MICROLOG DATABEHANDLERAVTALE

Mellom Microlog AS, org. nr.: 815 469 232, Haugenveien 29, 1423 Ski, Norge (databehandler) og selskap som følger av Avtalen (behandlingsansvarlig) hver omtalt som en «part» eller sammen som «partene». Partene har avtalt de følgende standard kontraktsbestemmelser (Kontraktsbestemmelsene) etter artikkel 28(3) i forordning 2016/679 (GDPR) (som basert på Opinion 14/2019 av Personvernrådet) for å oppfylle kravene i GDPR og for vern av den registrertes rettigheter.

Kontraktsbestemmelsene følger som vedlegg til Avtalen (avtale om bruksrett til programvare og kjøp av tjenester/produkter evt. andre kjøp/vedlikeholdsavtaler for slike tjenester) mellom Databehandler og Behandlingsansvarlig slik dette er beskrevet i Avtalen og inngås ved inngåelse av Avtalen.

1. INNHOLD

Disse vilkårene samt følgende vedlegg

Vedlegg A Information om behandlingen

Vedlegg B Godkjente underdatabehandlere

Vedlegg C Vedlegg D Vurdering av personopplysninger avtalt mellom partene

2. INNLEDNING

1. Disse standard kontraktsbestemmelser (Kontraktsbestemmelsene) regulerer rettigheter og plikter for behandlingsansvarlig og databehandler, når det behandles personopplysninger på vegne av den behandlingsansvarlige.

2. Kontraktsbestemmelsene er utformet for å sikre partenes overholdelse med artikkel 28(3) i Europaparlaments- 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 (generell personvernforordning - GDPR).

3. I forbindelse med leveranse av tjenestene som følger av Avtalen, vil databehandleren behandle personopplysninger på vegne av den behandlingsansvarlige i henhold til Kontraktsbestemmelsene.

4. Kontraktsbestemmelsene skal ha forrang over andre tilsvarende bestemmelser i andre avtaler mellom partene.

5. Fire vedlegg er inntatt i Kontraktsbestemmelsene og anses som omfattet av Kontraktsbestemmelsene.

6. Vedlegg A inneholder detaljer om behandlingen av personopplysninger, herunder behandlingens formål og art, typen personopplysninger, kategorier av registrerte og varigheten av behandlingen.

7. Vedlegg B inneholder den behandlingsansvarliges vilkår for databehandlerens bruk av underdatabehandlere og en liste over underdatabehandlere godkjent av den behandlingsansvarlige.

8. Vedlegg C inneholder den behandlingsansvarliges instrukser for behandlingen av personopplysninger, minimum sikkerhetstiltak som skal implementeres av databehandleren og hvordan revisjoner av databehandleren og eventuelle underdatabehandlere skal gjennomføres.

9. Vedlegg D inneholder regulering av andre aktiviteter som ikke er dekket av Kontraktsbestemmelsene.

10. Kontraktsbestemmelsene sammen med vedleggene skal mottas skriftlig, inkludert elektronisk, av begge parter.

11. Kontraktsbestemmelsene skal ikke frita databehandleren fra plikter som databehandleren skal følge etter personvernforordningen (GDPR) eller annen lovgivning.

3. BEHANDLINGSANSVARLIGES RETTIGHETER OG PLIKTER

1. Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger utføres i samsvar med GDPR (se artikkel 24 i GDPR), personvernreglene i gjeldende EU eller Medlemsstats personvernregler og Kontraktsbestemmelsene.

2. Den behandlingsansvarlige har rett og plikt til å fatte beslutninger om formålene med og midlene for behandlingen av personopplysninger.

3. Den behandlingsansvarlige skal være ansvarlig, for blant annet, å sikre at behandlingen av personopplysninger, som databehandleren er instruert om å utføre, har et rettslig grunnlag.

