DATABEHANDLERAVTALE

mellom

OSLO UNIVERSITETSSYKEHUS HF

heretter benevnt "*Dataansvarlig*"

og

XXX

(Org.nr.: XXX)

heretter benevnt "*Databehandler*"

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

Innholdsfortegnelse

1 Innledning

Denne databehandleravtalen omfatter behandling av Personopplysninger på vegne av Oslo universitetssykehus som Dataansvarlig. Avtalen benyttes for tjenester etablert i nettverket til den Dataansvarlige når avtaleforholdet skal reguleres direkte mellom Dataansvarlig og Databehandleren i forbindelse med inngått tjenesteavtale/SLA, og uten at Sykehuspartner HF er en avtalepart.

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

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 behandles

- i samsvar med kravene i det til enhver tid gjeldende Personvernregelverket,
- i henhold til denne Databehandleravtalen, og
- i henhold til formelle, dokumenterte instruksjoner fra Dataansvarlig.

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

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. All annen gjeldende norsk lov og forskrift som regulerer Databehandlers behandling av personopplysninger, herunder lov som implementerer og gjennomfører GDPR, samt sektorlovgivning.
Personopplysning:	Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»), jf. GDPR art. 4 (1)
Særlige kategorier av personopplysninger	Tidligere kalt sensitive personopplysninger. Jf. personvernforordningens artikkel 9 nr. 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:	Den som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. GDPR art. 4 (7)
Databehandler:	Den som behandler personopplysninger på vegne av den Dataansvarlige, jf. GDPR art. 4 (8)
ROS:	ROS er forkortelse for risikovurdering. I ROS er det spesifikt angitt og beskrevet hva Dataansvarlig har bestilt av konkrete driftstjenester fra Databehandler, eksempelvis programvare eller hardware, og hvilke personopplysninger som blir behandlet. ROS inneholder også alle relevante informasjon i henhold til GDPR.
Tjenesteavtalen:	Tjenesteavtalen 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.
Tredjeland eller internasjonal organisasjon:	Overføring av Personopplysninger som Behandles eller skal Behandles etter overføring til en tredjeland eller til en internasjonal organisasjon som ikke sikrer et tilstrekkelig beskyttelsesnivå uten at det foreligger et overføringsgrunnlag, for eksempel land utenfor EØS-området.
Underleverandør:	Fysisk eller juridisk person som Underdatabehandler engasjerer, intensjonelt eller ikke, for å utføre Behandling av Personopplysninger
Regionalt styringssystem for informasjonssikkerhet:	Helse Sør-Østs felles styringssystem for informasjonssikkerhet sikrer at regionen samlet etterlever gjeldende krav til informasjonssikkerhet ved innsamling, registrering, behandling, lagring, utlevering og avslutning av personopplysninger, inkludert kodede/avidentifiserte opplysninger. Videre gjelder styringssystem for informasjonssikkerhet uavhengig av hvordan opplysningene teknisk er samlet inn og omfatter dermed også innsamling av personopplysninger ved bruk av medisinsk teknisk utstyr (MTU), og andre måter å samle inn opplysningene på. Dette omfatter bruk av personopplysninger med grunnlag i pasientjournalloven, helseregisterloven, helseforskningsloven, personopplysningsloven med flere, hvor personopplysningsloven gir sentrale føringer for informasjonssikkerhet.
Brudd på personopplysningssikkerheten:	Et Brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte Behandlet. Slikt Brudd på Personopplysningssikkerheten er ikke avhengig av at det har skjedd et brudd på Personvernregelverket, jf. GDPR art. 4 (12).

4 Databehandlers Behandling av Personopplysninger

4.1 Behandlingsgrunnlag

Det er Dataansvarlig som har ansvar for å angi behandlingsgrunnlaget.

Behandlingsgrunnlag
☐ Lovhjemmel
☐ Samtykke
☐ Kontrakt
☒ Annet, spesifiser: Installasjon, drift, vedlikehold og feilretting av medisinsk utstyr

4.2 Behandlingens formål og art

Databehandler vil behandle og ha tilgang til Personopplysninger i forbindelse med avtalte tjenesteleveranser i tilknytning til det medisinske utstyret Databehandler har levert til Dataansvarlig. Tjenesteleveransen er nærmere beskrevet i den/de Tjenesteavtaler (serviceavtale, kjøpsavtale) Dataansvarlig har inngått med Databehandler.

