SØRLANDET SYKEHUS

DATABEHANDLERAVTALE

mellom

Sørlandet sykehus HF

Org.nr.: 983 975 240

heretter benevnt "*Dataansvarlig*"

og

Leverandør

Org.nr.: nnn nnn nnn

heretter benevnt "*Databehandler*"

i forbindelse med levering av tjenester i henhold til den til enhver tid gjeldende Tjenesteavtale

Innholdsfortegnelse

1 Innledning 3
1.1 Fotnoter 3
2 Formål 3
2.1 Databehandlers oppdrag 3
2.2 Behandlingens art 3
2.3 Behandlingens formål 3
2.4 Kategorier av registrerte 3
2.5 Hvilke personopplysninger behandles 3
3 Definisjoner 3
4 Forholdet mellom Dataansvarlig og Databehandler 4
5 Forholdet mellom Databehandleravtalen og Tjenesteavtalen 4
5.1 Rangordning 5
6 Databehandlerens rolle og ansvar 5
7 Krav til Databehandlerens informasjonssikkerhet 6
7.1 Overordnede krav 6
7.2 Databehandlerens tiltak 6
7.3 Krav til teknisk sikkerhet 6
7.4 Krav til adgangskontroll 7
7.5 Krav til fysisk sikkerhet 7
7.6 Risikovurdering ved endringer i databehandlingen 7
8 Varsel og bistand ved avvik 7
8.1 Varselets innhold 8
9 Ansvar for behandlingen 8
10 Taushetsplikt 8
11 Databehandlerens bruk av underleverandører 8
12 Overføring 9
12.1 Overføring til utlandet eller internasjonale organisasjoner 9
13 Innsyn, verifikasjon og revisjon mv. 9
14 Varighet, oppsigelse og opphør 10
15 Opphør 10
16 Mislighold 10
17 Tvisteløsning 10
18 Undertegning 10

1 Innledning

Databehandler og Dataansvarlig, i fellesskap omtalt som «*Partene*», har inngått herværende databehandleravtale, heretter «*Databehandleravtalen*».

Databehandler er leverandør av tjenesten tjenestenavn og Databehandleravtalen omfatter alle forhold knyttet til leveranse av denne tjenesten.

1.1 FOTNOTER

Når det i Databehandleravtalen vises til dokumentasjon eller informasjon med bruk av fotnoter med elektronisk url må Dataansvarlig, Databehandler, og eventuelle underleverandører sørge for å lese og forstå disse.

2 Formål

Denne Databehandleravtalen har som formål å regulere Databehandlers behandling av personopplysninger på vegne av Dataansvarlig.

Databehandleravtalen skal sikre at personopplysninger ikke behandles i strid med lov, ikke deles med uvedkommende, og at all behandling av personopplysninger er i henhold til den Dataansvarliges instruksjoner.

Databehandleravtalen skal sikre at personopplysninger behandles i samsvar med kravene i den til enhver tid gjeldende personvernlovgivning, og Partenes rettigheter og plikter.

Behandlingen av Personopplysninger omfatter kun den behandling som er nødvendig for at Databehandler skal kunne gjennomføre Tjenesteavtalen med den Dataansvarlige.

2.1 DATABEHANDLERS OPPDRAG

<Temaet skal beskrive hva databehandleroppdraget faktisk går ut på. Er for eksempel oppdraget at databehandleren skal lagre den behandlingsansvarliges kundeopplysninger i sin skyløsning? Skal databehandleren sende ut markedsføringshenvendelser på vegne av databehandleren? Skal databehandleren administrere den behandlingsansvarliges kameraovervåkingssystem?>

2.2 BEHANDLINGENS ART

<Beskriv om behandlingen gjøres i et system, hvorfor leverandøren trenger å utføre behandlingen, og hva systemet som benyttes skal brukes til.>