4. DATABEHANDLEREN SKAL HANDLE ETTER INSTRUKSER

1. Databehandleren skal behandle personopplysninger bare på dokumenterte instrukser fra den behandlingsansvarlige, med mindre det kreves i henhold til unionsretten eller Medlemsstatenes nasjonale rett som databehandleren er underlagt. Slike instrukser skal være spesifisert vedlegg A og C. Senere instrukser kan også gis av den behandlingsansvarlige iløpet av behandlingen av personopplysninger, men slike instrukser skal alltid være dokumenterte og oppbevares i

skriftlig form, herunder elektronisk, i overensstemmelse med Kontraktsbestemmelsene.

2. Databehandleren skal omgående underrette den behandlingsansvarlige dersom vedkommende mener at en instruks gitt av den behandlingsansvarlige er i strid med GDPR eller andre bestemmelser om vern av personopplysninger i unionsretten eller Medlemsstatenes nasjonale rett.

5. KONFIDENSIALITET

1. Databehandleren skal kun gi tilgang til personopplysninger som behandles på vegne av den behandlingsansvarlige til personer som er under databehandlerens myndighet og som er forpliktet til konfidensialitet eller er underlagt egnet lovfestet taushetsplikt og kun som har nødvendig behov for tilgang. Listen over personer som har tilgang til personopplysningene skal regelmessig gjennomgås. Som følge av gjennomgang skal tilgang til personopplysningene bli trukket tilbake dersom slik tilgang ikke lenger er nødvendig til for personene.

2. Databehandleren skal på anmodning fra den behandlingsansvarlige påvise at de involverte personene under databehandlerens myndighet er omfattet av ovennevnte konfidensialitetsplikt.

6. SIKKERHET VED BEHANDLINGEN

1. Artikkel 32 i GDPR angir at, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål av behandlingen og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

Den behandlingsansvarlige skal vurdere risikoen til rettigheter og friheter for fysiske personer som omfattes av behandling og implementere tiltak for å redusere risikoen. Avhengig av relevans, kan slike tiltak omfatte følgende:

a. Pseudonymisering og kryptering av personopplysninger,

b. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,

c. evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,

d. en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

2. I henhold til artikkel 32 i GDPR, skal databehandleren også – uavhengig fra den behandlingsansvarlige – vurdere risikoen til rettigheter og friheter for fysiske personer som omfattes av behandlingen og implementere tiltak for å redusere risikoen. For dette formal skal den behandlingsansvarlige tilveiebringe databehandleren med all informasjon som er nødvendig for å identifisere og vurdere slik risiko.

3. Videre skal databehandleren bistå den behandlingsansvarlige i å sikre overholdelse av den behandlingsansvarliges plikter etter artikkel 32 i GDPR, ved å bl.a. å sørge for at den behandlingsansvarlige får informasjon om tekniske og organisatoriske tiltak som er implementert av databehandleren i henhold til artikkel 32 i GDPR sammen med all annen informasjon som er nødvendig for den behandlingsansvarlige til å overholde dennes plikter under artikkel 32 i GDPR.

Dersom det i ettertid – ved vurderingen foretatt av den behandlingsansvarlige – viser seg at reduksjon av den identifiserte risiko krever implementering av ytterligere tiltak av databehandleren enn de tiltak som allerede er implementert av databehandleren etter artikkel 32 i GDPR, den behandlingsansvarlige skal spesifisere disse ytterligere tiltak som skal implementeres i Vedlegg C.

7. BRUK AV UNDERDATABEHANDLERE

1. Databehandleren skal overholde kravene inntatt i artikkel 28(2) og (4) i GDPR for å engasjere en annen databehandler (en underdatabehandler).

2. Databehandleren skal derfor ikke engasjere annen databehandler (underdatabehandler) for oppfyllelse av Kontraktsbestemmelsene uten at det på forhånd er innhentet generell skriftlig tillatelse fra den behandlingsansvarlige.

3. Databehandleren er gitt generell tillatelse fra den behandlingsansvarlige for å engasjere underdatabehandlere. Databehandleren skal skriftlig underrette den behandlingsansvarlige om eventuelle planer om å benytte andre underdatabehandlere eller skifte ut underdatabehandlere minst fire uker på forhånd, og dermed gi den behandlingsansvarlige muligheten til å motsette seg slike endringer før underdatabehandler(e) engasjeres. Ytterligere tid for underrettelse for spesifikk underdatabehandling kan inntas i Vedlegg B. Liste over underdatabehandlere som allerede er godkjent av den behandlingsansvarlige kan inntas i Vedlegg B.

