, user ID, age group, IP address, city, usage patterns, timezone, hours format, and device information.

We follow the principle of data minimization. This means we only share the absolute minimum data required for each service to work properly. For example,

- error reporting service provider is only able to process technical information needed for the quality assurance, it does not receive the gist of your conversation or your email address;
- analytic service providers receive aggregated, often anonymized usage data; and
- AI service providers receive the content necessary to generate your personalized responses only.

Please note, if you contact us through third party providers, such as other messengers or our social media, you are subject to their Terms of Use. We do not control how these providers process your data.

Our Security Framework

We take the security and protection of your personal data seriously. We work closely with our Information Security Officer to ensure the safety of your data and our Services. If you have any suggestions or questions, please reach out to us at info@css-pa.org.

PIN

You can set up a secure and convenient PIN code. We encourage you not to use your date of birth, sequential numbers, or other “easy-to-guess” codes which are not strong enough to protect your account from misuse.

Session Management

We use a secure session system with refresh and access tokens to protect your account. If you do not log into the system for two weeks, you will be automatically logged out. This prevents inactive sessions from being misused.

Data Retention Periods

For active users:

If you decide to delete your account, we maintain a **30-day freezing period** for your convenience. This allows you to restore your account if you change your mind. After 30 days, all associated data will be permanently deleted.

You have full control over your conversational data. When you delete your account, all related messages and communications will also be permanently erased.

Please keep in mind that we may still process anonymized data even after your data is deleted. Once anonymized, the data no longer qualifies as personal data under privacy regulations. We may use such **anonymized data for system improvement and training**, ensuring identifying information is removed before processing.

Technical and Organizational Security Measures

We implement a layered security approach to protect personal data and ensure the confidentiality, integrity, and availability of our systems. These technical safeguards are continuously reviewed and improved to maintain alignment with industry best practices, including those outlined in SOC 2 and HIPAA.

Data Encryption

- All communication between clients and servers is secured using HTTPS with TLS 1.2 or higher.
- All data stored in databases and cloud storage is encrypted using Google Cloud's native encryption mechanisms, with secure key management practices.
- Authentication data, such as PIN codes, is stored using one-way cryptographic hashing.

Identity and Access Management

- Access to production systems and data is restricted based on predefined security groups and job responsibilities.
- Privileged access is limited to authorized personnel and reviewed regularly.
- Regular audits are performed to verify access rights and remove outdated privileges.
- All access to sensitive systems and data is logged and monitored for anomalies.

Infrastructure and Application Security

- Infrastructure components follow secure baseline configurations managed via automation and configuration management tools.
- Network traffic is filtered through firewalls and access control layers, while backend systems are logically isolated by design.
- All infrastructure and application changes are tracked in a centralized issue management system with approval workflows.
- Web Application Firewalls and Intrusion Detection Systems monitor and filter inbound and outbound traffic for threats.

Threat and Vulnerability Management

- Automated scans are performed weekly to identify known threats, which are triaged and remediated based on severity.
- We use enterprise-grade tools to continuously monitor system performance, latency, and security events.
- We maintain a documented incident response plan, which includes detection, containment, remediation, communication, and post-incident reviews.

Compliance, Risk, and Governance

- Security operational risk assessments are conducted at least annually. Results are logged, prioritized, and tracked in a formal risk register.
- We perform continuous control monitoring and testing to ensure controls are operating effectively.
- Policies and procedures are reviewed, approved, and redistributed annually.

HR Security

- All new hires must pass a background screening prior to onboarding.
- All team members complete security awareness training during onboarding and annually thereafter, including incident reporting procedures and best practices.

Business Continuity

- Encrypted backups are performed regularly and tested to ensure data can be restored in the event of disruption.
- A formal Business Continuity Plan is in place and tested annually through tabletop exercises.
- System resource usage is continuously monitored to ensure scalability and availability.

Vulnerability Disclosure

We take security seriously and encourage responsible disclosure of any vulnerabilities found in our applications or infrastructure. If you believe you've discovered a security issue, please report it to us at info@css-pa.org. We appreciate your contribution to keeping the CSS Sidekick App safe.