2.3 BEHANDLINGENS FORMÅL

<Beskriv formålet med behandling av personopplysninger.>

2.4 KATEGORIER AV REGISTRERTE

<Beskriv kategorier av de registrerte, der eksempler på kategorier av registrerte er ansatte, medlemmer, kunder, pasienter, elever og lignende.>

2.5 HVILKE PERSONOPPLYSNINGER BEHANDLES

<Beskriv hva slags personopplysninger som behandles, for eksempel navn, telefonnummer, fødselsdato, kjøpshistorikk, kundenummer, logginformasjon, helseopplysninger og så videre.>

3 Definisjoner

Databehandleravtalen skal forstås på bakgrunn av følgende definisjoner:

Personvernregelverket:	Inkluderer norsk implementering av Europaparlament- og Rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (GDPR) i lov om behandling av personopplysninger. Med mindre annet er spesifisert gjelder alle referanser til GDPR som en henvisning til norsk implementering av personvernforordningen i nasjonal rett, og norsk tolkning av denne.
Personopplysning:	Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»), jf. GDPR art. 4 (1)
Behandling:	Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring, jf. GDPR art. 4 (2)
Dataansvarlig:	Virksomheten som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. GDPR art. 4 (7)
Databehandler:	Leverandør som behandler personopplysninger på vegne av den Dataansvarlige, jf. GDPR art. 4 (8)
Protokoll over behandlingsaktiviteter:	Protokoll over behandlingsaktiviteter er Databehandler sin oversikt over de behandlinger av personopplysninger som gjøres på vegne av Dataansvarlig. Protokoll over behandlingsaktiviteter dekker pålagte krav i henhold til GDPR, i tillegg til annen informasjon som er nødvendig for arbeidet med personvern. Protokoll over behandlingsaktiviteter vedlegges denne avtalen som en interaktiv URL, og skal linkes både til ROS og Tjenesteavtalen.
ROS:	ROS er forkortelse for risiko- og sårbarhetsvurdering. I ROS fremgår det hvilke personopplysninger som blir behandlet, samt annen relevant informasjon i henhold til GDPR. ROS kartlegger informasjonssikkerhetsmessig risiko ved behandlingen, og identifiserer risikoreduserende tiltak. Det er Dataansvarlig som aksepterer risiko.
Tjenesteavtale:	Tjenesteavtale er en fellesbetegnelse på de avtaler som regulerer de kommersielle forhold knyttet til leveransene fra Databehandler, og regulerer blant annet hva som kan bestilles, hvilke krav som kan stilles til leveransen og hvilke prismekanismer som kan legges til grunn. Begrepet innbefatter blant annet vedlikeholdsavtaler, driftsavtaler og service- og supportavtaler.

4 Forholdet mellom Dataansvarlig og Databehandler

Det er kun Dataansvarlig som kan akseptere endring av risiko, og Dataansvarlig må derfor godkjenne bruk av tjenester i henhold til ROS på bakgrunn av utført og behandlet risikovurdering før databehandlingen kan starte.

5 Forholdet mellom Databehandleravtalen og Tjenesteavtalen

Databehandler vil behandle og ha tilgang til Personopplysninger i forbindelse med Tjenesteavtalen med den Dataansvarlige.

Før Behandling kan igangsettes skal det gjøres ROS. ROS inneholder alle relevante krav og informasjon i henhold til personvernloven og relevante særlover, og vil bli oppsummert og oppdatert i Databehandlers til enhver tid gjeldende Protokoll over behandlingsaktiviteter.

5.1 RANGORDNING

Partene er enige om at dersom det er eller oppstår motstrid mellom Tjenesteavtalen og denne Databehandleravtale, skal reguleringen i denne Databehandleravtale vinne frem.

