Personal Data Protection When Using Masimo SafetyNet™

Masimo Österreich GmbH ("Masimo") prepared this brochure to help answer frequently asked questions from its registered hospitals regarding Masimo's data protection compliance program and help legal counsels quickly understand the basic facts regarding Masimo SafetyNet services.

This brochure does not contain or constitute a substitute for legal advice and does not create legal rights for any party.

Should you have any further questions about Masimo's data protection compliance program, please contact privacy@masimo.com.

Masimo

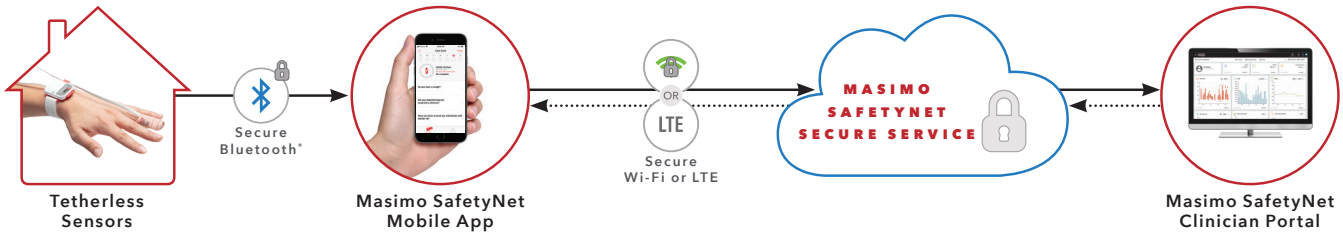
General Information

Masimo developed **Masimo SafetyNet** to collect key health data directly from patients and to provide information to healthcare providers ("HCPs") so they can remotely monitor patient health status.

Masimo SafetyNet is designed to be a secure, scalable, cloud-based patient management platform, featuring clinical-grade spot-checking and continuous measurements, digital care pathways, and remote patient surveillance.

Masimo SafetyNet is only available **through hospitals that have registered to use Masimo SafetyNet ("Registered Hospitals") and associated HCPs.**

Patients receive a multi-day supply of disposable sensors or reusable devices such as Radius PPG™ and/or Radius T°™, along with access to the Masimo SafetyNet mobile application (the "Masimo SafetyNet App"), which, after being downloaded to the patient's mobile device, allows the patient to register to use Masimo SafetyNet.



End-to-end security measures with data security standard deployed

Patient registers for free to use the mobile app.

Patient gives consent to processing of his/her data.

Only registered HCPs* have access to the clinician portal with individual authentication.

Personal data is hosted in the European Union by a reputable cloud services provider.

When the patient uninstalls the app, it automatically removes all app data from his/her mobile device.

** Only registered HCPs of the Registered Hospital have access to the Masimo SafetyNet Clinician Portal, with individual authentication.*

Masimo SafetyNet receives and stores personal data and health information from its users, who are generally patients of an HCP using the data as part of patient care.

Patients have access to their personal data and health information on their mobile device through the Masimo SafetyNet App. When the patient uninstalls the Masimo SafetyNet App, all data stored on the app is automatically removed from his/her mobile device.

The data is **encrypted** at rest and in transit across public networks.

This data is processed and stored on a private "cloud" provided by **Amazon Web Services (AWS)** through a contract and the AWS GDPR Data Processing Addendum. AWS's cloud services are certified for compliance with multiple commonly recognized data security standards.

The secure and private "cloud" is located in the European Union (Frankfurt, Germany for the Primary Data Center and Dublin, Ireland for the Disaster Recovery Center).

Only registered HCPs of the Registered Hospital have access to the Masimo SafetyNet Clinician Portal, with individual authentication.

Masimo and **AWS** have taken comprehensive steps to comply with the **EU General Data Protection Regulation ("GDPR")**. (Please also see the below Amazon Web Service compliance program extract.)

Masimo SafetyNet's General Data Protection Regulation ("GDPR") Compliance Measures

This section is intended to provide you with relevant information about Masimo SafetyNet and the measures that Masimo has taken to comply with the GDPR.

1. How is each patient's personal data collected?

Masimo SafetyNet receives and stores personal data and health information from its users (the patients) when they register to use the Masimo SafetyNet App and when they wear the sensors and reusable devices connected to the Masimo SafetyNet App.

