

Version dated January 26, 2023

PRIVACY POLICY WITHINGS – HEALTH MATE

OUR COMMITMENTS TOWARDS PERSONAL DATA RELATING TO YOU

Your privacy at the heart of our solutions. We, at WITHINGS, value your privacy and are committed to keeping Personal Data relating to you confidential.** We process the Personal Data relating to you to help you improve your health with the utmost care. We are thankful for your trust and are doing our best to honor it. Respect for privacy is a core principle that we place at the heart of our strategy for developing our Products and Services. We are committed to a continuous improvement process in order to ensure the security of Personal Data relating to you. If you have any question, or wish to exercise your rights, please [contact us](#).

The secured hosting of data health, our daily priority. As data controller, we are committed to giving the highest level of attention to the security and protection of your privacy. We apply high standards (GDPR, ISO 27001:2017 and Health Data Hosting), which allows us to give you the same security as provided by healthcare professionals. We host health data on [our certified health data processing platform](#), whose servers are located in France, at a European operator (BSO).

Uniformized Application for our Users. We take into account the personal data regulations applicable to the markets in which WITHINGS sells their Products and Services. This Policy applies uniformly to all WITHINGS Users, regardless of where you live.

CONTENTS

OUR COMMITMENT TOWARDS PERSONAL DATA RELATING TO YOU

CONTENTS

I. FEW KEY CONCEPTS

The personal health data you entrust to us is sensitive data that we process in accordance with identified legal basis and with the highest security standards.

II. SOURCE OF THE PERSONAL DATA WE PROCESS

Personal Data is collected when you visit our website, use our Products and Services, browse on the application and contact customer support.

III. YOUR CONSENT

Your consent is collected in specific cases. You may withdraw it at any time.

IV. PROCESSING PERSONAL DATA

We process all Personal Data (as identified below) for a particular purpose and on a necessary identified legal basis. We retain the Personal Data for a specific period.

V. HOSTING, TRANSFER AND SECURITY OF DATA

When you use our Products and Services in Europe, the Personal Data relating to you is hosted in France and Health Data is not transferred outside the EEA. However, other data may be transferred to our partners located outside of the EEA. WITHINGS will take several actions in case of data breach.

VI. EXERCISING YOUR RIGHTS

You may exercise your rights under GDPR and HIPAA by contacting us at [_privacy@withings.com](mailto:privacy@withings.com). You may also file a complaint to the supervisory data protection authority.

VII. PRIVACY POLICY'S APPLICATION

This Privacy Policy informs you on __how we collect and use data relating to you while using our Products and Services. This Policy is part of our Terms of Use. Parental consent is needed for the creation of a Health Mate account.

VIII. PATIENT PRIVACY POLICY

Specific provisions relating to the collection and use of Personal Data relating to you, their security, and third-party sharing apply to you if you are using our remote patient monitoring services.

1. FEW KEY CONCEPTS

The personal health data you entrust to us is sensitive data that we process in accordance with identified legal basis and with the highest security standards.

1.1. PERSONAL DATA RELATING TO YOU

a. Personal Data means any information relating to a person and allowing him or her to be identified. This includes various types of information: last name, first name, postal address, email address, etc. This definition also covers the notion of "Personally Identifiable Information" (PII) provided by the United States regulations.

b. Health Data means personal data regarding your health conditions, past, present or future, including, but not limited to age, gender, weight, height, medical history, symptoms. Health data is particularly sensitive and is therefore subject to special protection measures.

c. Pseudonymised Data means personal data in which the directly identifying data (name, surname, etc.) has been replaced by indirectly identifying data (alias, increment number, etc.).

1.2. SECURITY OF OUR HOSTING

ISO 27001:2017 is a certification that proves the quality and security of information systems. In France, it is complemented by the "HDS" requirements (Health Data Hosting). In the United States, it is in compliance with the "HIPAA" standard.

