

DATABEHANDLERAVTALE

1. Formål med denne databehandleravtalen

1.1 Denne databehandleravtalen ("DPA") fastsetter partenes rettigheter og plikter når Databehandleren (Appsens AS, eier av ECG247) behandler personopplysninger og pasientopplysninger på vegne av helsepersonellet som opptrer som Behandlingsansvarlig.

1.2 Formålet med denne databehandleravtalen er å sikre at partene etterlever gjeldende personvernlovgivning, herunder forordning (EU) 2016/679 ("GDPR"), nasjonal personvernlovgivning, samt lover og regler som regulerer behandling, lagring, sikkerhet og beskyttelse av helseopplysninger, inkludert regulatoriske krav som gjelder for medisinsk utstyr

1.3 Denne databehandleravtalen inneholder bestemmelser om den Behandlingsansvarliges ansvar og forpliktelser, herunder avklaring av behandlingsgrunnlag, opprettelse og vedlikehold av brukerdatabaser, sletting av pasientinformasjon og håndtering av hendelser

1.4 Partene erkjenner at ECG247 er et CE-merket medisinsk utstyr regulert av forordning (EU) 2017/745 (MDR), og at enkelte behandlingsaktiviteter kan være nødvendige for å oppfylle regulatoriske forpliktelser knyttet til overvåking etter markedsføring, rapportering av alvorlige hendelser, klagehåndtering, trendrapportering og sporbarhet.

2. Definisjoner

Gjeldende personvernlovgivning betyr gjeldende versjon av personvernforordningen (EU) 2016/679 ("GDPR"), nasjonal personvernlovgivning som gjennomfører eller supplerer GDPR, samt annen lovgivning som regulerer behandling og beskyttelse av personopplysninger og pasientopplysninger.

For personvernbegreper som ikke er definert i denne avtalen, gjelder definisjonene i GDPR artikkel 4.

3. Formålet med behandlingen

Den Behandlingsansvarlige bruker ECG247-systemet for hjerteovervåking, levert av Databehandleren, til overvåking, deteksjon, analyse og diagnostisering av hjerterytmier og relaterte kliniske tilstander hos pasienter.

Behandlingen omfatter:

Opplysninger om den Behandlingsansvarlige

- Navn
- E-postadresse
- Passord
- Mobiltelefonnummer

Pasientopplysninger

- Fødselsnummer/ID
- Navn (valgfritt)
- Adresse (valgfritt)
- Mobiltelefonnummer (valgfritt)
- Risikofaktorer (valgfritt)
- EKG-opptak

Mulighet for pseudonymisering

Ved registrering av en pasient i ECG247-portalen kan den Behandlingsansvarlige benytte en pseudonymiseringsprosess hvor den Behandlingsansvarlige opprettholder en separat kodenøkkel uavhengig av ECG247-systemet. I slike tilfeller lagres ingen direkte identifiserende pasientopplysninger i ECG247-tjenesten.

4. Behandlingens varighet

Personopplysninger skal ikke oppbevares lenger enn nødvendig for å oppfylle formålene de ble samlet inn og behandlet for, med mindre en lengre lagringsperiode kreves etter gjeldende lovgivning, regulatoriske krav eller dokumenterte instruksjoner fra den Behandlingsansvarlige.

5. Den Behandlingsansvarliges ansvar og plikter

Den Behandlingsansvarlige er ansvarlig for at alle personopplysninger innsamles og behandles i samsvar med gjeldende personvernlovgivning, og at det foreligger et gyldig behandlingsgrunnlag for behandlingsaktivitetene som utføres ved bruk av ECG247.

Den Behandlingsansvarlige skal sikre at:

- Behandlingen er begrenset til spesifiserte formål og bygger på gyldig behandlingsgrunnlag.
- Registrerte har mottatt nødvendig informasjon om behandlingen.
- Eventuelt nødvendig pasientsamtykke er innhentet der samtykke utgjør behandlingsgrunnlaget.
- Bruken av ECG247 er i samsvar med gjeldende helselovgivning.

