

DATENVERARBEITUNGSVEREINBARUNG

(Data Processing Agreement)

1. Zweck dieser Datenverarbeitungsvereinbarung

1.1 Diese Datenverarbeitungsvereinbarung („DPA“) regelt die Rechte und Pflichten der Parteien, wenn der Auftragsverarbeiter (**Appsens AS**, Eigentümer von **ECG247**) personenbezogene Daten und Patientendaten im Auftrag des medizinischen Fachpersonals verarbeitet, das als Verantwortlicher handelt.

1.2 Zweck dieser DPA ist es, sicherzustellen, dass die Parteien die geltenden Datenschutzgesetze einhalten, einschließlich der Verordnung (EU) 2016/679 („DSGVO“), der anwendbaren nationalen Datenschutzgesetzgebung sowie der Gesetze zur Verarbeitung, Speicherung, Sicherheit und zum Schutz gesundheitsbezogener Informationen, einschließlich regulatorischer Anforderungen für Medizinprodukte.

1.3 Diese DPA enthält Bestimmungen zu den Verantwortlichkeiten und Pflichten des Verantwortlichen, einschließlich der Klärung der Rechtsgrundlage der Verarbeitung, der Erstellung und Pflege von Benutzerdatenbanken, der Löschung von Patientendaten sowie des Vorfallsmanagements.

1.4 Die Parteien erkennen an, dass **ECG247** ein CE-gekennzeichnetes Medizinprodukt ist, das gemäß der Verordnung (EU) 2017/745 (MDR) reguliert wird, und dass bestimmte Verarbeitungsvorgänge erforderlich sein können, um regulatorische Verpflichtungen hinsichtlich Marktüberwachung nach dem Inverkehrbringen, Vigilanzmeldungen, Bearbeitung von Beschwerden, Trendberichterstattung und Rückverfolgbarkeit zu erfüllen.

2. Begriffsbestimmungen

Anwendbare Datenschutzgesetzgebung bezeichnet die jeweils geltende Fassung der Datenschutz-Grundverordnung (EU) 2016/679 („DSGVO“), nationale Datenschutzgesetze zur Umsetzung oder Ergänzung der DSGVO sowie sonstige anwendbare Gesetze zur Verarbeitung und zum Schutz personenbezogener Daten und Patientendaten.

Für Datenschutzbegriffe, die in dieser DPA nicht definiert sind, gelten die Begriffsbestimmungen gemäß Artikel 4 DSGVO.

3. Zweck der Verarbeitung

Der Verantwortliche nutzt das vom Auftragsverarbeiter bereitgestellte Herzmonitoring-System **ECG247** zur Überwachung, Erkennung, Analyse und Diagnose von Herzrhythmusstörungen und damit verbundenen klinischen Zuständen bei Patienten.

Die Verarbeitung umfasst:

Daten des Verantwortlichen

- Name
- E-Mail-Adresse
- Passwort
- Mobiltelefonnummer

Patientendaten

- Personenkennziffer/Identifikationsnummer
- Name (optional)
- Anschrift (optional)
- Mobiltelefonnummer (optional)
- Risikofaktoren (optional)
- EKG-Aufzeichnungen

Möglichkeit der Pseudonymisierung

Bei der Registrierung eines Patienten im **ECG247**-Portal kann der Verantwortliche ein Pseudonymisierungsverfahren verwenden, bei dem der Verantwortliche einen separaten Code-Schlüssel führt, der unabhängig vom **ECG247**-System verwaltet wird. In solchen Fällen werden innerhalb des **ECG247**-Dienstes keine unmittelbar identifizierenden Patienteninformationen gespeichert.

4. Dauer der Verarbeitung

Personenbezogene Daten dürfen nicht länger gespeichert werden, als es zur Erfüllung der Zwecke erforderlich ist, für die sie erhoben und verarbeitet wurden, es sei denn, eine längere Aufbewahrungsfrist ist aufgrund geltender Gesetze, regulatorischer Anforderungen oder dokumentierter Weisungen des Verantwortlichen erforderlich.

5. Verantwortlichkeiten und Pflichten des Verantwortlichen

Der Verantwortliche ist dafür verantwortlich sicherzustellen, dass alle personenbezogenen Daten gemäß der anwendbaren Datenschutzgesetzgebung erhoben und verarbeitet werden und dass für die mit **ECG247** durchgeführten Verarbeitungstätigkeiten eine gültige Rechtsgrundlage besteht.

Der Verantwortliche stellt sicher, dass:

- die Verarbeitung auf festgelegte Zwecke beschränkt ist und auf einer gültigen Rechtsgrundlage beruht;

- betroffene Personen die erforderlichen Informationen über die Verarbeitung erhalten haben;
- erforderliche Einwilligungen der Patienten eingeholt wurden, sofern die Einwilligung die Rechtsgrundlage der Verarbeitung darstellt;
- die Nutzung von **ECG247** den geltenden Gesundheitsgesetzen entspricht.

6. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter stellt die Plattform **ECG247** und die zugehörigen Dienstleistungen bereit und betreibt diese, einschließlich der technischen Infrastruktur, die für die sichere Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen erforderlich ist:

- Sichere Cloud-Backend-Dienste zur Speicherung der von **ECG247** generierten Daten.
- Sichere Authentifizierungs- und Autorisierungsdienste.
- **ECG247**-Mobilanwendung für Patienten.
- **ECG247**-Webportal für medizinisches Fachpersonal.
- Die **ECG247**-Cloud-Umgebung basiert auf den Cloud-Diensten von **Microsoft Azure**, wobei sich die primäre Datenspeicherung innerhalb des Europäischen Wirtschaftsraums (EWR) befindet und derzeit über **Microsoft Azure**-Dienste in Nordeuropa gehostet wird.
- **Appsens AS** hat mit **Microsoft** eine separate Datenverarbeitungsvereinbarung für Cloud-Hosting-Dienste abgeschlossen.
- Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern nicht Unionsrecht oder das Recht eines Mitgliedstaats etwas anderes vorschreibt.

7. Vertraulichkeit

7.1 Der Auftragsverarbeiter stellt sicher, dass Mitarbeiter und andere Personen mit Zugang zu in **ECG247** gespeicherten Daten zur Verarbeitung solcher Informationen befugt sind.

7.2 Der Zugang wird ausschließlich Personen gewährt, die diesen Zugang benötigen, um einen sicheren und zuverlässigen Betrieb des **ECG247**-Dienstes aufrechtzuerhalten oder gesetzliche Verpflichtungen zu erfüllen.

7.3 Autorisierte Personen unterliegen angemessenen Vertraulichkeitsverpflichtungen.

8. Unterstützung des Verantwortlichen

8.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen auf Anfrage bei der Erfüllung der Rechte betroffener Personen gemäß Kapitel III DSGVO durch angemessene technische und organisatorische Maßnahmen.

8.2 Der Auftragsverarbeiter leitet Anfragen betroffener Personen bezüglich ihrer Rechte nach geltendem Datenschutzrecht unverzüglich an den Verantwortlichen weiter.

8.3 Der Auftragsverarbeiter unterstützt den Verantwortlichen angemessen bei der Erfüllung seiner Verpflichtungen gemäß den Artikeln 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen:

- Sicherheit der Verarbeitung
- Meldung von Datenschutzverletzungen
- Datenschutz-Folgenabschätzungen (DSFA/DPIA)
- Vorherige Konsultationen mit Aufsichtsbehörden

8.4 Sofern die Unterstützung über die gesetzlichen Verpflichtungen des Auftragsverarbeiters hinausgeht, kann dieser die nachgewiesenen und angemessenen Kosten in Rechnung stellen.

9. Sicherheit der Verarbeitung

9.1 Der Auftragsverarbeiter setzt angemessene technische und organisatorische Maßnahmen um, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten.

9.2 Der Auftragsverarbeiter implementiert und unterhält geeignete technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO, um sicherzustellen:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit der Verarbeitungssysteme

9.3 Der Auftragsverarbeiter dokumentiert Risikobewertungen und Sicherheitsmaßnahmen und stellt relevante Unterlagen auf angemessene Anfrage zur Verfügung.

10. Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über jede Verletzung des Schutzes personenbezogener Daten.

Die Mitteilung umfasst:

- Art der Verletzung
- Kategorien und Anzahl betroffener Personen
- Kategorien und Umfang der betroffenen Daten
- Kontaktdaten für weitere Informationen

- Wahrscheinliche Folgen
- Bereits ergriffene oder vorgeschlagene Abhilfemaßnahmen

Der Verantwortliche bleibt für Meldungen an Aufsichtsbehörden und betroffene Personen gemäß den Artikeln 33 und 34 DSGVO verantwortlich.

11. Einsatz von Unterauftragsverarbeitern

Zum Inkrafttreten dieser Vereinbarung setzt der Auftragsverarbeiter folgenden Unterauftragsverarbeiter ein:

Microsoft Ireland Operations Limited (Microsoft Azure Cloud-Hosting- und Infrastrukturdienste).

Der Auftragsverarbeiter schließt mit allen Unterauftragsverarbeitern schriftliche Vereinbarungen ab, die gleichwertige Datenschutzpflichten vorsehen.

Der Verantwortliche wird im Voraus über wesentliche Änderungen bei Unterauftragsverarbeitern informiert.

12. Übermittlungen außerhalb des EWR

Der Auftragsverarbeiter übermittelt personenbezogene Daten nicht außerhalb des EWR, außer in Übereinstimmung mit Kapitel V DSGVO und nur dann, wenn geeignete Garantien umgesetzt wurden.

