Your Privacy

Last updated: June 2024

1. About this Privacy Notice

1.1 ResMed (‘**ResMed**,‘ ’**we**,‘ ’**our**’ ’**us**) is committed to protecting the privacy and security of your Personal Data (as defined below) and we want to be transparent about the types of Personal Data we collect about you and how we use it. This Privacy Notice (hereafter the ‘**Notice**’), explains how we collect, use and share any information gathered about you (‘**Personal Data**’) through your use of the ResMed device (the ‘**Device**’) and aims to inform you about the rights and freedoms that you can exercise with our use of your Personal Data. This Notice also describes the measures we implement to protect your Personal Data.

1.2 This Device is managed by ResMed SAS, headquartered at 292 Allée Jacques Monod, 69791 Saint-Priest, France, which is the data controller for all Personal Data that is collected via this Device. For more information about this app, please refer to this user guide.

1.3 If you do not want ResMed to process any of your Personal Data through this Device, as set out in this Notice, please do not activate the ‘connectivity’ functionality on the Device. (Contact your healthcare provider to ensure the ‘connectivity’ functionality on your Device is not activated.)

2. The types of Personal Data we collect and why

2.1 When you use our Device, we collect the following types of Personal Data about you, which we will only process for the sole purposes described below:

Types of Personal Data	Purpose for processing	Legal basis
	❶ **For ResMed legal obligations**	
Identification data: date of birth, gender, user ID, country of residence. **Account data**: User ID, Login, password, preferences. **Log data**: date and type of request. **Sleep-related data collected via your device as health data**: usage hours, mask seal, AHI events per hour, mask on/off events, sessions/night. **Sleep-related data collected via our questions as health data:** when did you start your therapy, AHI events on sleep test, location of the sleep test,	ResMed must: • improve the usability, performance and security of its medical devices. • run post-market clinical follow up of our medical devices. • perform materiovigilance.	Compliance with: • our legal obligation (Article 6.1.c) GDPR) • public interest in public health to ensure high standards of quality and safety of health care (Article 9. 1.i) GDPR)

how do you feel after the therapy and any other information that you decide to provide us. **Cookies data:** screens accessed by the user, time spent on a screen, occurrence of myAir being launched and how (for example, email notification), login/logout occurrences, email open occurrences.		
	❷ **For health research, evaluation and studies**	
Identification data:, date of birth, user ID, country of residence. **Device-related data:** serial number, type of device and mask, therapy mode, device settings that are used. **Log data**: date and type of request. **Sleep-related data collected via your device as health data**: usage hours, mask seal, AHI events per hour, mask on/off events, sessions/night. **Sleep-related data collected via our questions as health data:** when you started your therapy, AHI events on sleep test, location of the sleep test, how you feel after therapy, and any other information that you decide to provide us. **Cookies data:** screens accessed by the user, time spent on a screen, occurrence of myAir being launched and how (for example, email notification), login/logout occurrences, email open occurrences.	ResMed reuses your data for retrospective health studies, research and evaluation.	Compliance with: • legitimate interests of ResMed, researchers or ResMed's partners (Article 6.1.f) GDPR) • explicit consent (Article 9. 1.a) GDPR).
	❸ **For products and services development**	
Device-related data: serial number, type of device and mask (including mask acoustic signature) and device settings.	ResMed uses your data to improve our products and services and improve therapy effectiveness.	• Our legitimate interest to help us understand how our products and services are being used and improve therapy effectiveness.

2.2 Sleep data

The Device enables us to collect information about your sleep pattern and disorders. Sleep-related data is considered health-related (health data) when it is used to analyse your state of health and to assess your health risks. This is the case, for

example, where our analysis of your sleeping disorders is based on the high number of apnoeas per hour measured over a certain period of time.

ResMed will process your health data for the following purposes:

❶ Fulfilment of legal obligations in connection with the marketing of medical devices:

(i) to improve the usability, performance and security of its medical devices.
(ii) to run post-market clinical follow-up of our medical devices.
(iii) to perform materiovigilance.

❷ Conducting health studies, research and evaluations:

Your health data may also be reused under the responsibility of ResMed, researchers or ResMed's partners for the purposes of retrospective studies of public interest in the field of health and aimed at improving knowledge. Under the General Data Protection Regulation (GDPR), this processing requires us to obtain your prior explicit consent for this purpose.

This Privacy Notice will be updated on a regular basis. We recommend that you regularly consult it so you're informed of all the studies undertaken by ResMed, researchers or ResMed's partners based on the reuse of your Personal Data.

Those health studies implemented from the reuse of your Personal Data:

(i) aim to improve scientific knowledge,
(ii) must provide a public interest in accordance with the meaning of current legal and regulatory provisions,
(iii) will be conducted by ResMed, researchers or ResMed's partners, who have previously completed the required formalities before the authorities, and in particular the CNIL,
(iv) will be approved by the Scientific Committee of ResMed.

3. How we obtain your Personal Data

3.1 Most of the information we process is obtained directly through the ResMed Device, which monitors your sleep.

3.2 ResMed processes customer Personal Data on the customer's behalf as a processor in relation to its provision of the ResMed HI services.