2. Limited categories of patient's personal data are processed:

In accordance with Articles 4, 5, and 9 of the GDPR, Masimo SafetyNet only collects and processes the following categories and data from patients:

- Name, phone number, email address, login credentials
- Patient's age, gender, and date of birth
- Information about user's device (e.g., IP address) and type of device used to capture the patient's data
- User's usage behavior when logged into the Masimo SafetyNet App and behavioral use of the solution
- Patient's physical activity
- Health data (e.g., oxygen saturation, respiration rate, perfusion index, pulse rate, pleth variability index, temperature, and current/past/trend of the same)
- The contact information of the patient's HCP, friends, family, and any other third party the patient has designated to receive the patient's data

3. Personal data is processed on a legal basis:

In accordance with Articles 6 and 9 of the GDPR, Masimo processes personal data on the following legal bases:

- For health data, the legal basis of processing is the patient's express consent per Article 9(2)(a) of the GDPR as health data is considered a special category of personal data. The patient has the right to withdraw his/her consent at any time. Such withdrawal does not affect the lawfulness of processing based on his/her consent before withdrawal. However, after such withdrawal, Masimo will no longer be able to provide Masimo SafetyNet.
- In extenuating circumstances, such as where the processing is necessary to protect the patient's vital interests or to establish, exercise, and defend legal claims, the legal basis of processing special categories of personal data may be another legal basis set forth under Article 9(2) of the GDPR.
- The legal bases for processing of personal data that is not health data are:
    - The performance of the contract entered into with the patient for the use of the Masimo SafetyNet App (i.e., Masimo's SafetyNet Terms of Use), per Article 6(1)(b) of the GDPR.
    - The pursuit of legitimate interests per Article 6(1)(f) of the GDPR: It is in Masimo's legitimate interests to provide good service, ensure the security of our services, and analyze how users access and use our services so that we can further develop and improve them.
    - Compliance with Masimo's legal obligations per Article 6(1)(c) of the GDPR.

4. Personal data is processed for limited purposes and according to the data minimization principle.

Limited Purposes:

The purpose limitation principle of Article 5 of the GDPR means that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Masimo processes personal data for the primary purposes of Masimo SafetyNet to enable:

- The patient to provide health information to his/her HCPs for purposes of remote monitoring to assist in the treatment of the patient.
- The patient to share the health information with family, friends, or any other person or caregiver the patient wishes to keep informed of the wellbeing and health of the patient.
- Authentication: some data (e.g., users' contact information and IP addresses) authenticates the patient and his/her HCPs as users of Masimo SafetyNet, and ensures that the correct users are connected to the correct patient or the correct HCPs.

Masimo does not sell users' personal data.

Data Minimization:

The data minimization principle of Article 5 of the GDPR means that personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Masimo SafetyNet is designed according to the data minimization principle as stated in Article 5 of the GDPR:

- The patient and his/her HCPs determine what health data Masimo SafetyNet receives.
- The patient can modify and correct his/her settings and personal information directly on the Masimo SafetyNet App.
- Masimo SafetyNet and Masimo only use the data necessary to fulfill the purposes described in the Masimo SafetyNet Privacy Notice.

5. The Data Controllers:

A data controller is the legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data.

The Registered Hospital or HCP and Masimo are data controllers.

