

## **DATA PROCESSING AGREEMENT**

### **1. Purpose of this Data Processing Agreement**

1.1 This Data Processing Agreement ("DPA") sets out the rights and obligations of the parties when the Data Processor (Appsens AS, owner of ECG247) processes personal data and patient data on behalf of the healthcare professional acting as Data Controller.

1.2 The purpose of this DPA is to ensure that the Parties comply with applicable data protection laws, including Regulation (EU) 2016/679 (the "GDPR"), applicable national data protection legislation, and laws governing the processing, storage, security, and protection of health-related information, including regulatory requirements applicable to medical devices.

1.3 This DPA contains provisions regarding the Data Controller's responsibilities and obligations, including clarification of the legal basis for processing, creation and maintenance of user databases, deletion of patient information, and incident management.

1.4 The Parties acknowledge that ECG247 is a CE-marked medical device regulated under Regulation (EU) 2017/745 (MDR) and that certain processing activities may be necessary to fulfil regulatory obligations relating to post-market surveillance, vigilance reporting, complaint handling, trend reporting, and traceability

### **2. Definitions**

Applicable Data Protection Legislation means the applicable version of the General Data Protection Regulation (EU) 2016/679 ("GDPR"), national data protection legislation implementing or supplementing the GDPR, and any other applicable laws governing the processing and protection of personal data and patient data.

For privacy terms not defined in this DPA, the definitions contained in Article 4 GDPR shall apply.

### **3. Purpose of the Processing**

The Data Controller uses the ECG247 cardiac monitoring system provided by the Data Processor for the monitoring, detection, analysis, and diagnosis of cardiac arrhythmia and related clinical conditions in patients.

The processing includes:

- Data relating to the Data Controller
- Name
- Email address

- Password
- Mobile phone number
- Patient Data
- Personal identification number/ID
- Name (optional)
- Address (optional)
- Mobile phone number (optional)
- Risk factors (optional)
- ECG recordings
- Possibility of Pseudonymization

When registering a patient in the ECG247 portal, the Data Controller may use a pseudonymization process where the Data Controller maintains a separate code key independent of the ECG247 system. In such cases, no directly identifying patient information is stored within the ECG247 service.

#### **4. Duration of Processing**

Personal Data shall not be retained for longer than necessary to fulfil the purposes for which it was collected and processed, unless a longer retention period is required by applicable law, regulatory requirements, or documented instructions from the Data Controller.

#### **5. Responsibilities and Obligations of the Data Controller**

The Data Controller shall be responsible for ensuring that all Personal Data is collected and processed in accordance with Applicable Data Protection Legislation and that a valid legal basis exists for the processing activities conducted using ECG247.

The Data Controller shall ensure that:

- Processing is limited to specified purposes and is based on a valid legal basis.
- Data subjects have received necessary information regarding the processing.
- Any required patient consent has been obtained where consent constitutes the legal basis for processing.
- The use of ECG247 complies with applicable healthcare legislation.

#### **6. Obligations of the Data Processor**

The Data Processor provides and maintains the ECG247 platform and associated services, including the technical infrastructure necessary for the secure processing of Personal Data on behalf of the Data Controller:

- Secure cloud backend services for storage of data generated by ECG247.
- Secure authentication and authorization services.
- ECG247 mobile application for patients.
- ECG247 web portal for healthcare professionals.
- The ECG247 cloud environment is based on Microsoft Azure cloud services with primary data storage located within the European Economic Area (EEA), currently hosted through Microsoft Azure services in Northern Europe.
- Appsens AS has entered into a separate Data Processing Agreement with Microsoft for cloud hosting services.
- The Data Processor shall process personal data only on documented instructions from the Data Controller unless otherwise required by Union or Member State law.

## **7. Confidentiality**

7.1 The Data Processor shall ensure that employees and other people with access to data stored in ECG247 are authorized to process such information.

7.2 Access shall only be granted to people who require such access in order to maintain secure and reliable operation of the ECG247 service or to comply with legal obligations.

7.3 Authorized persons shall be bound by appropriate confidentiality obligations.

## **8. Assistance with the Data Controller**

8.1 The Data Processor shall, upon request, assist the Data Controller in fulfilling data subject rights under Chapter III of the GDPR through appropriate technical and organizational measures.

8.2 The Data Processor shall promptly forward any requests received from data subjects concerning their rights under applicable data protection legislation.