Werden Zugriffsanfragen von Behörden aus Drittländern gestellt, wendet der Auftragsverarbeiter geeignete Schutzmaßnahmen an und prüft die Einhaltung der DSGVO-Anforderungen, einschließlich der Grundsätze, die sich aus dem Urteil **Schrems II** ergeben.

13. Laufzeit und Beendigung

Diese DPA bleibt in Kraft, solange der Verantwortliche die **ECG247**-Dienste nutzt.
Bei Beendigung:

- Der Verantwortliche kann den Auftragsverarbeiter anweisen, personenbezogene Daten zurückzugeben oder sicher zu löschen, sofern keine gesetzliche oder regulatorische Pflicht zur weiteren Aufbewahrung besteht.
- Die Zugriffsrechte werden entzogen.
- Personenbezogene Daten werden gelöscht oder anonymisiert, sofern keine gesetzliche Aufbewahrungspflicht oder Verpflichtung nach der MDR besteht.

- Der Auftragsverarbeiter stellt auf Anfrage eine schriftliche Bestätigung der Löschung zur Verfügung.

14. Einhaltung der Medizinproduktevorschriften

Die Parteien erkennen an, dass **ECG247** ein CE-gekennzeichnetes Medizinprodukt gemäß der Verordnung (EU) 2017/745 über Medizinprodukte („MDR“) ist und dass bestimmte Verarbeitungsvorgänge erforderlich sein können, um regulatorische Verpflichtungen hinsichtlich Produktsicherheit, Vigilanz, Marktüberwachung nach dem Inverkehrbringen und Rückverfolgbarkeit zu erfüllen.

Der Auftragsverarbeiter unterhält:

- eine gültige CE-Kennzeichnung, soweit anwendbar;
- ein MDR-konformes Qualitätsmanagementsystem;
- Verfahren zur Vigilanzberichterstattung und Marktüberwachung nach dem Inverkehrbringen;
- angemessene Cybersicherheits- und Software-Lifecycle-Kontrollen;
- die nach MDR erforderlichen Aufzeichnungen zur Rückverfolgbarkeit, Sicherheitsüberwachung und regulatorischen Compliance.

Diese Datenverarbeitung ist auf das zur Erfüllung der anwendbaren MDR-Verpflichtungen erforderliche Maß beschränkt.

15. Einhaltung von Artikel 28 DSGVO

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisungen des Verantwortlichen und in Übereinstimmung mit den geltenden Datenschutzgesetzen.

Der Auftragsverarbeiter wird:

- sicherstellen, dass zur Verarbeitung personenbezogener Daten befugte Personen Vertraulichkeitsverpflichtungen unterliegen;
- geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten gemäß Artikel 32 DSGVO umsetzen;
- den Verantwortlichen angemessen bei der Erfüllung seiner Verpflichtungen hinsichtlich Betroffenenrechten, Datenschutzverletzungen, Datenschutz-Folgenabschätzungen (DPIAs) und Konsultationen mit Aufsichtsbehörden unterstützen;
- den Verantwortlichen unverzüglich benachrichtigen, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist;

- Unterauftragsverarbeiter nur auf Grundlage schriftlicher Vereinbarungen einsetzen, die gleichwertige Datenschutzverpflichtungen enthalten, und für deren Leistung verantwortlich bleiben;
- dem Verantwortlichen die Informationen bereitstellen, die vernünftigerweise erforderlich sind, um die Einhaltung dieser Vereinbarung und der geltenden Datenschutzgesetze nachzuweisen;
- nach Beendigung der Dienstleistungen die personenbezogenen Daten nach Wahl des Verantwortlichen löschen oder zurückgeben, sofern keine gesetzliche oder regulatorische Aufbewahrungspflicht besteht;
- personenbezogene Daten nicht außerhalb des Europäischen Wirtschaftsraums (EWR) übermitteln, außer unter Einhaltung von Kapitel V DSGVO und unter Anwendung geeigneter Schutzmaßnahmen.

16. Auditrechte

Der Verantwortliche kann nach angemessener Vorankündigung und höchstens einmal jährlich ein Audit durchführen oder relevante Unterlagen anfordern, um die Einhaltung dieser Vereinbarung zu überprüfen.

Der Auftragsverarbeiter kann solchen Anfragen nachkommen, indem er relevante Zertifizierungen, Auditberichte, Sicherheitsbewertungen oder gleichwertige Dokumentationen bereitstellt.

17. Benachrichtigung über Unterauftragsverarbeiter

Der Auftragsverarbeiter informiert den Verantwortlichen mindestens dreißig (30) Tage im Voraus über jede beabsichtigte Hinzunahme oder Ersetzung eines Unterauftragsverarbeiters.

Der Verantwortliche kann innerhalb der Benachrichtigungsfrist aus begründeten datenschutzrechtlichen Gründen Einspruch gegen die vorgeschlagene Änderung erheben.

07. Oktober 2026

Appsens AS

Für Datenschutz- und Sicherheitsanfragen: post@ecg247.com