6 Databehandlerens rolle og ansvar

Databehandler har et selvstendig ansvar for å sikre at behandlingen av Personopplysninger er i overenstemmelse med

a) helseregisterloven (20. juni 2014 nr. 43), pasientjournalloven (20. juni 2014 nr. 42 og personopplysningsloven (14. april 2000 nr. 31) og personopplysningsforskriften (15. desember 2000 nr. 1265) og enhver lov og forskrift som erstatter disse, herunder lov som implementerer EUs Personvernforordning 2016/679 (GDPR) i norsk rett, samlet benevnt «*Personvernlovgivningen»*

b) Normen for informasjonssikkerhet[1]

c) Dataansvarliges styringssystem for informasjonssikkerhet[2], og

d) denne Databehandleravtale

De begreper som er definert i gjeldende personopplysningslov av 14. april 2000 nr. 31, §2 og lov som implementerer EUs Personvernforordning 2016/679 (GDPR) artikkel 4 i norsk rett skal ha tilsvarende betydning hvis benyttet i denne Databehandleravtalen.

Databehandler skal videre bidra til å sikre at Dataansvarlig oppnår sitt overordnede formål om å sikre de registrertes rettigheter i henhold til Personvernlovgivningen blant annet ved å

a) gjennomføre nødvendige tekniske og organisatoriske sikkerhetstiltak som angitt i Personvernlovgivningen og følge de krav som følger av denne Databehandleravtalen

b) sikre at Personopplysninger som behandles holdes atskilt fra andre parters data

c) kunne dokumentere system og rutiner for behandling av Personopplysninger, herunder, men ikke begrenset til beskrivelse av rutiner for autorisasjon og bruk, samt tekniske og organisatoriske sikkerhetstiltak

d) på forespørsel kunne fremlegge slik dokumentasjon som nevnt i c), over, for Dataansvarlig, Datatilsynet, Helsetilsynet og øvrige tilsynsmyndigheter

e) uten ugrunnet opphold meddele Dataansvarlig dersom Underdatabehandler har grunn til å tro at den Dataansvarliges instrukser er i strid med Personvernlovgivningen

f) etter forespørsel bistå Dataansvarlig med å håndtere anmodninger fra de registrerte som gjelder deres rettigheter etter Personvernlovgivningen

[1] Norm for informasjonssikkerhet i helse- og omsorgssektoren
[2] Felles regionalt styringssystem for informasjonssikkerhet

g) bistå med vurdering av personvernkonsekvenser i henhold til Personvernlovgivningen dersom det er trolig at en type databehandling vil medføre en høy risiko for de registrertes rettigheter og plikter

h) føre protokoll over sine egne databehandlingsaktiviteter i henhold til Personvernlovgivningen

Databehandlerens bistand i forbindelse med ovennevnte skal faktureres i henhold til Tjenesteavtalen.

7 Krav til Databehandlerens informasjonssikkerhet

7.1 OVERORDNEDE KRAV

Databehandler skal til enhver tid oppfylle de krav til informasjonssikkerhet som følger av Personvernlovgivningen, dataansvarliges styringssystem for informasjonssikkerhet, denne Databehandleravtale samt sikre at all behandling av Personopplysninger som er omfattet av denne Databehandleravtale skjer i henhold til det nivå for akseptabel risiko som er fastsatt av Dataansvarlig.

For å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen skal Databehandler gjennomføre relevante tekniske og organisatoriske tiltak, eksempelvis ved å

a) ha og vise evne til å sikre vedvarende fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssystemene og – tjenestene

b) ha evne til å gjenopprette tilgjengeligheten og tilgangen til Personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse, og

c) ha etablert en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er

7.2 DATABEHANDLERENS TILTAK

Databehandler skal, etter instruks fra Dataansvarlig, utarbeide sikkerhetsmål, - strategi, og –organisering i samsvar med Personvernlovgivningen.

Sikkerhetsbrudd eller mistanke om sikkerhetsbrudd skal umiddelbart rapporteres til dataansvarliges personvernombud.