8.3 The Data Processor shall provide reasonable assistance to the Data Controller in fulfilling its obligations under Articles 32 to 36 of the GDPR, considering the nature of the processing and the information available to the Data Processor:

- Security of processing
- Personal data breach notifications
- Data Protection Impact Assessments (DPIAs)
- Prior consultations with supervisory authorities

8.4 Where assistance exceeds the Data Processor's statutory obligations, the Data Processor may charge documented and reasonable costs.

## **9. Security of Processing**

9.1 The Data Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

9.2 The Data Processor shall implement and maintain appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR. to ensure:

- Confidentiality
- Integrity
- Availability
- Resilience of processing systems

9.3 The Data Processor shall document risk assessments and security measures and make relevant documentation available upon reasonable request.

## **10. Personal Data Breaches**

The Data Processor shall notify the Data Controller without undue delay of any personal data breach.

The notification shall include:

- Nature of the breach
- Categories and number of affected data subjects
- Categories and volume of affected data
- Contact details for further information
- Likely consequences
- Mitigation and remediation measures taken or proposed

The Data Controller remains responsible for notifications to supervisory authorities and affected data subjects as required by GDPR Articles 33 and 34.

## **11. Use of Subprocessors**

At the Effective Date of this Agreement, the Data Processor engages the following Subprocessor: Microsoft Ireland Operations Limited (Microsoft Azure cloud hosting and infrastructure services).

The Data Processor shall enter into written agreements with all subprocessors imposing equivalent data protection obligations.

The Data Controller shall be informed of material changes to subprocessors in advance.

## **12. Transfers Outside the EEA**

The Data Processor shall not transfer Personal Data outside the EEA except in accordance with Chapter V of the GDPR and only where appropriate safeguards have been implemented.

Where access requests from third-country authorities occur, the Data Processor shall apply appropriate safeguards and assess compliance with GDPR requirements, including the principles established following the Schrems II judgment.

## **13. Term and Termination**

This DPA remains in force for as long as the Data Controller uses the ECG247 services.

Upon termination:

- Upon termination or expiry of the services, the Data Controller may instruct the Data Processor to return or securely delete Personal Data, except where continued retention is required by applicable law or regulatory obligations.
- Access shall be revoked.
- Personal data shall be deleted or anonymized unless retention is required by applicable law or MDR obligations.
- The Data Processor shall provide written confirmation of deletion upon request.

## **14. Medical Device Regulatory Compliance**

The Parties acknowledge that ECG247 is a CE-marked medical device regulated under Regulation (EU) 2017/745 on Medical Devices ("MDR"), and that certain processing activities may be necessary to fulfil regulatory obligations relating to product safety, vigilance, post-market surveillance, and traceability.

The Data Processor shall maintain:

- A valid CE marking where applicable.
- An MDR-compliant Quality Management System.
- Procedures for vigilance reporting and post-market surveillance.
- Appropriate cybersecurity and software lifecycle controls.
- Records required by MDR for traceability, safety monitoring, and regulatory compliance.

This data processing shall be limited to what is necessary to meet applicable MDR obligations.

## **15. GDPR Article 28 Compliance**

The Data Processor shall process Personal Data only on documented instructions from the Data Controller and in accordance with applicable data protection laws.

The Data Processor shall:

- Ensure that persons authorized to process Personal Data are subject to confidentiality obligations;
- Implement appropriate technical and organizational measures to protect Personal Data in accordance with Article 32 GDPR;
- Assist the Data Controller, where reasonably required, in fulfilling its obligations regarding data subject rights, personal data breaches, Data Protection Impact Assessments (DPIAs), and consultations with supervisory authorities;
- Notify the Data Controller without undue delay after becoming aware of a Personal Data Breach;
- Engage subprocessors only under written agreements imposing data protection obligations equivalent to those set out in this Agreement and remain responsible for their performance;
- Provide the Data Controller with information reasonably necessary to demonstrate compliance with this Agreement and applicable data protection laws;
- Upon termination of the Services, delete or return Personal Data at the choice of the Data Controller unless retention is required by applicable law or regulatory obligations.
- The Data Processor shall not transfer Personal Data outside the European Economic Area (EEA) except in compliance with Chapter V of the GDPR and subject to appropriate safeguards.

## **16. Audit rights**

The Data Controller may, upon reasonable notice and no more than once annually, conduct an audit or request relevant documentation to verify compliance with this Agreement. The Data Processor may satisfy such requests by providing relevant certifications, audit reports, security assessments or equivalent documentation

## **17. Subprocessor Notification**

The Data Processor shall notify the Data Controller at least thirty (30) days in advance of any intended addition or replacement of a subprocessor. The Data Controller may object to the proposed change on reasonable data protection grounds within the notification period.

07. October 2026

Appsens AS

For privacy and security matters: **post@ecg247.com**