4. Dersom databehandleren engasjerer en underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal de samme forpliktelsene som er fastsatt i Kontraktsbestemmelsene bli pålagt underdatabehandleren ved avtale eller et annet rettslig dokument i henhold til unionsretten eller Medlemsstatenes nasjonale rett, der

det særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i Kontraktsbe- stemmelsene og GDPR.

Databehandleren skal derfor være ansvarlig for at underdatabehandleren minimum overholder de forpliktelser som databehandleren er pålagt etter Kontraktsbestemmelsene og GDPR.

5. En kopi av slik underdatabehandleravtale og etterfølgende endringer skal – på den behandlingsansvarliges forespørsel – oversendes den behandlingsansvarlige, og dermed gi den behandlingsansvarlige muligheten til å sikre at de samme plikter for behandling av person-opplysninger pålegges underdatabehandleren. Bestemmelser for kommersielle forhold som ikke har betydning for behandling av personopplysninger under underdatabehandleravtalen, er ikke omfattet plikten til oversendelse til den behandlingsansvarlige.

6. Databehandleren skal avtale med underdatabehandleren at – i tilfelle konkurs hos databehandleren – den behandlingsansvarlige skal ha rettigheter som tredjepart under under-databehandleravtalen og skal kunne håndheve rettigheter overfor underdatabehandleren som engasjert av databehandleren, som f.eks. å gi den behandlingsansvarlige rett til å instruere underdatabehandleren til å slette eller tilbakelevere personopplysningene.

7. Dersom underdatabehandleren ikke oppfyller sine forpliktelser for databehandling, skal databehandleren overfor den behandlingsansvarlige ha fullt ansvar for at underdatabehandler oppfyller sine forpliktelser. Dette har ikke betydning for de rettigheter den registrerte har under GDPR – spesielt de rettigheter som er forutsatt i artikkel 79 og 82 i GDPR – overfor den behandlingsansvarlige and databehandleren, inkludert underdatabehandleren.

8. OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJESTATER ELLER INTERNASJONALE ORGANISASJONER

1. Enhver overføring av personopplysninger til tredjestat eller internasjonale organisasjoner av databehandleren skal kun finne sted på grunnlag av dokumenterte instrukser fra den behandlingsansvarlige og skal kun skje i overensstemmelse med kapittel V i GDPR.

2. Dersom overføring til tredjestat eller internasjonale organisasjoner, som databehandleren ikke er blitt instruert til å foreta av den behandlingsansvarlige, som er påkrevet etter unionsretten eller Medlemsstatenes nasjonale rett som databehandleren er underlagt, skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre de rettslige kravene av hensyn til viktige allmenne interesser forbyr en slik underretning.

3. Uten dokumenterte instrukser fra den behandlingsansvarlige, kan databehandleren derfor ikke innenfor disse Kontraktsbestemmelser:

a. overføre personopplysninger til en behandlingsansvarlig eller databehandler i en tredjestat eller en internasjonal organisasjon

b. overføre behandlingen av personopplysninger til en underdatabehandler i en tredjestat

c. la personopplysningene behandles av en databehandler i en tredjestat

4. Den behandlingsansvarliges instrukser vedrørende overføring av personopplysninger til en tredjestat inkludert, hvis relevant, overføringsgrunnlagene etter kapittel V i GDPR som de er basert på, skal inntas i Vedlegg C.6.

5. Kontraktsbestemmelsene skal ikke forstås som standard personvernbestemmelser etter artikkel 46(2)(c) og (d) i GDPR, og Kontraktsbestemmelsene kan benyttes som grunnlag som overføringsgrunnlag etter kapittel V i GDPR.

9. BISTAND TIL DEN BEHANDLINGSANSVARLIGE

1. Hensyntatt arten av behandling, databehandleren skal bistå den behandlingsansvarlige ved hjelp av egnede tekniske og organisatoriske tiltak, i den grad det er mulig, med å oppfylle den behandlingsansvarliges plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i kapittel III i GDPR.