Databehandler plikter videre å følge opp disse med et tilfredsstillende internkontrollsystem og øvrige planlagte og systematiske tiltak, herunder dokumenterbare prosedyrer for logging av feil, avvik, varsling av avvik og avvikshåndtering.

7.3 KRAV TIL TEKNISK SIKKERHET

Følgende minimumskrav til teknisk sikkerhet skal være implementert, der det er relevant:

a) Kun autoriserte medarbeidere skal ha tilgang til Personopplysninger

b) Tilgang til tjenester og opplysninger i nettverket skal være basert på individuelle brukerkoder og passord.

c) All tilgang til Personopplysninger skal logges

d) Helseopplysninger skal sikres mot uaktsom utlevering. Tekniske tiltak skal være på plass for å forhindre at Personopplysninger kan flyttes ut av sikker sone eller fra godkjent lagringssted

e) Sikkerhet skal ivaretas ved fjerndrift av Dataansvarliges systemer. Det skal benyttes kryptert VPN-forbindelse med sperring mot samtidig tilgang til internett. Utstyr som benyttes i forbindelse med fjerntilgang skal ikke brukes av venner, familie eller andre uautoriserte personer

f) 2-nivå autentisering skal benyttes dersom tilgang til Dataansvarliges systemer skjer via usikre nettverk

g) Kommunikasjon skal sikres med kryptering dersom den går over usikre nettverk

7.4 KRAV TIL ADGANGSKONTROLL

Databehandler skal ha rutiner for tilgangsautorisasjon og -styring som sikrer at bare de av Databehandlerens medarbeidere med et reelt behov for tilgang til systemet og Personopplysningene, har tilgang. Tilgangsnivå skal være i henhold til reelt behov knyttet til å gjennomføre leveransen.

Databehandler skal til enhver tid ha oversikt over eget personell som er autorisert for tilgang til informasjon og tjenester relatert til Tjenesteavtalen. På forespørsel skal slik oversikt forelegges Dataansvarlig.

Dersom Dataansvarlig har innvendinger mot at én eller flere angitte personer har fysisk og/eller elektronisk adgang til systemet, skal autorisasjon for disse inndras.

Databehandler skal ha rutiner og teknisk mulighet til å slette, begrense eller overføre til andre den registrertes opplysninger dersom den registrerte ønsker det med hjemmel i Personvernlovgivningen.

Databehandler skal benytte midlertidige passord eller tilsvarende. Passordene skal kunne endres/sperres umiddelbart, også når behovet for tilgang opphører.

7.5 KRAV TIL FYSISK SIKKERHET

Databehandler skal benytte adgangskontroll med bruk av adgangskort med personlig kode eller tilsvarende.

Tilgang til begrensede områder, eksempelvis drifts- og serverrom, skal være basert på reelt behov.

Personell som ikke er autoriserte, skal følges av en ansatt hos Dataansvarlig.

Adgangskontroll med låste dører skal benyttes for følgende typer lokaler: datahall/serverrom, IT lokaler (drift/support), lokaler med IT relatert utstyr (koblingsmatriser, svitsjer/rutere) mv.

7.6 RISIKOVURDERING VED ENDRINGER I DATABEHANDLINGEN

Enhver endring av databehandlingen hos Databehandler som har eller kan ha betydning for informasjonssikkerheten skal risikovurderes og godkjennes av Dataansvarlig før endring gjennomføres, eventuelt med slike ytterligere tiltak Dataansvarlig har anvist.

8 Varsel og bistand ved avvik

Ved kjennskap til et brudd på personopplysningssikkerheten, herunder for eksempel uautorisert utlevering eller tilgang til personopplysninger, skal Databehandler uten ugrunnet opphold varsle Dataansvarlig og umiddelbart iverksette tiltak for å avhjelpe (lukke) avvikene og begrense skadevirkningene av dem. Dersom det er nødvendig for å avklare hva som har skjedd skal Databehandler samarbeide med Datatilsynet.