Masimo

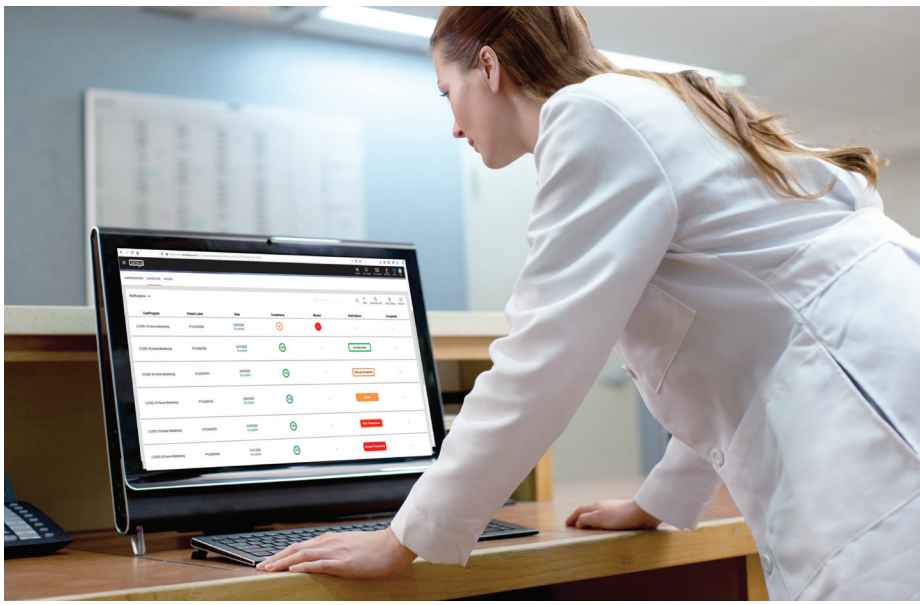
Masimo (Masimo Österreich GmbH) is a data controller because it determines the purposes and means of the processing of personal data through its Masimo SafetyNet solution:

- Patients can download and use the Masimo SafetyNet App independently from a particular hospital's or HCP's treatment plan, and so Masimo has to be able to separately and independently determine the means and purposes of processing users' data.
- Masimo takes full responsibility for its own data processing and compliance practices. For example, it issues privacy notices to users in its own name and answers data-related requests directly.
- If Masimo instead acted as a processor for its Registered Hospitals for the purposes of data protection law, its Registered Hospitals would generally be fully responsible for its actions vis-à-vis their respective patients.

Masimo's address is Mariahilfer Straße 136, 1150 Wien, Austria.

The Registered Hospital

The Registered Hospital is also a separate independent data controller when it processes personal data made available through the Masimo SafetyNet Clinician Portal because the Registered Hospital determines the purposes and means of processing the personal data, including providing care to the patient. Masimo has no control over such personal data processing.



Therefore, the Registered Hospital shall ensure its own compliance with the GDPR when it collects and processes patients' data through Masimo SafetyNet.

According to Article 28 of the GDPR, a processing contract or legal act is required only between a data controller and a data processor. Moreover, according to Article 26 of the GDPR, an arrangement between data controllers is required only between joint data controllers. Two or more controllers are joint controllers only when they jointly determine the purposes and means of processing.

Consequently, no Article 28 GDPR data processor agreement or Article 26 GDPR arrangement is required between two separate data controllers (i.e., Masimo and the Registered Hospital). Nevertheless, Masimo can provide the Registered Hospital with a set of Data Protection Terms describing how it processes personal data as a data controller and other commitments it makes regarding the processing of personal data.

6. Masimo's data protection officer:

In accordance with Article 37 of the GDPR, Masimo has appointed a data protection officer: Dr. Sebastian Kraska.

You can reach him directly at privacy@masimo.com.

7. Masimo's authorized processors:

A processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

- Masimo's main processor is Amazon Web Services (AWS). Masimo has made a data protection agreement with its processor AWS in accordance with Article 28 of the GDPR: the Service Terms between Masimo and AWS incorporate the AWS GDPR Data Processing Addendum (DPA) and the AWS Supplementary Addendum to the DPA (see: https://aws.amazon.com/service-terms/).
- Masimo's secondary processors include Masimo Corporation (the parent entity) and other subsidiaries or branches depending on the location of the Registered Hospital, which may provide troubleshooting services from time to time. Masimo has made a data protection agreement and EU Standard Contractual Clauses with Masimo Corporation and its subsidiaries and affiliates within the Masimo Group in accordance with Articles 28 and 46 of the GDPR.

8. Patients can exercise their data subject rights:

Masimo has taken steps to enable patients to exercise their rights as data subjects related to their data received by Masimo SafetyNet in accordance with Articles 12-23 of the GDPR. For instance:

- At the time the patient registers to use Masimo SafetyNet, Masimo provides the patient with its Masimo SafetyNet Privacy Notice and a request of consent to process the patient's data.
- Masimo will provide patients with access to their data and respond to their requests to delete their data.
- The patient can restrict Masimo's processing and sharing of the data and withdraw consent by notifying Masimo or otherwise terminating their account.
- The patient can also export his/her data to other applications, such as Apple Health, Google Fit, and Samsung Health.
- The patient can submit a request to exercise his/her rights to Masimo or to the Registered Hospital. Masimo follows a standard procedure for responding to data subject rights requests via privacy@masimo.com or via regular mail.

