

Welcome to the Mendi Privacy Notice

Mendi Innovation AB respects your privacy and is committed to protecting your personal data.

“Personal data” means any information relating to an identified or identifiable natural person.

This privacy notice aims to give you information on how we collect and process your personal data when you visit or use our mobile app (“Mendi app”, “App”, “Application”), coupled with the usage of Mendi’s headset sensor and inform you about your privacy rights and how the law protects you.

Users under the age of 16 years may not create, register or use a Mendi account without parent's or guardian’s permission and supervision.

The Mendi app does not currently include hyperlinks to external or third-party websites, pages, or services. If such hyperlinks are introduced in the future, please note that this Privacy Notice will not apply to any third-party sites accessed through those links. By clicking on a hyperlink, you may allow the third-party to collect or share data about you. Mendi Innovations does not control, and is not responsible for, the content or privacy practices of any third-party websites.

We recommend reviewing each third-party’s Privacy Policy before providing any personal information.

What is Mendi

Mendi is the Service (“the Service” or “Services”) designed and developed by Mendi Innovation AB (“Mendi,” “us,” “we,” “our,” the “Data Controller”) that processes Personal Data collected from the Mendi headband sensors using proprietary algorithms to provide simple, visually comprehensible, and easy-to-learn local feedback signals directly in the Mendi mobile App (“the App”). A key aspect of our technology is that it measures the brain’s response to changes in activation, enabling more efficient and precise neurofeedback training.

Everything is clearly explained and trackable within the App, making brain training accessible and enjoyable for users. If you want to learn more about our technology and the science behind it, please visit <https://www.mendi.io/pages/science>.

We do not process Personal Data for automated decision-making activities. You retain full discretion over whether to follow the suggestions provided by the application.

Data controller

Mendi Innovation AB, Reg. No 559075-4510, Östermalmsgatan 26A, 114 26 Stockholm, Sweden is the Data Controller ("Controller") for the use and processing of your personal data as described in this Privacy notice.

Data protection officer

We have appointed a Data Protection Officer ("DPO") who is responsible for overseeing our privacy practices and our compliance with the General Data Protection Regulation ("GDPR"). You can contact the DPO at the following email: mendi-dpo@chino.io.

What data we process

Whenever you access or use our Service, we may process (e.g. collect, use, store, transfer) different categories of personal data about you, including data concerning your health. We process personal data only to the extent necessary to provide a functional Service. We do not process personal data relating to criminal convictions and offenses (Art. 10 GDPR).

Category of personal data processed	Data items processed
Identification Data	First name, Surname, Email, Username, User ID, IP addresses
Personal Characteristics	Gender, Date of Birth
Mendi Headset Raw Data Please note that this category includes sensitive health-related personal data as defined under Article 9 of the GDPR.	Blood oxygenation data from the prefrontal cortex and - to ensure robust signal accuracy and reliability - metrics such as head motion and orientation, superficial blood oxygenation in skin and muscle tissue, temperature, and ambient light.
Wellness Data and Measurements Please note that this category includes sensitive health-related personal data as defined under Article 9 of the GDPR.	Computed blood oxygenation levels in your prefrontal cortex
Training goals and notes Please note that if you include such information, it may constitute sensitive data (e.g., health-related data) under Article 9 of the GDPR.	Personal goals, specific distractions that affect you, notes about your sessions to record progress, emotions, and other pertinent details. Please note that if you include such information, it may constitute sensitive data (e.g., health-related data) under Article 9 of the GDPR.
Mental health data	Answers to questionnaires about Mental health.

Category of personal data processed	Data items processed
Please note that this category includes sensitive health-related personal data as defined under Article 9 of the GDPR.	
User Feedback	Feedback on app features and performance metrics (such as NPS and CSAT)
Log and Usage Data	Log usage data such as device carrier details, configuration data, user interaction metrics, usage patterns, and specific device attributes (e.g., phone model, operating system, brightness settings, and battery level).
Progress data	Your progress during Mendi training sessions, capturing performance metrics such as your Mendi Score.

How we collect your data

Data collected via direct interactions: You may give us your personal data (sensitive data included) when using our Services, by filling in forms or by corresponding with us by post, email or otherwise.

This includes personal **data you provide** when you:

- create an account on our App;
- use our Services;
- give us feedback or contact us.