Databehandler skal underrette Dataansvarlig dersom en instruks er i strid med personvernregelverket i Norge eller innen EØS-området.

Dataansvarliges personvernombud skal varsles samtidig.

8.1 VARSELETS INNHOLD

Databehandler skal utferdige et varsel for melding av avvik til Dataansvarlig, hvor det kreves beskrevet

a) innsenders org.nr., navn, adresse, postnummer og sted

b) avviket, herunder forklaring av årsak, tidsrom, tidspunktet avviket ble oppdaget, hvor mange som kan være berørt av avviket, hva slags type personopplysninger som ble berørt mv.

c) konsekvenser for de berørte personer, og

d) tiltak som er gjort og planlagt for å forhindre at hendelsen skjer igjen

9 Ansvar for behandlingen

Databehandler er kun ansvarlig for skade forårsaket av Databehandlers behandling, og bare dersom forpliktelsene i personvernregelverket som særlig er rettet mot databehandlere ikke er oppfylt, eller dersom Databehandler har opptrådt utenfor eller i strid med instrukser fra Dataansvarlig.

Dersom Dataansvarlig har vært involvert i behandlingen, har Databehandler rett til å kreve tilbake den delen av en eventuell erstatning som svarer til Dataansvarliges del av ansvaret for skaden.

10 Taushetsplikt

Databehandlerens ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av Personopplysninger i henhold til denne Databehandleravtale er underlagt taushetsplikt.

Taushetsplikten gjelder alle personopplysninger, sikkerhetsmessige og forretningsmessige forhold og opplysninger som kan skade en av Partene eller som kan utnyttes av utenforstående i næringsvirksomhet.

Databehandler skal påse at alle som behandler Personopplysninger er kjent med taushetsplikten og har undertegnet tilfredsstillende taushetserklæring. Ansatte som har tilgang til helseopplysninger skal være pålagt taushetsplikt etter helseregisterloven § 17.

Taushetsplikten gjelder også etter Databehandleravtalens opphør.

Partene plikter å ta nødvendige forholdsregler for å sikre at materiell og opplysninger ikke blir gjort kjent for uvedkommende, og på forespørsel fremlegge dokumentasjon av forholdsreglene.

11 Databehandlerens bruk av underleverandører

Databehandler kan ikke benytte underleverandører til behandling av Personopplysninger, herunder overføre Personopplysninger til slike, uten at følgende er gjennomført:

a) Dataansvarlig har godkjent risikovurderingen
b) Dataansvarlig har skriftlig godkjent bruk av underleverandør
c) Det er inngått separat og skriftlig underdatabehandleravtale med underleverandøren, med tilsvarende krav og forpliktelser som følger av denne Databehandleravtale

Databehandler er ansvarlig for utførelsen av oppgaver hos underleverandører på samme måte som om Databehandleren selv stod for utførelsen av disse. Databehandlers underleverandører skal være bundet av de samme avtalemessige og lovmessige forpliktelser som Databehandler er underlagt i henhold til denne Databehandleravtalen, gjennom egne databehandleravtaler.

Databehandler skal sikre at eventuelle underleverandører er informert om og aktivt påtar seg å følge lovbestemt taushetsplikt.

Dataansvarlig og tilsynsmyndighetene har rett på opplysninger om underleverandør, herunder innhold i databehandleravtale og informasjon om tekniske og organisatoriske tiltak underleverandør har iverksatt for å etterleve personvernregelverket.

12 Overføring

Databehandler kan ikke overføre Personopplysninger til tredjeparter med mindre dette er eksplisitt avtalt med Dataansvarlig.