6. Databehandlerens forpliktelser

Databehandleren leverer og vedlikeholder ECG247-plattformen og tilknyttede tjenester, inkludert den tekniske infrastrukturen som er nødvendig for sikker behandling av personopplysninger på vegne av den Behandlingsansvarlige.

Dette omfatter:

- Sikre skybaserte backend-tjenester for lagring av data generert av ECG247.
- Sikre autentiserings- og autorisasjonstjenester.
- ECG247 mobilapplikasjon for pasienter.
- ECG247 webportal for helsepersonell.

- ECG247s skymiljø er basert på Microsoft Azure-tjenester, med primær datalagring innenfor EØS, for tiden lokalisert i Nord-Europa.
- Appsens AS har inngått en egen databehandleravtale med Microsoft for skytjenestene.
- Databehandleren skal kun behandle personopplysninger i henhold til dokumenterte instruksjoner fra den Behandlingsansvarlige, med mindre annet kreves etter EU- eller nasjonal lovgivning.

7. Konfidensialitet

7.1 Databehandleren skal sikre at ansatte og andre personer med tilgang til data lagret i ECG247 er autorisert til å behandle slik informasjon.

7.2 Tilgang skal kun gis til personer som trenger slik tilgang for å opprettholde sikker og pålitelig drift av ECG247-tjenesten eller for å oppfylle lovpålagte forpliktelser.

7.3 Autoriserte personer skal være underlagt passende taushetsplikt.

8. Bistand til den Behandlingsansvarlige

Databehandleren skal på forespørsel bistå den Behandlingsansvarlige med å oppfylle de registrertes rettigheter etter GDPR kapittel III gjennom passende tekniske og organisatoriske tiltak. Databehandleren skal også uten ugrunnet opphold videreformidle forespørsler fra registrerte.

Databehandleren skal gi rimelig bistand til oppfyllelse av GDPR artikkel 32-36, herunder:

- Behandlingssikkerhet
- Varsling om personopplysningsbrudd
- Personvernkonsekvensvurderinger (DPIA)
- Forhåndsdrøftelser med tilsynsmyndigheter

Dersom bistanden går utover Databehandlerens lovpålagte plikter, kan Databehandleren kreve dokumenterte og rimelige kostnader dekket.

9. Behandlingssikkerhet

Databehandleren skal implementere og vedlikeholde egnede tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som står i forhold til risikoen, i samsvar med GDPR artikkel 32.

Tiltakene skal sikre:

- Konfidensialitet
- Integritet
- Tilgjengelighet
- Robusthet i behandlingssystemene

Databehandleren skal dokumentere risikovurderinger og sikkerhetstiltak og gjøre relevant dokumentasjon tilgjengelig etter rimelig forespørsel.

10. Personopplysningsbrudd

Databehandleren skal uten ugrunnet opphold varsle den Behandlingsansvarlige om ethvert personopplysningsbrudd.

Varslingen skal inkludere:

- Bruddets art
- Kategorier og antall berørte registrerte
- Kategorier og omfang av berørte opplysninger
- Kontaktinformasjon for videre oppfølging
- Sannsynlige konsekvenser
- Iverksette eller foreslåtte avbøtende tiltak

Den Behandlingsansvarlige er ansvarlig for varsling til tilsynsmyndigheter og registrerte i henhold til GDPR artikkel 33 og 34.

11. Bruk av underdatabehandlere

På ikrafttredelsestidspunktet benytter Databehandleren følgende underdatabehandler:

- Microsoft Ireland Operations Limited (Microsoft Azure skytjenester og infrastruktur) Databehandleren skal inngå skriftlige avtaler med alle underdatabehandlere som pålegger tilsvarende personvernforpliktelser som i denne avtalen.

Den Behandlingsansvarlige skal informeres på forhånd om vesentlige endringer i bruk av underdatabehandlere.