Dette omfatter at databehandleren skal, i den grad det er mulig, bistå den behandlingsansvarlige i den behandlingsansvarliges overholdelse av:

a. Retten til å bli informert ved innsamling av personopplysninger fra den registrerte

b. retten til å bli informert dersom personopplysninger ikke har blitt samlet inn fra den registrerte

c. retten til innsyn av den registrerte

d. retten til retting

e. retten til sletting («retten til å bli glemt»)

f. retten til begrensning av behandling

g. underretningsplikt i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling

h. retten til dataportabilitet

i. retten til å protestere mot å omfattes av automatiserte individuelle avgjørelser, inkludert

profilering

2. I tillegg til databehandlerens plikt til å bistå den behandlingsansvarlige i henhold til punkt 6.3., databehandleren skal videre, hensyntatt arten av behandlingen and informasjon som er tilgjengelig for databehandleren, bistå den behandlingsansvarlige med overholdelse av:

a. Den behandlingsansvarliges plikt uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde brudd på personopplysnings-sikkerheten til vedkommende tilsynsmyndighet, Datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter,

b. den behandlingsansvarliges plikt til å underrette om brudd på personopplysningssikkerheten til den registrerte, om det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter,

c. den behandlingsansvarliges plikt til å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (en vurdering av personvernkonsekvenser),

d. den behandlingsansvarliges plikt til å rådføre seg med vedkommende tilsyns-myndighet, Datatilsynet, før behandling hvor en vurdering av personvern-konsekvensene som tilsier at behandlingen vil medføre en høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.

3. Partene skal angi i Vedlegg C egnede tekniske og organisatoriske tiltak som databehandleren skal bistå den behandlingsansvarlige med i tillegg til omfang og om bistand er påkrevet. Dette gjelder de plikter som er forutsatt i punkt 9.1. og 9.2.

10. MELDING OM BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN

1. I tilfelle brudd på personopplysningssikkerheten, skal databehandleren uten ugrunnet opphold etter å ha fått kjennskap til det, underrette den behandlingsansvarlige om bruddet på personopplysningssikkerheten.

2. Databehandlerens underretning til den behandlingsansvarlige skal, om mulig, skje innen 24 timer etter databehandleren har fått kjennskap til bruddet på personopplysnings-sikkerheten for å overholde den behandlingsansvarliges plikt til å melde bruddet på personopplysningssikkerheten til relevant tilsynsmyndighet, jf. artikkel 33 i GDPR.

3. I henhold til punkt 9(2)(a), databehandleren skal bistå den behandlingsansvarlige i å melde bruddet på personopplysningssikkerheten til vedkommende tilsynsmyndighet, hvilket omfatter at databehandleren skal bistå i å innhente informasjonen nedenfor som, i henhold til artikkel 33(3) i GDPR, skal inntas i den behandlingsansvarliges melding til vedkommende tilsynsmyndighet:

a. Arten av personopplysninger, herunder når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt,

b. de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,

c. de tiltak som er truffet eller foreslått å bli tatt av den behandlingsansvarlige for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger.

4. Partene skal angi i Vedlegg D det databehandleren skal tilveiebringe når denne bistår den behandlingsansvarlige i meldingen av bruddet på personopplysningssikkerheten til tilsynsmyndigheten.

11. SLETTING OG RETUR AV DATA

1. Ved opphør av bestemmelsene om tjenestene knyttet til behandling av personopplysninger, er databehandleren forpliktet til å slette alle personopplysninger som er behandlet på vegne av den behandlingsansvarlige og bekrefte overfor den behandlingsansvarlige at dette er gjort eller tilbakeleverer alle personopplysningene til den behandlingsansvarlige og sletter eksisterende kopier, med mindre unionsretten eller Medlemsstatenes nasjonale rett krever at personopplysningene lagres.

2. Databehandleren påtar seg å kun behandle personopplysninger for det formål og for den varighet som pålegges etter nevnte bestemmelser og kun under de betingelser som bestemmelsene setter.