Third parties data: We will receive your signup and log in information from Google or Apple should you choose to sign up to our Service using your personal Gmail account or Apple ID.

Computed data: These are the wellness data and measurements that we calculate with our proprietary algorithms starting from the collected Mendi Headset Raw Data.

How we use your personal data

We use your Personal Data for the following purposes:

Provide the Service

Purpose: provide you the Service as described in our terms and conditions (e.g. Creation of User Account; Provision of brain exercises, lifestyle recommendations and training materials based on your brain activity measurements, age and goals for training; Creation of potential wellness status measurements based on the analysis of the levels of your brain's blood oxygenation; notify you of any available new App versions; Communicate with you when you need support with our Services; Resolve bugs and issues that you might encounter when using our App).

Types of data	Legal Basis
<ul style="list-style-type: none"> • Identification Data • Personal Characteristics • Mendi Headset Raw Data • Wellness data and Measurements • Training goals and notes • Log, Usage and Progress Data 	Performance of the contract - Art. 6(1)(b) GDPR. Special categories of personal data (e.g. health related data) require an exception to be processed, and that is your explicit consent - art.9(2)(a) GDPR.
Are you required to provide your data?	
<p>While most data points are optional, providing a valid email address is required to create an account and access our Service. User IDs are automatically generated and managed by our system, ensuring seamless account identification. Additionally, our infrastructure logs and processes IP addresses to maintain security and deliver core functionalities.</p> <p>To use the primary features of our Service - neurofeedback brain training - you must consent to the processing of Mendi Headset Raw Data and Wellness Data & Measurements. These data points are essential for delivering personalized neurofeedback experiences.</p> <p>You may withdraw your consent at any time by contacting us or by deleting your account, which will permanently remove your data from our systems.</p>	

Mental Health Self-Evaluation

Purpose: Provide you with an additional and optional service that can help you Self-Assess and track your Mental health while using our App.

Types of data	Legal Basis
<ul style="list-style-type: none"> • Identification Data • Mental health data 	Performance of the contract - Art. 6(1)(b) GDPR. Special categories of personal data (e.g. health related data) require an exception to be processed, and that is your explicit consent - art.9(2)(a) GDPR.
Are you required to provide your data?	
<p>Participation is entirely voluntary. You always have the option to decline completing surveys or opting in to provide this information. In order to access this functionality you must explicitly consent to the processing of your sensitive data (mental health data). You may withdraw your consent at any time by contacting us or by deleting your account, which will permanently remove your data from our systems.</p>	

Improving Mendi

Purpose: Collect and aggregate demographic and statistical data in order to improve our Services.

Types of data	Legal Basis
<ul style="list-style-type: none"> • Identification Data • Usage data 	Our legitimate interest (Art 6 (1) (f) GDPR) in improving our Services.
Are you required to provide your data?	

Types of data	Legal Basis
<p>These data categories are processed to collect aggregated statistic about the usage of our Services. They are then used for the purpose of improving and developing our Services only in their aggregated form.</p> <p>We collect this data automatically when you use our App. In any case, you may oppose the processing at any time by contacting us.</p>	

Improve our Services by collecting your suggestions and feedback.

Types of data	Legal Basis
<ul style="list-style-type: none"> • Identification Data • User Feedback 	<p>Your consent to providing feedback (Art. 6 (1) (a) GDPR; and 9 (2) (a) in case you decide to include sensitive data in your feedback).</p>
<p>Are you required to provide your data?</p>	
<p>The provision of feedback data is entirely voluntary.</p>	

Safety and Security

Purpose: When necessary, we may use your personal data to promote the safety and security of our Services and our users. We may use your personal data to monitor operations, authenticate users, detect and protect against fraud and other criminal activity and enforce our Terms and Conditions and other policies.

Types of data	Legal Basis
<ul style="list-style-type: none"> • Any data necessary to achieve this purpose. 	<p>Our legitimate interests (Art. 6 (1) (f) GDPR) when processing personal data in detecting and preventing fraud and illegal conduct or, if necessary, for complying with a legal obligation to which we are subject.</p>

Manage and Defend Legal Claims

Purpose: If necessary we may use your personal data to manage and defend legal claims, e.g. in connection with a dispute or a court proceeding. We will in such a case process the personal data collected which is necessary in order to manage and defend the legal claim in question.