12. Overføringer utenfor EØS

Databehandleren skal ikke overføre personopplysninger utenfor EØS med mindre dette skjer i samsvar med GDPR kapittel V og med nødvendige garantier på plass

Ved forespørsler om tilgang fra myndigheter i tredjeland skal Databehandleren anvende nødvendige sikkerhetsmekanismer og vurdere etterlevelsen opp mot GDPR, inkludert prinsippene etablert gjennom Schrems II-dommen.

13. Avtalens varighet og opphør

Denne databehandleravtalen gjelder så lenge den Behandlingsansvarlige benytter ECG247-tjenestene.

Ved opphør:

- Den Behandlingsansvarlige kan instruere Databehandleren om å returnere eller sikkert slette personopplysninger, med mindre videre oppbevaring kreves etter lov eller regulatoriske krav.
- Tilgang skal tilbakekalles.
- Personopplysninger skal slettes eller anonymiseres med mindre oppbevaring kreves etter lov eller MDR-forpliktelser.
- Databehandleren skal på forespørsel gi skriftlig bekreftelse på sletting.

14. Etterlevelse av regelverk for medisinsk utstyr

Partene erkjenner at ECG247 er et CE-merket medisinsk utstyr regulert av MDR (EU) 2017/745, og at enkelte behandlingsaktiviteter kan være nødvendige for å oppfylle regulatoriske krav knyttet til produktsikkerhet, overvåkning etter markedsføring, rapportering av hendelser og sporbarhet.

Databehandleren skal opprettholde:

- Gyldig CE-merking der dette kreves.
- Et MDR-kompatibelt kvalitetsstyringssystem.
- Rutiner for rapportering av hendelser og overvåkning etter markedsføring.
- Egnede tiltak for cybersikkerhet og programvarelivssyklus.
- Nødvendige registre for sporbarhet, sikkerhetsovervåkning og regulatorisk etterlevelse.

Slik behandling skal begrenses til det som er nødvendig for å oppfylle MDR-forpliktelser.

15. Etterlevelse av GDPR artikkel 28

Databehandleren skal kun behandle personopplysninger etter dokumenterte instruksjoner fra den Behandlingsansvarlige og i samsvar med gjeldende personvernlovgivning.

Databehandleren skal:

- Sikre at autoriserte personer er underlagt taushetsplikt.
- Implementere egnede tekniske og organisatoriske sikkerhetstiltak i samsvar med GDPR artikkel 32.
- Bistå den Behandlingsansvarlige ved behov med registrertes rettigheter, personopplysningsbrudd, DPIA og dialog med tilsynsmyndigheter.
- Varsle uten ugrunnet opphold ved personopplysningsbrudd.
- Kun benytte underdatabehandlere som er kontraktsmessig pålagt tilsvarende personvernforpliktelser.
- Gi informasjon som er rimelig nødvendig for å dokumentere etterlevelse.
- Ved opphør slette eller returnere personopplysninger etter den Behandlingsansvarliges valg, med mindre oppbevaring kreves etter lov eller regulatoriske krav.
- Ikke overføre personopplysninger utenfor EØS uten at GDPR kapittel V etterleves og nødvendige garantier foreligger.

16. Revisjonsrett

Den Behandlingsansvarlige kan, etter rimelig varsel og ikke mer enn én gang årlig, gjennomføre en revisjon eller be om relevant dokumentasjon for å verifisere etterlevelsen av denne avtalen. Databehandleren kan oppfylle slike forespørsler ved å fremlegge relevante sertifiseringer, revisjonsrapporter, sikkerhetsvurderinger eller tilsvarende dokumentasjon.

17. Varsling om underdatabehandlere

Databehandleren skal varsle den Behandlingsansvarlige minst tretti (30) dager før planlagt tillegg eller utskifting av underdatabehandler. Den Behandlingsansvarlige kan innen varslingsperioden fremsette innsigelser på rimelige personvernmessige grunnlag.

7. oktober 2026

Appsens AS

For personvern- og sikkerhetsspørsmål: post@ecg247.com