12. REVISJON OG INSPEKSJONER

1. Databehandleren gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise overholdelse av pliktene som følger av artikkel 28 og Kontraktsbestemmelsene, og tillate og bidra til revisjoner, inkludert inspeksjoner, utført av den behandlingsansvarlige eller annen revisor bemyndiget av den behandlingsansvarlige.

2. Fremgangsmåter for den behandlingsansvarliges revisjoner, inkludert inspeksjoner, av databehand-

leren og underdatabehandlere er regulert nærmere i Vedlegg C.7 and C.8.

3. Databehandleren skal være pålagt å gi tilsynsmyndigheter, som etter relevant lovgivning skal ha tilgang til den behandlingsansvarliges og databehandlers lokaler, eller representanter som handler på vegne av slike tilsynsmyndigheter, tilgang til databehandlerens fysiske lokaler ved fremleggelse av egnet identifikasjon.

13. YTTERLIGERE BESTEMMELSER

Partene kan avtale ytterligere bestemmelser vedrørende behandling av personopplysninger som spesifiserer f.eks. ansvar, så lenge disse ikke er i direkte eller indirekte motstrid med Kontraktsbestemmelsene eller forringer de grunnleggende rettigheter og friheter for registrerte og den beskyttelse som GDPR gir.

14. START OG OPPHØR

1. Kontraktsbestemmelsene skal gjelde de er signert av begge parter.

2. Begge parter skal ha rett til å kreve at Kontraktsbestemmelsene reforhandles dersom det skjer endringer i rettslige forhold eller uventede forhold gir grunn til slik reforhandling.

3. Kontraktsbestemmelsene skal gjelde for så lenge det leveres tjenester knyttet til behandling av personopplysninger fra databehandleren. Så lenge det leveres tjenester for behandling av personopplysninger kan ikke Kontraktsbestemmelsene sies opp dersom ikke andre bestemmelser om behandling av personopplysninger er avtalt mellom partene.

4. Dersom bestemmelser om behandling av personopplysninger sies opp, og person-opplysningene slettes eller tilbakeleveres til den behandlingsansvarlige etter punkt 11.1. og Vedlegg C.4, Kontraktsbestemmelsene kan sies opp med skriftlig varsel fra en av partene til den andre part.

15. SIGNATUR

Kontraktsbestemmelsene inngås som del av Avtalen, og signeres i Avtalen.

16. DEN BEHANDLINGSANSVARLIGES OG DATABEHANDLERS KONTAKTOPPLYSNINGER

1. Partene kan kontakte hverandre ved følgende kontakter/kontaktpunkter:

Partenes kontaktpunkter følger av Avtalen.

2. Partene skal være forpliktet til å fortløpende informere hverandre om endringer i kontakter/kontaktpunkter.

VEDLEGG A INFORMATION OM BEHANDLINGEN

A.1 Formålet med databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlig: Gjennomføre Avtalen, ved at den Behandlingsansvarlige eller dennes representanter kan benytte systemet (programsuite), som eies og forvaltes av Databehandler, og eventuelle tilhørende integrerte systemer – for å kunne føre helse- og legejournaler i.h.h.t. norsk lov. (Det vises her spesielt til oppbevaringsplikt for denne type data / Lagring av data).

Navn på tjeneste	Formålet med behandlingen	Varigheten av behandlingen
INFODOC Plenario (installert hos kunde eller tredjepart etter kundens valg)	Yte konsulenthjelp, eller bistå med support i form av fjernoppkobling/skjermdeling mot den Behandlingsansvarlige på den Behandlingsansvarlige sin forespørsel.	Til formålet er oppnådd
Infodoc i SKY Webmed	Drift og lagring for at kunden skal kunne føre pasientjourna- ler og nødvendige administrative funksjoner knyttet til pasientbehandling.	Så lenge partene har et kontraktsforhold
INFODOC Plenario (i SKY) Webmed	Drift og lagring i INFODOC Plenario for at kunden skal kunne føre pasientjournaler og nødvendige administrative funksjoner knyttet til pasientbehandling.	Så lenge partene har et kontraktsforhold

A.2. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skal i hovedsak relatere seg til (behandlingens gjenstand):

Databehandleravtalen gjelder alltid, herunder, men ikke begrenset til; både for innsamling, registrering, organisering, strukturering, tilpasning eller endring, gjenfinning/backup, sammenstilling, sletting eller tilintetgjøring og utlevering/overføring, som følge av at Databehandleren har ansvar for lagring og drift av systemet.