Types of data	Legal Basis
<ul style="list-style-type: none"> • Any data necessary to achieve this purpose. 	<p>Our legitimate interest (Art. 6 (1) (f) GDPR) in managing and defending legal claims.</p>

Fulfill Legal Obligations

Purpose: We may use your personal data to fulfill legal obligations that we have, e.g. accounting requirements or obligations under data protection laws.

Types of data	Legal Basis
<ul style="list-style-type: none"> Any data necessary to achieve this purpose. 	We will in such a case process the personal data collected which is necessary in order to fulfill the legal obligation in question (Art. 6(1)(c) GDPR).

We do not process your personal data for other purposes other than the ones stated in this Notice. If we need to process your data for another purpose we will inform you and, if necessary, we will ask for your consent.

How We Share Your Data

We will only share your personal data in connection with providing you with the Service as agreed per our Terms and Conditions.

In general, we do not disclose the personal data about you to third parties without your consent or otherwise as specified in this policy.

The circumstances in which we may disclose or share your personal data under this policy, include as follows:

- Lawful requests: we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- Third-Party Data Processors: We leverage trusted third-party service providers, to facilitate specific data processing functions on our behalf. These providers act as our authorized data processors, supporting:
 - Analytics & User Insights: Collecting and analyzing user interactions to improve our product experience.
 - Customer Engagement & Messaging: Overseeing feedback collection, app update notifications, and personalized communications to enhance user engagement and experience.
 - Data Hosting & Infrastructure: Securely storing and processing data to ensure platform reliability and performance.

When acting as our authorized data processors, they are required to only process data in accordance with our instructions and are subject to appropriate legal, confidentiality and security obligations.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. Our third-party service providers may only process your personal data for specified purposes and in accordance with our instructions and are not permitted to use your personal data for their own purposes.

Storage location and International Transfers

We transfer your Usage Data to the US and we rely for this on specific providers based in the US. These providers are covered by the EU-US Data Privacy Framework. All the other categories of data are stored in the EEA and we rely on trusted service providers for this. However, these service providers could have access to the data

form outside the EU for the provision of some services. In this case, the transfer occurs in accordance with the safeguards set out in Chapter V of the GDPR (adequacy decision or, in the absence, on the basis of the Standard Contractual Clauses adopted by the EU Commission). If you wish to know more about these transfers please contact us.

How We Protect Your Data

At Mendi, we implement industry-leading security practices to protect your personal data, ensuring compliance with GDPR and other relevant data protection regulations. Our data handling follows the highest security standards, incorporating both technical and organizational safeguards to prevent unauthorized access, misuse, or unlawful disclosure.

Security Measures We Implement:

- **Encryption & Secure Storage:** Personal data is encrypted both in transit (e.g., SSL/TLS) and at rest using industry-standard encryption protocols.
- **Access Controls:** Access to personal data is strictly limited to authorized personnel on a need-to-know basis.
- **Infrastructure Security:** We employ physical, electronic, and procedural safeguards aligned with best practices to ensure data integrity and protection.

While we take rigorous steps to safeguard your data, no method of storage or transmission is entirely foolproof. We cannot guarantee absolute security but we aim to continuously improve our protocols to minimize risks.

Data Retention

Mendi retains personal data only for as long as necessary to fulfill the purposes for which it was collected, including compliance with legal, tax, and accounting obligations. In certain cases, an extended retention period may be required due to legal claims or disputes related to contractual obligations.

Retention Period Determination Factors:

We assess the appropriate retention period based on:

- **Purpose & Necessity:** Whether the data is still required for its original purpose or if the objective can be achieved by other means.
- **Data Sensitivity & Volume:** The nature, scope, and sensitivity of the personal data.
- **Risk & Security Considerations:** The potential risk of harm from unauthorized access, use, or disclosure.

If processing is based on consent, personal data will be retained until consent is withdrawn. If no longer required for our legitimate interests or legal obligations, and no alternative legal basis applies, the data will be permanently deleted.