HDS designates the applicable procedure to obtain the "Health Data Hosting" certificate in light of section L. 1111-8 of the French Public Health Code. This certificate is mandatory for any company wishing to host health data obtained in a medical context, on behalf of patients or health professionals.

HIPAA means the U.S. federal law ensuring the privacy and security of Personal Health Information (PHI), applicable in the United States for data intended for health professionals (covered entities).

Our Certified Platform for Health Data Processing refers to the hosting solutions developed by WITHINGS and for which we have obtained certifications.

1.3. GDPR GLOSSARY

GDPR means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. WITHINGS applies the GDPR all over the world.

Legal basis designates the basis on which the Data controller may process personal data (including consent, performance of a contract, legitimate interest, safeguarding vital interests, legal obligation).

Legitimate interest means the pursuit of the essential mission of the Data controller (WITHINGS processes non-identifying data to improve research on the basis of the legitimate interest). The legitimate interest is a reflection process involving several teams in order to assess its lawfulness and the legitimacy.

2. SOURCE OF THE PERSONAL DATA WE PROCESS

Personal Data is collected when you visit our website, use our Products and Services, browse on the application and contact customer support.

2.1. OUR WEBSITE. You can visit the WITHINGS website without providing any personal information. If personal information is requested, you are under no obligation to provide it to WITHINGS. However, you will not receive the full benefit of certain Services. More information is available on our [Cookie Policy](#).

2.2. USE OF PRODUCTS AND SERVICES. The use of our Products and Services generates the creation of data in the following cases.

a. Account creation. When you create a WITHINGS account, you fill in personal data relating to your identity, such as your name, surname(s), age, email address. This account allows you to access the Personal Data generated during the use of the Products and Services, and it also allows you to modify certain data.

b. Use of our Products and Services. When you use our Products and Services, Personal Data is collected (such as number of steps, distance traveled, calories burned, weight, heart rate, sleep patterns, minutes of activity, and in some cases your location). The data collected will depend on the device you use and how you use it. You may consult the [Privacy User Guide](#) to learn about all categories of Personal Data processed by the Product, as well as its settings.

c. Partner Applications. WITHINGS may exchange personal data relating to you with third-party applications **(i)** when you decide to connect your HEALTH MATE account with other applications, WITHINGS will send data relating to you to these applications and, **(ii)** reciprocally, these third-party applications may send us data relating to you to improve your experience and our Services. You should review the privacy policies of these third-party applications as our Policy Privacy only applies to our Products and Services.

d. Customer Support. When you contact customer support, certain Personal Data relating to your WITHINGS account may be momentarily accessible by our teams depending on the problem encountered, such as data relating to the Products you use or your contact information. No Health Data is accessible to our customer support staff without your prior consent.

2.3. APPLICATION TRACKING. Some Personal Data is collected automatically when you use the Products and Services, including through the use of tracking devices. We collect IP addresses, language, operating system, Product information, location (as authorized by you), and smartphone information.

3. YOUR CONSENT

Your consent is collected in specific cases. You may withdraw it at any time.

3.1. COLLECTION OF YOUR CONSENT. We collect your consent to process Personal Data for:

- Creating your HEALTH MATE account;
- Participating in our research programs;
- Sharing Data relating to you with third-party partner applications;
- Enabling dual authentication (2FA);
- Marketing communications;
- Activating geolocation on your connected watch.

3.2. WITHDRAWAL OF YOUR CONSENT. At any time, you can withdraw your consent. To do so, simply:

- Delete your account (link [here](#)) ;
- Uncheck "Research Center" in your notification center (link [here](#));
- Remove the connection with third-party applications;
- Remove double authentication in your account settings (link [here](#));
- Uncheck "Promotional offer" in your notification center (link [here](#)) ;
- Disable geolocation on your connected watch.

4. PROCESSING PERSONAL DATA

We process all Personal Data (as identified below) for a particular purpose and on a necessary identified legal basis. We retain the Personal Data for a specific period._

4.1. NECESSITY OF PROCESSING. We collect Personal Data from you in order to provide you with Products and Services. If you do not wish to provide it, you will not be able to access certain parts of the Products and Services, or services offered by our customer support.

