

Version dated August 11, 2023

PRIVACY POLICY WITHINGS

YOUR PRIVACY AT THE HEART OF OUR SOLUTIONS

We thank you for your trust and do our best to honor it. We process the personal data you entrust to us to help you improve your health with the utmost care. 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 process of continuous improvement to ensure the utmost respect for your personal data. If you have any questions please [contact us](#).

THE SECURED HOSTING OF HEALTH DATA, OUR DAILY PRIORITY

We pay maximum attention to the security of the hosting of your health data. We apply demanding regulations and standards. Thus, in addition to our compliance with the GDPR, we are certified ISO 27001 and HDS (Health Data Hosting) which allows us to provide you with the same level of security as health professionals. We host health data on [our certified health data processing platform](#), whose servers are located in France, at a European operator (BSO). Withings is also ISO 27701 certified, an international standard guaranteeing a high level of protection for personal data.

GLOBAL AND UNIFORM APPLICATION

This Policy applies uniformly to all Users of the Withings App, regardless of where you live. We take into consideration the regulations on the protection of personal data applicable to the markets in which WITHINGS sells its Products and Services.

SUMMARY

I. FEW KEY CONCEPTS

The personal health data you entrust to us is sensitive data that we process in accordance with identified legal bases 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 specific purpose and on an identified and necessary legal basis. We retain Personal Data for a specified period of time.

V. DATA RETENTION

When you use the Products and Services in Europe, your Personal Data is hosted in France and Health Data is not transferred outside the EEA.

VI. HOSTING, TRANSFER AND SECURITY OF DATA

Your Personal Data is hosted in France and Health Data is not transferred outside the EEA. However, other data may be transferred to our partners located outside the EEA. WITHINGS will take several steps in the event of a data leak.

VII. EXERCISING YOUR RIGHTS

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

VIII. PATIENT PRIVACY POLICY

Specific provisions regarding the collection and use of your Personal Information, its security and sharing with third parties apply to you if you use our Remote Patient Monitoring ("RPM") services.

IX. GENERAL TERMS AND CONDITIONS

The present privacy policy is subject to the General Terms and Conditions.

I. FEW KEY CONCEPTS

This Privacy Policy applies to the use of the Withings App published by Withings. Withings App is a free application (web and mobile) that focuses on three areas: (i) health monitoring, (ii) motivation maintenance, (iii) installation of WITHINGS products. Withings App can be used alone or in conjunction with our products. The personal health data you entrust to us is sensitive data that we process in accordance with identified legal bases and with the highest security standards.

1.1. Personal Data relating to you

« **Anonymized Data** » means data resulting from the processing of personal data in such a way as to prevent the identification of the data subject in an irreversible manner, taking into account the techniques that can reasonably be implemented.

« **Pseudonymized Data** » means Personal Data that is not directly linked to a natural person without the use of additional information.

« **Personal Data** » means any information relating to an identified or identifiable individual. This includes all kinds of information: last name, first name, postal address, e-mail address, etc. It also covers the notion of Personally Identifiable Information (PII) provided for by the American regulation.

« **Health Data** » means personal data relating to your past, present or future state of health (physical or mental). Health Data is particularly sensitive data and is therefore subject to special protection measures.

1.2. 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).

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.

2.1. Our website. Regarding the data collected on the website of WITHINGS, please refer to our [Cookies Policy](#).

2.2. Use of Products and Services. The use of our Products and Services generates the creation of personal 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.

c. Partner Applications. When you connect your Withings App account with third-party applications or products, data from Withings App will be synchronized with those applications. You can also consent so Withings may also collect data from these third-party applications or products to improve your experience and our Services. You can modify or withdraw your consent directly in the settings of your Withings App. Please note that editors of third-party applications become data controllers once data has been transmitted. We invite you to read the privacy policy of these third-party applications. This policy applies only to Products and Services offered by Withings.

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. No Health Data is accessible to our customer support staff without your prior consent.

e. Event tracking. Some Personal Data is collected automatically when you use the Products and Services, including through the use of tracking devices. We collect technical information such as: IP addresses, language, operating system, location (as authorized by you), and smartphone information (model, version...).

III. 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:

- 1. Creating your Withings App account;
- 2. Participating in our research programs;
- 3. Sharing your Data with third-party partner applications;

- 4. Enabling dual authentication (2FA);
- 5. Marketing communications.