A.3. Behandlingen omfatter de følgende typer personopplysninger om de registrerte:

A.4. Behandlingen omfatter følgende kategorier registrerte:

Personopplysninger som blir behandlet vil i hovedsak være opplysninger som skal dokumenteres i henhold til pasient- og helseregisterloven. Dette kan eksempelvis inkludere følgende helse- og personopplysninger:

Generelle personopplysninger:

- Navn
- Fødselsnummer

- Bosted
- Pårørende informasjon
- Familiesituasjon
- Timeavtaler
- Frikortstatus og betalingsinformasjon

Helseopplysninger:

- Opplysninger fra konsultasjon med pasient
- Legemiddelliste
- Diagnoseopplysninger
- Funn og tiltak
- Opplysninger fra helseregistre
- Prøvesvar
- Resepter
- Øvrige opplysninger fra konsultasjon med pasient

A.5. Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig kan utføres når Kontraktsbestemmelsene får virkning. Behandlingen har følgende varighet:

Behandlingen vil skje så lenge Avtalen gjelder.

VEDLEGG B GODKJENTE UNDERDATABEHANDLERE

B.1. Godkjente underdatabehandlere

Ved inngåelse av Kontraktsbestemmelsene, den behandlingsansvarlige gir tillatelse til engasjement av følgende underdatabehandlere:

Navn	Dagens Org.nr.	Stedlig plassering	Type behandling
Microsoft Azure	957 485 030	Nederland	Drift / Lagring
Microsoft Azure	957 485 030	Irland	Backup

Den behandlingsansvarlige skal ved inngåelse av Kontraktsbestemmelsene gi tillatelse til bruk av de ovennevnte underdatabehandlere for behandlingen beskrevet for denne. Databehandleren skal ikke ha rett til – uten den behandlingsansvarliges eksplisitte skriftlige tillatelse – å engasjere en underdatabehandler for «annen» behandling enn den som er blitt avtalt eller benytte en annen underdatabehandler til å foreta den beskrevne behandlingen.

VEDLEGG C INSTRUKSER FOR BRUK AV PERSONOPPLYSNINGER

C.1. Omfanget av/instrukser for behandlingen

Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig skal bli utført av databehandleren på følgende måte:

Ingen utover det som følger av Kontraktsbestemmelsene.

C.2. Sikkerhet ved behandlingen Sikkerhetsnivået skal ta hensyn til: At behandlingen omfatter et stort omfang av person-
opplysninger som omfattes av artikkel 9 i GDPR om 'særlige kategorier personopplysninger' som er årsaken til et 'høyere' nivå av sikkerhet bør etableres.

Databehandleren skal heretter ha rett til å ta beslutninger om tekniske og organisatoriske sikkerhetstiltak som skal iverksettes for å sørge for det nødvendige (og avtalte) sikkerhetsnivå.

Ovennevnte omfatter:

Norm for informasjonssikkerhet i helse- og omsorgssektoren: Databehandler skal følge relevante krav i Norm for informasjonssikkerhet (se faktaark 6b, og hvilke krav som er angitt for Databehandler)

Sikring av data: Databehandler skal ha mekanismer for data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet.

Systemadgang: Alle systemer og tjenester hos Databehandleren er sikret med tilgangskontroller som tilfredsstiller gjeldende regelverk og egne risikovurderinger. Herunder bl.a. men ikke begrenset til brukernavn/passord, multifaktor autentisering. Alle data som Databehandleren oppbevarer eller håndterer på vegne av Behandlingsansvarlige sikres for å hindre uautorisert tilgang. Systemene og tjenestene har løsninger for tilgangskontroll slik at Behandlingsansvarlig selv begrense egne brukeres tilganger.