4.2. PURPOSE OF PROCESSING. We process Personal Data in order to graphically present it to you via your HEALTH MATE account accessible from a smartphone or web browser (e.g., user-triggered step count). Data may be collected (i) by a WITHINGS product connected to the application, such as a watch or a scale, (ii) by direct input from you into your HEALTH MATE account, (iii) or from third-party applications.

a) USE OF OUR PRODUCTS AND SERVICES

|
 | **Purchase and delivery of your WITHINGS Products and Services** |
 | --- | --- |
 | **Processed data** | Email address / Postal address / Name / Surname / Card number/ IP address / MAC address of the purchased product / |
 | **Basis for the processing** | Performance of the contract (acceptance of the [Sales conditions](#)) |
 | **Retention period** | WITHINGS must retain billing data for 10 years due to legal requirements.

When you sign up for a Health+ subscription, your bank details may be stored with one of our partners to simplify the renewal of your subscription. |

|

| **Creation of the HEALTH MATE account and authentication during the connection** |

| --- | --- |

| **Processed data** | Email address / Birthday date / Name / Surname / Password (optional) / IP address / MAC address / Profile picture (optional) / Height / Weight |

| **Basis for the processing** | Performance of the contract (acceptance of the [Terms of Use](#)) |

| **Retention period** | Data is retained until your delete your HEALTH MATE account. |

|

| **Graphic presentation of Data relating to you, including Health Data, via HEALTH MATE** |

| --- | --- |

| **Processed data** | Physiological and technical data collected during the use of our Products and Services* |

| **Basis for the processing** | Performance of the contract (acceptance of the [Terms of Use](#)) |

| **Retention period** | Data is retained until deletion of your HEALTH MATE account. |

You may also delete certain data via your HEALTH MATE application. |

|

| **Optional sharing of Personal Data with third-party applications** |

| --- | --- |

| **Processed data** | The data shared vary depending on the product used |

| **Basis for the processing** | Your consent to the sharing of Personal Data relating to you |

| **Retention period** | Data is shared until deletion of the User's account. |

|

| **Extraction of the "Health Report" in pdf. format via the HEALTH MATE application** |

| --- | --- |

| **Processed data** | Name / Surname / Age / Physiological data |

| **Basis for the processing** | Performance of the contract (acceptance of the [Terms of Use](#)) |

| **Retention period** | Data is stored only on your mobile phone. |

|

| **Geolocation of Products (only watches and scales)** |

| --- | --- |

| **Device** | _ Watches _ | _ Scales _ |

| **Processed data** | Location data in the context of physical activity | IP Address / Geographical location |

| **Basis for the processing** | Consent | Required for the performance of the Contract (acceptance of the [Terms of Use](#)) |

| **Retention period** | Data is retained until deletion of the User's account |

|

| **[FOR THE UNITED STATES ONLY]: Activation of the ECG functionality on ScanWatch** |

| --- | --- |

| **Processed data** | Name / Surname / Birthday Date / Phone number / Email address / Country of residence |

|

| **Basis for the processing** | Consent |

| **Retention period** | Data is retained 7 years by the supplier, Heartbeat Health |

b) COMMUNICATION & SUPPORT

|

| **Marketing Communication** |

| --- | --- |

| **Processed data** | E-mail address |

| **Basis for the processing** | Consent to this processing when creating your account |

| **Retention period** | Data is retained as long as your account is active or when you no longer wish to be notified |

|

| **Customer Support** |

| --- | --- |

| **Device** | _ **Responding to Users' requests** _ | _ **Producing statistics** _ |

| **Processed data** | E-mail address / Name / Surname / Content of the request | The data associated with the ticket is retained for a maximum of 5 years. |

| **Basis for the processing** | Required for the performance of the contract (acceptance of the [Sales Conditions](#) and [Terms of Use](#))

| Legitimate interest (statistics) |

| **Retention period** | The data associated with the ticket is retained for a maximum of 5 years. |