3.3 ResMed processes your Personal Data as a controller for the purposes of 1, 2 and 3 defined above.

4. Who we share your Personal Data with

We may disclose your Personal Data to the following recipients:

(a) **our European Union-based, third-party vendors, services providers and partners** who provide data processing services to us, or who otherwise process

Personal Data for purposes that are described in this Notice or communicated to you when we collect your Personal Data. This may include disclosures to European Union-based, third-party vendors and other service providers we use in connection with the services they provide to us, including to support us in areas such as IT platform management or support services, infrastructure and application services, marketing and data analytics. We use the following third-party suppliers and service providers:

Subcontractors	Address	Treatment
Amazon Web Services	038 Avenue John. F Kennedy, L-1855 Luxembourg	Data hosting
Snowflake	Snowflake Computing Netherlands B.V., FOZ Building, Gustav Mahlerlaan 300-314, 1082 ME Amsterdam, Netherlands	Hosting and support of their activity management solution (fast and large-scale data analysis)
Qlik	Qlik Tech France SARL,93 Avenue Charles de Gaulle, 92200 Neuilly Sur Seine, France	Support provided to their data visualization solution

(b) **any competent law enforcement body, regulatory, government agency, court or other third party** where we believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights or (iii) to protect your vital interests or those of any other person;

(c) **our auditors, advisors, legal representatives and similar agents** in connection with the advisory services they provide to us for legitimate business purposes and under contractual prohibition of using the Personal Data for any other purpose;

(d) **a potential buyer** (and its agents and advisers) in connection with any proposed purchase, merger or acquisition of any part of our business, provided that we inform the buyer it must use your Personal Data only for the purposes disclosed in this Notice;

(e) **any other person** if you have provided your prior consent to the disclosure.

5. How we protect your privacy

We will process Personal Data in accordance with the following principles:

(a) **Fairness**: We will process Personal Data fairly. This means we are transparent about how we process Personal Data.

(b) **Lawfulness**: We will process Personal Data only on lawful grounds.

(c) **Purpose limitation**: We will process Personal Data for specified explicit and legitimate purposes and will not process it in a manner that is incompatible with those purposes, unless permitted by applicable data protection laws.

(d) **Data minimisation**: We will process Personal Data that is adequate, relevant and

limited to what is necessary to achieve the purposes for which the data are processed.

(e) **Data accuracy**: We take appropriate measures to ensure that the Personal Data that we hold about you is accurate, complete and, where necessary, kept up to date. However, it is also your responsibility to ensure that your Personal Data is kept as accurate, complete and current as possible by informing us promptly of any changes or errors. You should notify us of any changes to the Personal Data that we hold about you (for example, a change of address).

(f) **Data security**: We use appropriate technical and organisational measures to protect the Personal Data that we collect and process about you. The measures we use are designed to provide a level of security appropriate to the risk of processing your Personal Data. In particular, all data is protected according to the varying levels of risks through physical measures, such as secure areas, technical measures, such as encryption, and organisational measures, such as employee security through vetting and supervision.

(g) **Limited Retention**: We keep your Personal Data in a form that allows us to identify you for as long as necessary to achieve the purposes for which we are processing your data and do not store your data for longer, unless we must comply with applicable laws.

6. Data storage, retention and deletion

The Personal Data we collect from you is stored on our servers located in a country in the European Economic Area (currently in France and/or Germany).

Customer Personal Data is archived by ResMed for the durations/data retention periods described in the following 'Purpose for processing' table.

ResMed has a legal obligation to comply with these retention periods pursuant to applicable laws (including, but not limited to, the Medical Device Regulation [EU] 2017/745 of 5 April 5th, 2017), acting as Data Controller.

Purpose for processing		Data retention period
Purpose ❶	Improve the usability, performance and security of its medical devices.	Health data, maximum 10 years from receipt by ResMed.
	Run post-market clinical follow up of our medical devices.	10 years after the end of the marketing of the medical device.
	Perform materiovigilance	15 years from the date of withdrawal of the drug, device or product market
Purpose ❷	For health research, evaluation and studies	Depending on the storage period defined for the specific study concerned (for example, MR or CNIL authorisation)
Purpose ❸	To improve our products and services and therapy effectiveness.	5 years from the date of data collection.

7. Technical and organisational measures

7.1 We use various data security and privacy measures to protect your Personal Data and comply with applicable data protection laws.

7.2 Your Personal Data is hosted in a secure data centre in France or Germany by an HDS certified health hosting provider. Our subcontractor operates under our strict and precise instructions. The subcontractor is audited on a regular basis by independent third-party auditors, including penetration testing and certification audits. The hosting subprocessor is responsible for maintenance, physical hardware and network security for the customer Personal Data they store.

7.3 A confidentiality agreement was signed by all ResMed's employees who receive security and privacy training (e-learning and privacy champions training). By implementing this training, ResMed ensures their privacy and security processes are understood and followed by all of its employees processing European Personal Data.

7.4 Your Personal Data is protected in terms of confidentiality and integrity by using, partitioning (meaning the test and production environments are separated), pseudonymisation, strong authentication, encryption controls, securing the data at rest and in transit. Adequate encryption policies are put in place to ensure the adequacy of the implemented controls.