12.1 OVERFØRING TIL UTLANDET ELLER INTERNASJONALE ORGANISASJONER

Overføring til tredjeland som ikke er godkjent av Europakommisjonen kan kun skje på følgende vilkår:

a) Overføringen kan bare skje i henhold til Personvernlovgivningen
b) Det skal alltid være utført en risikovurdering som skal skriftlig godkjennes av Dataansvarlig før overføringen starter

Databehandler er kjent med at overføring til utlandet utenfor EU/EØS ikke er et statisk begrep knyttet til den geografiske plasseringen for de avtalte tjenesteleveransene i henhold til Tjenesteavtalen, men et dynamisk begrep knyttet til enhver databehandling som utføres i forbindelse med herværende Databehandleravtale.

Forutsatt at Dataansvarlig skriftlig har godkjent overføring til utlandet utenfor EU/EØS må Databehandler sørge for at overføringen

a) skjer på grunnlag av en beslutning om tilstrekkelig beskyttelsesnivå eksempelvis ved bruk at EUs standardkontrakter, eller

b) omfattes av andre former for nødvendige garantier, eller

c) blir omfattet av godkjente bindende konsernregler

13 Innsyn, verifikasjon og revisjon mv.

Dataansvarlig kan til enhver tid kreve innsyn i og verifikasjon av Databehandlers behandling av Personopplysninger for Dataansvarlig, herunder, men ikke begrenset til dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og system for internkontroll.

Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten i tjenesten, herunder, men ikke begrenset til

a) relevant dokumentasjon, herunder testdokumentasjon

b) intervjuer og møter med Databehandlerens ansatte i verifikasjonssammenheng, og

c) dokumentasjon knyttet til sikkerhetsovervåkning av nettverkstrafikk og serveraktivitet

Dataansvarlig skal så vidt mulig gi Databehandler rimelig varsel om krav om innsyn og kontroll, vanligvis med minst 30 dagers varsel. For krav om dokumentinnsyn skal det normalt gis minst 14 dagers varsel. Innsyn og kontroll kan gjennomføres av Dataansvarlig eller av tredjepart.

Databehandler skal gi Datatilsynet og annen relevant tilsynsmyndighet slik tilgang som nevnt over.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik som avdekkes gjennom revisjon og skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

14 Varighet, oppsigelse og opphør

Databehandleravtalen løper fra den er undertegnet og gjelder så lenge Databehandler behandler eller har tilgang til Personopplysninger på vegne av Dataansvarlig. Databehandleravtalen kan revideres ved behov for tilpasninger til preseptorisk lovgivning og tolkninger av GDPR som nødvendiggjør slik revisjon.

Dataansvarlig kan til enhver tid velge å stanse videre behandling, eller kreve endring i behandlingsmåten av Personopplysninger hos Databehandler.

15 Opphør

Når Databehandleravtalen opphører skal Databehandler tilrettelegge for og medvirke til overføring (tilbakelevering) av alle opplysninger som Databehandler behandler på vegne av Dataansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at opplysningene er overført til Dataansvarlig, og det er bekreftet mottak av disse, skal Databehandler slette opplysningene i sitt system. Kravet til sletting omfatter også sikkerhetskopier av Personopplysninger fra perioden etter at regulær behandling opphørte og frem til overlevering er gjennomført.

Databehandler skal gi Dataansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt ovenfor.

Dersom Databehandler har inngått avtale med underleverandør, skal underleverandørens databehandling opphøre senest samtidig med herværende Databehandleravtale, og Databehandler skal sikre at underleverandør oppfyller plikten til sletting mv. på samme måte som Databehandler.

16 Mislighold

Mislighold reguleres fullt ut av Tjenesteavtalens bestemmelser om dette.

17 Tvisteløsning

Tvister løses og reguleres i henhold til Tjenesteavtalens bestemmelser om dette.

18 Undertegning

Denne Databehandleravtale er undertegnet i to eksemplarer, hvorav hver part beholder ett eksemplar.

Sted: _____, den __ /10/2018

_____	_____
Dataansvarlig (signatur)	Databehandler (signatur)
_____	_____
(med trykte bokstaver)	(med trykte bokstaver)
Stilling: AD/Klinikkdirektør____	Stilling: _____