Your Data Processing Rights

You as a user have various rights. Find how they are enforceable below:

Scope of the Right	Enforcement in practice
Right to be informed means that you have the right to know how we collect, use, and share your personal information before we do it.	We must provide you with clear, comprehensive Privacy notices (policies) like this one and provide you with the Terms of Use.
Right of Access enables you to ask us for a copy of all the personal information we have about you.	You can request to see what data we have collected, where it came from, and how we are processing (using) it.
Right to Rectification means if any of your personal information is wrong or incomplete, you can ask us to fix it.	You can contact us to correct the email in your profile. Likewise, you will be able to update outdated information or mistakes or add missing details, so the Services will deliver more personalized replies.
Right to Erasure (Right to be forgotten) allows you to make us delete your	You can request deletion when the information is no longer needed, for example, you want to

personal information completely.	delete the data or account overall.
Data Portability means you can get your personal data in a format that allows you to easily move it to another service, for example.	We must provide your data in a common, machine-readable format (like CSV or JSON files) so you can transfer it elsewhere.
Right to Opt Out outlines several options to withdraw your consent out of: • Sale, meaning to object against the selling of your data to other companies for money or other benefits. • Targeted advertising, meaning you choose not to receive personalized ads based on your personal information.	CSS does not conduct any of these actions, so you can be sure we do not sell your data, do not target it with any ads, sell to advertisers, or sell overall.
Right to Opt Out of automated decision-making and/or profiling , meaning to object against AI systems making important decisions about you without human involvement where such decisions significantly influence your rights and obligations.	The aim of our AI application is to build the conversation around your scope of interest in mental health topics only. You can contact us to explain to you the available user controls.
In terms of opting out of processing your sensitive data , you can stop providing us with the sensitive information.	You solely decide to share your sensitive information with us or not. We will not push you toward sensitive topics unless you decide to raise the issue in the conversation with our AI chatbot.
The general right to opt out i.e., the consent withdrawal or opting out of newsletters , means that you can stop using our Services or refuse to receive the emails accordingly.	You can easily withdraw your consent. It will lead to the deletion of all your data or your account overall. Find more details about retention periods in Our Security Framework Chapter of this Privacy Policy.

How to Exercise Your Rights

Some rights can be exercised directly through our Services. Simply navigate to Settings to manage your preferences, adjust privacy controls, or delete your data.

For additional requests or inquiries, please contact us at info@css-pa.org. This might include, but is not limited to:

- changing the email associated with your registration;
- requesting access to all data we retain about you;
- seeking further clarification on security, data retention, or AI processing features toward data processing; or

- any other privacy-related concerns.

The Response Standard

We acknowledge receipt of your request within 10 business days and reserve 45 calendar days to respond. We may also extend the response time, adding 15 more calendar days, notifying you promptly.

Regardless of your location, if your request does not require additional information or is not complex, we typically aim to provide a response in less than **5** days.

To process your request efficiently, we may require additional information to verify your identity and the nature of your request. If needed, we will reach out to request further details.

Please note that using VPN services may impact our ability to timely process your request.

Sometimes your request might be unenforceable

In some cases, we may refuse to fulfill your request. This can happen if:

- the request is unclear or not directly related to your own data;
- it may be restricted due to legal requirements or specific case-by-case limitations;
- your data has already been permanently deleted.

If we are unable to process your request, we will inform you promptly and provide further details where applicable.

Our Contacts and Inquiries

CSS Sidekick APP is operated by Consumer Satisfaction Services, Inc.

If you have any privacy-related inquiries, please contact us directly at info@css-pa.org.

For any other questions, comments, or feedback related to the Services, as well as any complaints or claims about them, please contact us directly through our contact number (717) 651-1070 or by email at info@css-pa.org.

Changes to this Privacy Policy

We may amend this Privacy Policy from time to time. If we decide to do so, we will update this Policy to align it with the changes. You will be able to see the last revised date on the top. The logs of previous versions of the Policy will also be maintained at the bottom of the page. If the updates are significant and materially impact your experience, we will notify you via push notifications in the app or by email.

By continuing to use our Services after the changes take effect, you acknowledge and agree to the updated Privacy Policy. Once you find the amended Policy contradicts your beliefs or privacy concepts, you may seek the refund or cancellation of the subscription. Find more about cancellation and refunds in our Terms of Use.

Changes Log

I. Date: _____

What has changed:

- 1.
- 2.
- 3.

II. Date: _____

What has changed:

- 1.
- 2.
- 3.