Fysisk sikkerhet: Ved bruk av underleverandører vil Databehandleren gjennom avtaler sikre at kravet til fysisk sikring er tilfredsstillende.

Systemmessig sikkerhet: Databehandleren benytter bare anerkjente underleverandører for våre løsninger. Systemer og tjenester sikres ved regelmessig testing, vurdering og evaluering, der formålet er å sikre konfidensialitet, integritet og tilgjengelighet for leverte systemer og tjenester. Alle data i løsningene er logisk separert på klientnivå for å sikre mot uautorisert tilgang. Alle tjenester og systemer vi drifter overvåkes kontinuerlig, og hendelser håndteres løpende av driftspersonell i henhold til egne prosedyrer og rutiner. Alle data som lagres i våre skyløsninger blir regelmessig sikkerhetskopiert. I tillegg vil egne sikkerhetskopier regelmessig kopieres til en annen sekundær lokasjon.

Systemene og tjenestene har støtte for tilgangsstyring slik at den Behandlingsansvarlige selv kan, og har ansvar for, å administrere hva den enkelte bruker har tilgang til.

For å lese mer om Microsoft sin egen beskrivelse av sikkerhet i datasenteret, se: https://www.microsoft.com/en-

us/trustcenter/privacy/you-own-your-data. C.3. Bistand til den behandlingsansvarlige Databehandleren skal såfremt det er mulig – innenfor omfanget og i den grad bistanden er spesifisert nedenfor – bistå den behandlingsansvarlige i henhold til punkt 9.1 and 9.2 ved å implementere de følgende tekniske og organisatoriske tiltak: Ingen er avtalt uten det som følger av Kontraktsbestemmelsene.

C.4. Fremgangsmåte for lagringstid/sletting

Behandlingen er ikke tidsbegrenset og varer til Avtalen sies opp eller avbrytes av en av partene.

I de tilfeller hvor det er Databehandleren som oppbevarer/lagrer personopplysninger og det ikke er tilgjengeliggjort verktøy for den Behandlingsansvarlige til å selv slette personopplysninger, blir personopplysningene oppbevart av Databehandleren inntil den Behandlingsansvarlige anmoder om å få opplysningene slettet og/eller tilbakelevert.

I de tilfeller hvor det er Databehandleren som oppbevarer/lagrer personopplysninger og det er tilgjengeliggjort verktøy for den Behandlingsansvarlige til selv å hente eller slette personopplysninger, blir personopplysningene oppbevart av Databehandleren inntil den Behandlingsansvarlige selv har hentet og/eller slettet disse.

I de tilfeller hvor Databehandleren ikke oppbevarer/lagrer personopplysninger er den Behandlingsansvarlige selv ansvarlig for oppbevaring og sletting av slike opplysninger.

I de tilfeller hvor Databehandleren oppbevarer midlertidige kopier, f.eks. i form av backup tilsendt for hjelp/support skal disse slettes så snart som mulig etter at behovet for slike data er borte, og senest innen 10 dager, og uansett på anmodning fra den Behandlingsansvarlige.

Databehandler vil foreta sletting i tråd med det ovenforstående med mindre ufravikelige rettsregler krever at personopplysningene fortsatt lagres.

C.5. Behandlingssted

Behandling av personopplysninger etter Kontraktsbestemmelsene skal ikke utføres på andre lokasjoner enn de følgende uten at det foreligger skriftlig forhåndssamtykke fra den behandlingsansvarlige:

Behandling av de i Databehandleravtalen omfattede personopplysninger kan ikke uten den Behandlingsansvarliges aksept skje på andre enn følgende steder:

- Norge
- Andre Lokasjoner - Av andre underleverandører, som angitt i punkt B.1.

C.6. Instrukser for overføring av personopplysninger tredjestat

Databehandleren kan overføre de personopplysningene Databehandleren behandler på vegne av den Behandlingsansvarlige til de land der Databehandleren og underleverandørene driver sin virksomhet og lagre dem her.

Den Behandlingsansvarlige er kjent med dette og godtar denne overføringen så lenge den er nødvendig for å gjennomføre de avtalte leveransene.