c) SECURITY AND EXERCISING YOUR RIGHTS

|

| **Activation of the double authentication (2FA)** |

| --- | --- |

| **Processed data** | Phone number |

| **Basis for the processing** | Your consent when activating this feature |

| **Retention period** | The phone number is retained until the user account is deleted or this feature is deactivated. |

|

| **Prevention and fight against computer fraud** |

| --- | --- |

| **Processed data** | Pseudonymized data relating to the different actions performed by the User |

| **Basis for the processing** | Legitimate interest |

| **Retention period** | One year from the date of registration of the action. |

|

| **Customer requests** |

| --- | --- |

| **Device** | _ **Complaints and requests to exercise rights under the GDPR** _ | _ **Management of other complaints and requests** _ |

| **Processed data** | Sex / Name / Surname / Email address / Content of the request / Identity card (when necessary) |

| **Basis for the processing** | Legal obligation | Legitimate interest |

| **Retention period** | 5 years from the date of the request. Identity card: retained for the time necessary retained for the time necessary to verify the identity. |

d) RESEARCH & DEVELOPMENT

	Sending out "Research Questionnaires" and analyzing the responses received
	--- ---
	Processed data User IDThe content of the questionnaire varies according to the issues addressed
	Basis for the processing Consent of the person filling in the questionnaire
	Retention period Personal Data is retained until the User withdraw his or her consent
	Anonymization of data for research purposes**
	--- ---
	Processed data Personal data, including health data, needed to conduct the study
	Basis for the processing Legitimate interest
	Improvement of the navigation on the Website
	--- ---
	Processed data Login data
	Basis for the processing Legitimate interest
	Retention period Cf. Cookies Policy
	_ Improvement of Products and Services _ (including algorithms' performance and statistic evaluation)
	--- ---
	Processed data The relevant data related to the performance of these processings.It is exclusively pseudonymized data
	Basis for the processing Legitimate interest
	Retention period Personal Data is retained until deletion of the User's account

* For more details about the health data collected by our different products, please refer to our [Privacy User Guide](#)

** Anonymized data may be shared with third parties for research purposes. You can view current and past partnerships via this [link](#).

4.3. DATA SHARING. Because WITHINGS values privacy principles, we do not sell any personal. We only share such data in circumstances described below:

a. Your control over the Data. You may ask us to disclose information to others, such as when you use our community features like forums or programs that require sharing with third parties. You can change your choices at any time by changing your account settings or by visiting our [Help Center](#). If you have chosen to share personal data from WITHINGS Products and Services with third parties, we cannot ensure the deletion or anonymization of such data. We invite you to contact third parties for more information.

b. Internal and Legitimate Sharing. Personal Data may be processed by employees of WITHINGS SAS and its affiliates, within the limits of their respective duties and exclusively to fulfill the purposes of this Policy.

c. Use of our subcontractors. We share certain Data with subcontractors, who are experts in their field, in order to supply the Products and Services. Our subcontractors are required to comply with both the GDPR

and this Privacy Policy. They process the shared Data only for the intended purpose (we use subcontractors to help us ensure the quality of certain services and products, which you can find listed [here](#)).

d. Use of ScanWatch in the United States. WITHINGS may share certain personal information (name, date of birth, email, address, phone number) with Heartbeat Health, a U.S. company, which provides you with services such as the prescription necessary for the ECG functionality of the device, the organization of teleconsultations with our health professional partners, the provision of advice on your health. Your consent to receive text messages from Heartbeat Health is required to activate the ECG functionality on your device. Please see [Heartbeat Health's privacy policy](#) for more information.

e. Limited sharing within the WITHINGS group. We may also transfer Personal Data to a subsidiary, affiliate, in the event of a merger, sale, joint venture, assignment. In this case, the entity to which we transfer Personal Data is in turn bound by the same obligation to protect Personal Data relating to you, and the responsibilities of the Data Controller, as listed in the GDPR.

f. Legal reasons. We may share Personal Data relating to you when required by law, upon request of a court, in connection with a legal proceeding, or if we believe in good faith that disclosure is reasonably necessary to **(a)** investigate, prevent, or take action regarding suspected or actual unlawful activities, or to assist public authorities; **(b)** investigate and defend against any third-party claims or accusations; or **(c)** protect our Services' security or integrity. We will notify you of any legal proceedings that require access to Data relating to you, unless we are prohibited by law from doing so. Where a court order specifies a period of non-disclosure of the request to data subjects, we will send you a deferred notification after the non-disclosure period has expired.