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

- 1. Delete your account ([here](#)) ;
- 2. Uncheck "Research Center" in your notification center ([Android](#) / [iOS](#)) ;
- 3. Remove the connection with third-party applications ;
- 4. Remove double authentication in your account settings ([Android](#) / [iOS](#)) ;
- 5. Uncheck "Promotional offer" in your notification center ([Android](#) / [iOS](#)).

IV. PROCESSING PERSONAL DATA

4.1. NECESSITY OF PROCESSING. We collect Personal Data from you in order to provide the different purposes listed below. 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. LIST OF PROCESSING.

A) USE OF OUR PRODUCTS AND SERVICES

1. Purchase and delivery of your WITHINGS products and services via our website

- PROCESSED DATA: Name / First name / Email address / Postal address / Phone number / Credit card number / IP address / MAC address of the purchased product
- LEGAL BASIS: 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 Withings+ subscription, your bank details may be stored with one of our partners to simplify the renewal of your subscription

2. Withings App account creation

- PROCESSED DATA: Email address / Date of birth / First and last name / Password (optional) / IP address / MAC address / Profile picture (optional) / Height / Weight
- LEGAL BASIS: Performance of the contract (acceptance of the [Terms of Use](#))
- RETENTION PERIOD: Data is retained until you delete your Withings App account

3. Graphic presentation of your Data, including Health Data, via Withings App

- PROCESSED DATA: Physiological and technical data collected when using our Products and Services. For more details regarding the health data collected by our various products, please refer to our [User Guide](#).
- LEGAL BASIS: Performance of the contract (acceptance of the [Terms of Use](#))
- RETENTION PERIOD: Data is retained until deletion of your Withings App account. You may also delete certain data via your Withings App

4. Optional sharing of Personal Data with third-party applications

- PROCESSED DATA: The data shared vary depending on the product used
- LEGAL BASIS: Your consent to the sharing of Personal Data relating to you
- RETENTION PERIOD: Data is shared until sharing is deactivated or the user account is deleted

5. Display of the path taken via the Withings App during an activity

- DATA PROCESSED: Location data in the context of physical activity
- LEGAL BASIS: Your consent
- DURATION OF RETENTION: The data is kept until the user account is deleted

6. WITHINGS+ program and personalization of your experience (additional services)

- DATA PROCESSED: User ID / Weight objective / Muscular mass / Fat mass
- LEGAL BASIS: Your consent
- DURATION OF RETENTION: The data is kept until the user account is deleted

7. Weather display on scales

- DATA PROCESSED: IP address / Geographic location
- LEGAL BASIS: Necessary for the execution of the contract (acceptance of the [Terms of Use](#)).
- DURATION OF RETENTION: The data is kept until the user account is deleted

8. [UNITED STATES ONLY]: Activation of the ECG functionality on ScanWatch

- PROCESSED DATA: Name / First name / Date of birth / Phone number / E-mail address / State of residence
- BASIS FOR THE PROCESSING: Consent
- RETENTION PERIOD: Data is retained 7 years by the supplier, Heartbeat Health

B) COMMUNICATION & SUPPORT**1. Marketing Communication**

- PROCESSED DATA: E-mail address
- LEGAL BASIS: 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

2. Improvement of the navigation on the Site

- DATA PROCESSED: Connection data (see [Cookie Policy](#))
- LEGAL BASIS: Consent obtained through the cookie banner
- PERIOD OF RETENTION: 3 months

3. Customer support - Requests made on our Help Center

- DATA PROCESSED: E-mail address / Name / First name / Content of the request.
- LEGAL BASIS: Necessary for the execution of the contract (acceptance of the Terms of use / Sales conditions)
- DURATION OF RETENTION: The data associated with the ticket is kept for a maximum of 10 years or until the user account is deleted.

4. Customer support - Requests made via Withings official social networks accounts

- DATA PROCESSED: Name / First name / Content of the request / Username.
- LEGAL BASIS: Legitimate interest
- DURATION OF RETENTION: The data associated with the ticket is kept for a maximum of 10 years or until user account is deleted.

5. Feedback on the Customer support experience

- DATA PROCESSED: E-mail address
- LEGAL BASIS: Legitimate interest
- DURATION OF RETENTION: The data associated with the ticket is kept for a maximum of 5 years.

6. Vigilance of WITHINGS products

- DATA PROCESSED: Name / First name / E-mail address / Address / Phone number / Age / Description of the adverse incident and its consequences / Pathologies (only for adverse incidents happening during a clinical study)

- LEGAL BASIS: Compliance with legal requirements
- DURATION OF RETENTION: 15 years from the day of notification.