Den Behandlingsansvarlige godtar at Personopplysningene kan behandles utenfor Norge. Databehandler skal likevel ikke overføre personopplysninger til land utenfor EU/EØS-området uten et samtykke fra den Behandlingsansvarlige. Dersom den Behandlingsansvarlige godtar en slik overføring, skal Databehandleren sørge for at overføring skjer basert på godkjente overføringsgrunnlag, jfr. GDPR artikkel 44-46.

Databehandleren gis med dette rett til å inngå EUs standard kontraktsbestemmelser for overføring til tredjestater på vegne av Behandlingsansvarlig.

Dersom den behandlingsansvarlige verken i Kontraktsbestemmelsene eller i det etterfølgende gir dokumenterte instrukser vedrørende overføring av personopplysninger til en tredjestat, skal databehandleren ikke ha rett til å overføre personopplysninger til tredjestat innenfor rammene av Kontraktsbestemmelsene.

C.7. Fremgangsmåte for den behandlingsansvarliges revisjoner, inkludert inspeksjoner, av behandlingen av personopplysninger som utføres av databehandleren

Den behandlingsansvarlig kan gjennomføre inspeksjoner som beskrevet i Kontraktsbestemmelsene. Den behandlingsansvarliges kostnader, hvis aktuelt, knyttet til fysisk inspeksjon skal dekkes av den behandlingsansvarlige. Databehandleren skal imidlertid, være forpliktet til å bistå med ressurser (hovedsakelig tid) påkrevet for den behandlingsansvarlige til å gjennomføre inspeksjonen.

VEDLEGG D YTTERLIGERE BESTEMMELSER AVTALT MELLOM PARTENE

D.1 Databehandleravtalen omfatter også behandling etter:

- Lov om helseregistre og behandling av helseregistre Lov av 20. juni 2014 nr. 43 (helseregisterloven)
- Lov om behandling av helseopplysninger ved ytelse av helsehjelp av 20.juni 2014 nr. 42 (pasientjournalloven) og
- Enhver lov, forskrift eller annet regelverk som erstatter disse.

D.2 Vederlag for bistand til den Behandlingsansvarlige, eller dennes representanter

Generelt så vil Databehandler kunne fakturere timepris for medgått tid til bistand som beskrevet i denne avtales punkt: «Bistand til den Behandlingsansvarlige», samt eventuell annen bistand relatert til personlovgivningen, med den til enhver tid gjeldende timepris for konsulentbistand.

D.3 Vederlag for verktøy/funksjonalitet

Databehandler tilbyr i dag og vil kunne tilby spesielle verktøy eller funksjonalitet for at den Behandlingsansvarlige selv på en enkel måte settes i stand til å utføre operasjoner som kreves eller ønskes, etter den til en- hver tid gjeldende helse- og personvernlovgivning. Databehandler vil kunne kreve vederlag for å gi tilgang til slikt verktøy/funksjonalitet, for å dekke inn eventuel- le kostnader med utvikling og vedlikehold av dette.

D.4 Bruk av personopplysninger til egne formål

Databehandler får tilgang til brukernes programmessige bruksmønster via brukernes bruk av programmene/tjenestene. Databehandler benytter og Behandlingsansvarlig samtykker til at Databehandler kan benytte slike personopplysninger til å forbedre og utvikle kvaliteten, funksjonalitet og brukeropplevelsen av Databehandler sine produkter og tjenester. Databehandler bruker disse personopplysningene, dvs. brukernes programmessige bruksmønster til egne formål og er da Behandlingsansvarlig for denne bruken. Det presiseres at dette gjelder kun brukernes programmessige bruksmønster og ikke pasienters helse- eller personopplysninger. Databehandler vil derfor være hovedansvarlig for denne bruken og Kunden vil ikke ha ansvar for at personvernreglene blir fulgt ved denne behandlingen. Dette innebærer blant annet at Databehandler bl.a. er selv ansvarlig for at det foreligger et behandlingsgrunnlag for denne behandlingen og for at de aktuelle registrerte blir informert om behandlingen.