5. HOSTING, TRANSFER AND SECURITY OF DATA

When you use our Products and Services in Europe, the Personal Data relating to you is hosted in France and Health Data is not transferred outside the EEA. However, other data may be transferred to our partners located outside of the EEA. WITHINGS will take several actions in case of data breach.

5.1. HOSTING IN EUROPE. Our Services are provided via European hosting facilities located in France. The Health Data processed for the use of HEALTH MATE are not transferred outside the territory of the European Economic Area.

5.2. SUBCONTRACTORS. Other data may be communicated with partners located outside the European Economic Area for particular expertise (such as telecommunications or banking transaction security).

5.3. SECURITY. We invite you to visit our [dedicated security page](#).

5.4. DATA BREACH. In the event of a data or security breach, WITHINGS will take the following actions: **(i)** promptly investigate the security incident, validate the root cause, and, where applicable, remediate any vulnerabilities within WITHINGS' control which may have given rise to the security incident; **(ii)** comply with laws and regulations directly applicable to WITHINGS in connection with such security incident; **(iii)** as applicable, cooperate with any affected WITHINGS user or client in accordance with the terms of WITHINGS' contract with such user or client; and **(iv)** document and record actions taken by WITHINGS in connection with the security incident and conduct a post-incident review of the circumstances related to the incident and actions/recommendations taken to prevent similar security incidents in the future. WITHINGS will notify you of any data or security breaches as required by and in accordance with applicable law.

6. EXERCISING YOUR RIGHTS

You may exercise your rights under GDPR and HIPAA by contacting us at privacy@withings.com. You may also file a complaint to the supervisory data protection authority.

6.1. YOUR RIGHTS. You may exercise the following rights independently or with our assistance.

a. Right of Access. You can access the Personal Data about you processed, collected or stored by WITHINGS. You can find this information directly from your [account](#) or via [customer support](#).

b. Right of rectification. If you find that the data about you is inaccurate, you have the right to request its correction. Some personal data can be changed directly from your HEALTH MATE account.

c. Right of Limitation and Right to Object. If you find that any data about You is inaccurate, you may ask Us to stop processing that data until the situation is corrected. You may also ask Us to stop processing Data relating to you.

d. Right to Erasure. You may request the deletion of Personal Data relating to you. We will assist you in deleting Personal Data via your [account](#) or customer support.

e. Right to Portability. You may request that we send you the Personal Data relating to you so that you can share it with another company. Details on how to exercise your right to portability are available in our Help Center, under the [Data Import and Export section](#).

6.2. ASSISTANCE IN EXERCISING YOUR RIGHTS You may exercise your rights at any time by writing to privacy@withings.com. Proof of identity may be requested if we have no other way to verify that you are the owner of the account to which the data relates. WITHINGS processes all requests that are not excessive in nature within the time limits set by the GDPR.

6.3. ASSISTANCE OF THE CNIL. In case of dispute, you have the right to file a complaint with the Commission Nationale de l'Informatique et des Libertés (CNIL) whose headquarters are located at 3 Place de Fontenoy, TSA 80715, 75334 Paris Cedex 7.

6.4. CALIFORNIA RESIDENTS. The California Consumer Privacy Act may apply to you. Under California Civil Code sections 1798.83-1798.84, California residents are entitled to ask for and obtain from us an annual list identifying the categories of personal customer information which we shared, if any, with our affiliates and/or third parties in the preceding calendar year for marketing purposes. If you are a California resident and would like a copy of this notice, please submit a written request to privacy@withings.com.