9. A high level of security measures is in operation:

Masimo has implemented numerous technical and organizational security measures intended to protect personal data collected via Masimo SafetyNet and to prevent data breaches:

- Masimo maintains policies, procedures and protocols to ensure that it only processes personal data lawfully, fairly, transparently, and in accordance with other privacy standards.
- Masimo products transfer data in encrypted mode to the Masimo SafetyNet App on a user's device via Secure BLE 5.0 or similar technology.
- Data transferred from a patient's device to its internal systems is encrypted via HTTPS and TLS/SSL or similar technology.
- Data is encrypted at rest in Masimo's internal systems.
- AWS hosts Masimo SafetyNet in a private cloud that maintains high security standard certifications (see extract below).
- The patient can only access the Masimo SafetyNet App from his/her mobile device and only with individual authentication.
- The patient determines which third parties may access his/her health information, which may include the Registered Hospital, other HCPs, family members, friends, and/or other individuals.
- Only registered HCPs of the Registered Hospital have access to the Masimo SafetyNet Clinician Portal with individual authentication.
- When the patient uninstalls the Masimo SafetyNet App, all data stored in the app is automatically removed from his/her mobile device.
- Masimo designs its services and internal systems with data privacy principles in mind.
- Masimo has conducted a Data Protection Impact Assessment to review the risks to freedoms and rights of the data subjects and, through this process, determined medium risk.
- Masimo also regularly monitors and audits its data processing practices and security measures.

10. The data retention period:

Masimo's policy is to retain data only for **as long as is necessary to achieve the purposes** of Masimo SafetyNet.

Retention periods are dependent on the individual patient's and their HCP's preferences and how long they use Masimo SafetyNet. **Masimo follows an internal retention schedule for user data to help Masimo limit retention to that necessary to achieve the purposes of Masimo SafetyNet.**

The Registered Hospital, which is also a data controller for purposes of the GDPR, with access to the data, determines its own policies with respect to its retention of data if it has stored the data on its own information systems.

11. Storage locations of the data

Masimo SafetyNet's private "cloud" is located in the **European Union**:

- Frankfurt, Germany for the primary data center.
- Dublin, Ireland for the disaster recovery center.

The patient gives **express consent** to transferring his/her personal data outside of his/her jurisdiction when registering to use the SafetyNet App.

12. Standard contractual clauses:

According to Article 46 of the GDPR, EU Standard Contractual Clauses are only required where an entity within the European Economic Area (EEA) exports personal data to an entity outside the EEA or an adequate jurisdiction, and no other adequate mechanism applies.

No EU Standard Contractual Clauses with the Registered Hospital are required because there is no personal data exportation outside the EEA between the data controllers (i.e. the Registered Hospital and Masimo):

- The data controller, Masimo, is established in **Austria**.
- The Registered Hospital—which is also a data controller—is established in **a country of the EEA**.

Moreover, in accordance with Article 46 of the GDPR, Masimo has entered into Data Protection Agreements and Standard Contractual Clauses with its parent and affiliates to help ensure that user data is adequately protected by Masimo's affiliates in non-EEA countries, including Masimo Corporation in the United States.

Masimo undertakes appropriate due diligence and performs risk assessments regarding the data protection laws of the non-EEA jurisdictions to which personal data is exported.

Amazon Web Services Compliance Program

The AWS Compliance Program helps customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance Enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment.

IT standards AWS comply with are broken out by Certifications and Attestations; Laws, Regulations and Privacy; and Alignments and Frameworks. Compliance certifications and attestations are assessed by a third party, independent auditor and result in a certification, audit report, or attestation of compliance.

Extract from https://aws.amazon.com/compliance/programs/

Masimo U.S.
Tel: 1 877 4 Masimo
info-america@masimo.com

Masimo International
Tel: +41 32 720 1111
info-international@masimo.com

PLCO-005489/PLM-13585A-1221