7.5 Backups are implemented to ensure the availability and integrity of your data. The backup operations are monitored, secured and documented. Additionally, a disaster recovery plan and a business continuity plan are implemented and tested.

7.6 Automatic security updates are regularly applied to avoid any risk of vulnerability on the infrastructure. Protection against malware and malicious attacks is put in place through the implementation of next generation firewall solutions and antimalware/antivirus solutions and vulnerability scanning and system patching. A disposal process ensures the secure deletion of your data.

7.7 Access to system and application components is limited to authorised maintenance personnel based on the principles of least privilege, need to know and segregation of duties.

7.8 An audit mechanism reviews logs to detect malicious activities using the appropriate tools.

7.9 ResMed has implemented a change management procedure to ensure a security check is performed before any significant change.

7.10 A security incident response plan is implemented and tested. ResMed has implemented a security incident and events management tool that aims to report accesses and alert if a forbidden action occurred, allowing timely and effective response actions.

7.11 Despite the high standard of security measures we apply, it's impossible to guarantee an absolute level of security for data transmitted over the internet. If we

have confirmation that your Personal Data has been breached, we will comply with any relevant legal provisions regarding data security breach notification.

8. Transfers of Personal Data outside the EU/EEA

8.1 Your Personal Data is hosted on data centres within the European Economic Area ('EEA'). However, in limited circumstances, it may be necessary for your Personal Data to be remotely accessed by, or transferred to, ResMed or its service providers in countries outside of the EEA (for example, to provide technical support or for data security reasons).

8.2 Also, ResMed or its service providers may receive orders from governments outside of the EEA requiring disclosure of your Personal Data. These countries may not have data protection laws that are equivalent to those in the EEA.

8.3 Where we allow your Personal Data to be transferred to service providers or ResMed companies outside of the EEA, we will put in place appropriate safeguards (such as, the EU Commission's Standard Contractual Clauses on the basis of Article 46 GDPR) and take any other steps necessary to ensure your data is protected in accordance with data protection law. You have a right to request a copy of any safeguards used to transfer your Personal Data outside of the EEA. (See 'How to contact us.')

8.4 Following is a summary of potential transfers of Personal Data outside the EEA.

Subcontractors	**Purpose of the transfer outside the EEA**	**To which country(ies)?**	**Frequency**
Amazon Web Services	Orders from governments outside the EEA	United States	Rare or even hypothetical
Snowflake	Correction of technical faults (maintenance)	United States	Rare, accidental

9. Your data protection rights

9.1 You have the following data protection rights:

(a) You may exercise your right of access, which includes the right to information to understand how ResMed processes your Personal Data and the right to instruct ResMed to provide you with a copy of the Personal Data that we hold, including a copy of the Standard Contractual Clauses we use.

(b) If you wish to correct or update your Personal Data, contact us as indicated in the 'How to contact' us topic.

(c) You may request that we delete your Personal Data. However, when ResMed is only processing your Personal Data to comply with its quality and regulatory obligations under applicable laws, which is the case for purpose 1 of the processing (see topic '2.2 Sleep data') ResMed won't be able to delete your Personal Data on request.

(d) In addition, in certain circumstances, as stipulated in the applicable data protection legislation, you can object to processing of your Personal Data (only for purpose 2), ask us to restrict processing of your Personal Data or request portability of your Personal Data. To exercise these rights, contact us as indicated in the 'How to contact' us topic below.

(e) If we have collected, and are processing, your Personal Data with your consent, then you can withdraw your consent at any time. You may, opt-out from our mask acoustic signature feature from your Device settings. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your Personal Data conducted in reliance on lawful processing grounds other than consent.

(f) If you have a complaint or concern about how we are processing your Personal Data, we will endeavour to address such concern(s). If you feel we have not sufficiently addressed your complaint or concern, you have the right to complain to a data protection authority about our collection and use of your Personal Data. For more information, please contact your local data protection authority. Contact details for data protection authorities in the European Economic Area, Switzerland and certain non-European countries (including the US and Canada) are available here.

9.2 You may exercise any of the rights above, at any time. by contacting us as described in 'How to contact us.' We will respond to your request in accordance with applicable data protection laws.

9.3 We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

10. Updates to this Notice

10.1 We may update this Privacy Notice from time to time in response to changing legal, technical or business developments. When we update our Privacy Notice, we will take appropriate measures to inform you, consistent with the significance of the changes we make.

10.2 You can see when this Privacy Notice was last updated by checking the 'last updated' date displayed at the beginning of this Privacy Notice.

11. How to contact us

If you have any questions, concerns or complaints about this Notice or the way we process your Personal Data, or if you want to exercise your rights as described above, please contact our Privacy Office by email at privacy@resmed.eu or by postal mail at ResMed SAS, 292 Allée Jacques Monod, 69791 Saint-Priest, France.

You may also contact our Data Protection Officer by email at privacy@resmed.eu or by postal mail at Data Protection officer, ResMed SAS, 292 Allée Jacques Monod, 69791 Saint-Priest, France.