7. PRIVACY POLICY'S APPLICATION

This Privacy Policy informs you on how we collect and use data relating to you while using our Products and Services. This Policy is part of our Terms of Use. Parental consent is needed for the creation of a Health Mate account._

7.1. MINORS. Individuals under the age of 15, or the minimum age applicable in the relevant jurisdiction where such person resides, are not permitted to create accounts unless a parent has agreed to it, in accordance with applicable law. If we become aware that we have collected personal data from a child under the required minimum age without parental consent, we will take steps to deactivate the associated account and delete such information as soon as possible. Parents or legal guardians of a minor who wish to have the child's data deleted may contact us at privacy@withings.com.

7.2. SCOPE OF APPLICATION. This Privacy Policy applies to your use of the HEALTH MATE application with all of the features of our Products, to retrieve all data and information relating to you, as well as the content, services and information related to this application.

7.3. TERMS OF USE FOR WITHINGS PRODUCTS AND SERVICES. Our Privacy Policy is part of the Terms of Use available [here](#). By accessing or using our Products and Services, you acknowledge that you have read and agreed to the applicable Terms of Use.

7.4. CONTENT. This Privacy Policy may be updated. We encourage you to periodically review this Privacy Policy to ensure that you are aware of the current version. Your continued use of our Products and Services, after a new version of this Privacy Policy has been posted, will constitute your acceptance of that version. We will notify you if there are any material change to our Privacy Policy.

8. PATIENT PRIVACY POLICY

Specific provisions relating to the collection and use of Personal Data relating to you, its security, and third-party sharing apply to you if you are using our remote patient monitoring services.

8.1. SCOPE OF APPLICATION

a. Applicability to Patient Users. We also collect and use the Personal Data relating to you in the context of providing you with:

- the Health Mate application and
- the WITHINGS remote patient monitoring ("RPM") services, including all relevant content and functionality associated with Health Mate and the RPM services (collectively, the "**Patient Users Services**") to patients ("**Patient Users**").

This Privacy Policy, as well as the following specific provisions ("Patient Privacy Policy"), applies to Personal Data that we collect from Patient Users.

b. Patient Users Terms of Use. This Patient Privacy Policy is part of the **WITHINGS** Patient Users Terms of Use** available [here](#). By accessing or using our Patient Users Services, you acknowledge that you have read and agree to the applicable Terms of Use. If you do not agree, you must immediately cease using our Patient Users Services. We will notify you if there are any material changes to Our Patient Privacy Policy.

8.2. COLLECTION AND USE OF PERSONAL DATA. In addition to collecting and using Personal Data as specified in Section 5 – "*Authorization to Process Personal Data*" of this Privacy Policy, WITHINGS also collects Personal Health Information relating to you, and in particular all communications between you and your healthcare provider, who provides you with services via the Health Mate app when your healthcare provider has invited you to use the Health Mate app.

8.3. SECURITY OF PERSONAL DATA. While WITHINGS uses reasonable security controls, we cannot guarantee or warrant that such techniques will prevent unauthorized access to the Personal Data relating to you, and therefore, WITHINGS is unable to guarantee the security or integrity of Personal Data transmitted. Accordingly, we do not and cannot ensure or warrant the security or integrity of any personal data you transmit to us.

8.4. DATA SHARING WITH HEALTHCARE PROVIDERS. WITHINGS may share Personal Data relating to you to your healthcare providers for the purposes of providing the Patient Users Services. If at any point you want to deny access to one or more healthcare providers, you can do so by emailing privacy@withings.com.

8.5. PATIENT USERS' RIGHTS. Your rights are stated in Section 6 above. Please note that some information is sent by your healthcare provider, and therefore is not under our direct control. Questions or concerns about your medical record or Personal Data provided to us by your healthcare provider should be directed to your healthcare provider. **Such information is not under the direct control of WITHINGS.**