C) SECURITY AND EXERCISING YOUR RIGHTS

1. 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

2. Prevention and fight against computer fraud and cyberattacks

- 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

D) RESEARCH & DEVELOPMENT

1. Sending out "Research Questionnaires" and analyzing the responses received

- PROCESSED DATA: User ID. The content of the questionnaire varies according to the issues addressed
- BASIS FOR THE PROCESSING: Consent of the person filling in the questionnaire
- RETENTION PERIOD: Pseudonymized Data is retained until the account removal

2. Anonymization of data for research purposes

- PROCESSED DATA: Health data needed to conduct the study
- BASIS FOR THE PROCESSING: Your consent

3. Product and Service Improvement (including algorithm performance improvement and statistics))

- PROCESSED DATA: The relevant data related to the realization of these treatments. It is exclusively pseudonymized data
- BASIS FOR THE PROCESSING: Legitimate interest
- RETENTION PERIOD: Personal data is kept until the user account is deleted

4.3. DATA SHARING. 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](#).

b. Internal and Legitimate Sharing. Personal Data may be processed by the employees of WITHINGS SAS and its subsidiaries, within the limits of their respective responsibilities and exclusively for the purposes described in 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. They process the shared Data only for the intended purpose. Our subcontractors help us to provide you with high quality products and services, please find the list of subcontractors [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. 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 your Data, 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.

V. DATA RETENTION

5.1. RETENTION PERIOD. The retention period indicated in the list of treatments depends on the type of data, the purpose or our legal obligations. If you ask us to do so, WITHINGS will delete your data from its servers and will ask its subcontractors involved in the processing to perform the same operation. We use subcontractors to manage backup data. This data will be used in case of operational problems to ensure the continuity of our services and products. Please note that, for security reasons, we are not able to reflect the deletion or modification of data on backups already made, in order to protect the integrity of the backup data.

5.2. INACTIVE USER ACCOUNT. Your Withings App account will be considered inactive if for 3 years (i) you have not used the mobile or web application, (ii) you have not performed any measurements with the Withings products associated with the account, and (iii) you have not clicked on any link contained in an email sent by WITHINGS. You will receive an email notification 90 days before your account is considered inactive, giving you the opportunity to continue your WITHINGS experience. If no action is taken on your part, your account and associated data will be deleted in accordance with this Privacy Policy.

5.3. ANONYMIZED DATA. WITHINGS may anonymize your data in accordance with the applicable security standards and regulations. Once anonymized, it no longer identifies you and is no longer Personal Data. WITHINGS uses the data in this form to participate in research projects.

5.4. DATA SHARED WITH THIRD PARTIES. If you have chosen to share your data from WITHINGS Products and Services with third parties, we cannot ensure the deletion or anonymization of such data. We invite you to contact the third party for more information.

VI. HOSTING, TRANSFER AND SECURITY OF DATA

Your Personal Data is hosted in France and Health Data is not transferred outside the EEA. However, other data may be transferred to our partners located outside the EEA. WITHINGS will take several steps in the event of a data leak.

6.1. HOSTING IN EUROPE. Our Services are provided by our Platform certified for the processing of health data via a European host located in France. The processed Health Data are not transferred outside the territory of the European Economic Area.

6.2. SUBCONTRACTORS. Other data may be communicated with partners located outside the European Economic Area for specific purposes (such as telecommunication or security of banking transactions). The list of our subcontractors is available [here](#).

6.3. SECURITY. We invite you to consult our [dedicated page](#).

VII. EXERCISING YOUR RIGHTS

You may exercise your rights by contacting us at privacy@withings.com.

7.1. 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 Withings App 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 [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](#).

7.2. 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.

7.3. 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.

VIII. PATIENT PRIVACY POLICY

Specific provisions regarding the collection and use of your Personal Information, its security and sharing with third parties apply to you if you use our Remote Patient Monitoring ("RPM") 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 the use of the Withings App in the context of the WITHINGS remote patient monitoring ("WRPM") services. This Privacy Policy, as well as the following specific provisions (« **WRPM** ») services. 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 cease using our Patient Users Services. We will notify you if there are any material changes to Our Patient Privacy Policy.

8.2. PATIENT USERS' RIGHTS. Some information is sent by your healthcare professional and is therefore not directly under our control. Questions or concerns about your medical records or Personal Information provided to us by your healthcare professional should be directed to your healthcare professional. This information is not under the direct control of WITHINGS.

IX. GENERAL TERMS AND CONDITIONS

The present privacy policy is subject to the [General Terms and Conditions](#)