Your Privacy Rights

EU users' privacy rights

Right	Description
To Access Your Personal Data	Request access and a copy of stored personal data. Viewable in user account or by request.
To Update Your Personal Data	Request correction or completion of incorrect/incomplete data. Updatable in user account or by request.
To Withdraw Consent	You may revoke your consent at any time by contacting us or simply by deleting your account. Doesn't affect previous processing legality.
To Delete Your Personal Data (Right To Be Forgotten)	Request user account deletion. Request data deletion under certain circumstances. May affect service use. Data may be kept for legal obligations or claims.
To Restrict The Use of Your Personal Data	Request restriction under certain circumstances. Platform unusable during restriction.
To object to the processing of your personal data	Object to processing based on legitimate interest for specific situations. Processing will stop unless we have an overriding interest or legal claims.
To transfer your personal data (Data portability)	Obtain a copy of provided information in a structured, machine-readable format for transfer.

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at the email address below.

As a data subject, you have a right to lodge a complaint with the competent supervisory authority under the conditions provided in Article 77 GDPR or seek a remedy in the national courts if you think that your rights in relation to your personal data have been breached.

However, we would be grateful if you could give us the opportunity to address your complaint in the first instance by using the contact details provided in the following section.

Contact us

If you have questions, suggestions, or concerns about this Policy, or about our use of your Personal Data, please contact us at **privacy@mendi.io**.

Privacy Policy Update

If we make substantial changes to this Privacy Notice (or the App) that affect your privacy and confidentiality, we will notify you by email or display information in the App and ask you to read it.

This version was last updated on 13/04/2026.

US users' privacy rights

You, as the subject of personal data, have some specific privacy rights. To exercise them, write us an email at privacy@mendi.io.

Your rights vary depending on the laws that apply to you but may include:

- The right to be informed about the personal data we collect and/or process about you;
- The right to learn the source of personal data about you we process;
- The right to access, modify, and correct personal data about you;
- The right to know with whom we have shared your personal data, for what purposes, and what personal data has been shared (including whether personal data was disclosed to third parties for their direct marketing purposes);
- The right to withdraw your consent, where the processing of personal data is based on your consent; and
- The right to lodge a complaint with a supervisory authority located in the jurisdiction of your habitual residence, place of work, or where an alleged violation of law occurred.

Please see more detailed information about your state's privacy data protection laws in a separate section; you can find it in the navigation on the right of the page.

Virginia's Consumer Data Protection Act	Consumer Privacy Act and California Privacy Rights Act	Colorado Privacy Act	Nevada Privacy Law	Delaware Online Privacy and Protection Act Delaware Online Privacy and Protection Act
Right to Know whether the Controller is processing a customer's personal data.	Right to Know what personal information is collected and Right to Access personal information.	Right to Access Information.	Right to Know whether the Controller is processing the customer's personal data.	Right to Access Information.
Right to Access personal data processed by the Controller.	Right to Know if Personal Information is Sold.	Right to confirm the processing of personal data.	Right to opt out of Sale.	Right to withdraw consent.
Right to Correct.			Right to Correct.	Right to Correct.

Virginia's Consumer Data Protection Act	Consumer Privacy Act and California Privacy Rights Act	Colorado Privacy Act	Nevada Privacy Law	Delaware Online Privacy and Protection Act Delaware Online Privacy and Protection Act
Right to Erasure. Right to Data Portability. Right to opt out of targeted advertising, the sale of personal data, or profiling.	Right to Erasure. Subject to certain exceptions. Right to Data Portability. Right to Correct. Right to opt out of Sale. Right to Limit Use and Disclosure of Sensitive Personal Information.	Right to Access information. Right to Correct. Right to Erasure. Right to Data Portability. Right to opt out of targeted advertising, the sale of personal data, or profiling via a universal opt out mechanism.		Right for "do not track" request Right to opt out of Sale.

What do these rights mean?

1. **The right to access information.** You can request an explanation of the processing of your personal data: what data exactly we process and how.
2. **The right to withdraw consent.** After you once give us any consent, you can withdraw it at any time without any consequences for you.
3. **The right to portability.** You can request all the data you provided to us and request to transfer data to another Controller in a machine-readable format.
4. **The right to file complaints.** If your request is not satisfied, you can file a complaint to the regulatory body. But please first contact us, and we will do our best to help you.
5. **Right to erasure.** You can send us a request to delete your personal data from our systems.

Depending on the state and legislative requirements, we have from 30 to 60 days to exercise your request with the right for additional 30 days.