Behandlingens formål og art
Formålet med Behandlingen er å gi Databehandler mulighet til å levere nødvendige teknisk tjenester i tilknytning til det medisinske utstyret Databehandler har levert til Dataansvarlig. Omfanget av tekniske tjenester er beskrevet i Tjenesteavtalen(e) (ofte kalt serviceavtale) mellom Dataansvarlig og Databehandler. De tekniske tjenestene er typisk forebyggende vedlikehold, feilsøking og reparasjon, SW-vedlikehold, SW-installasjon og applikasjonssupport i tilknytning til det leverte medisinske utstyret. I forbindelse med oppfyllelsen av Databehandleravtalen vil Databehandler kunne foreta Behandlinger i form av tilgang, organisering, strukturering, tilpasning, gjenfinning, konvertering, lagring, flytting, konsultering og tilintetgjøring. Slik Behandling vil kun foregå i henhold til bestemmelsene i Tjenesteavtalen, og kun etter formelle, dokumenterte instruksjoner fra Dataansvarlig. Databehandler kan få tilgang til Personopplysninger ved følgende tilfeller i tilknytning til leveranse av de tekniske tjenester som angitt i Tjenesteavtalen(e):

Fysisk oppmøte:

- Behandlingen vil foregå ved at teknisk ressurs hos Databehandler møter opp fysisk hos Dataansvarlig, og der får tilgang til Personopplysninger fra det medisinske utstyret.

Fjerntilgang:

- I gitte tilfeller vil behandlingen kunne foregå ved at autoriserte tekniske ressurser hos Databehandler får fjerntilgang til det medisinske utstyret via Dataansvarliges til enhver tid godkjent løsning for fjerntilgang, hvor identifiserbare tekniske ressurser fra Databehandler kan gis tilgang til aktuelt medisinsk utstyr via Dataansvarlig sitt nettverk.
- Databehandler må innføre rutine for å kontinuerlig vurdere behov for tilgang til Fjernaksess til sine modaliteter ved OUS, med tilhørende instruks om å informere Dataansvarlig uten ugrunnet opphold hvis noen av deres ansatte ikke lenger trenger denne tilgangen.

Uttak av teknisk logg-fil:

- Det vil forekomme tilfeller der det er behov for teknisk ekspert-support fra Databehandler til å utføre feildiagnostisering vha. tekniske logg-filer fra det medisinske utstyret. I disse tilfeller kan det være aktuelt å hente ut tekniske logg-filer fra det medisinske utstyret som da overføres til Databehandler for avansert teknisk analyse og feilsøking.
- Dersom en teknisk logg-fil er av en type som inneholder sensitiv personinformasjon skal overføring av denne type logg-fil godkjennes av bemyndiget person hos Dataansvarlig.
- Dersom en teknisk logg-fil lagres hos Databehandler skal denne lagres på sikkert medium med adgangskontroll, og ikke være tilgjengelig for-, behandles av- eller overføres til personell utenfor godkjent geografisk område definert i pkt. 4.4.
- Tekniske loggfiler overført til Databehandler skal uten ugrunnet opphold slettes når teknisk analyse av logg-filen er utført, og lagringstid for tekniske logg-filer med sensitiv personverninformasjon skal maksimum lagres i 30 dager på dertil egnet og sikret sted hos Databehandler dersom ikke annet er spesifikt avtalt mellom Databehandler og Dataansvarlig.

Databehandler skal ikke Behandle Personopplysninger i større omfang enn det som er nødvendig for å oppfylle Databehandleravtalen. Annen Behandling kan kun skje unntaksvis og ved kortvarige tilfeller, og kun etter formelle, dokumenterte instruksjoner fra Dataansvarlig.

Dersom Databehandler er i tvil om Behandlingen av enkelte Personopplysninger er nødvendig, eller innenfor Databehandleravtalens omfang, skal det straks, og før Behandlingen starter, konsulteres med Dataansvarlig.

Under ingen omstendigheter er Databehandler berettiget til å Behandle Personopplysninger eller andre data som tilhører Dataansvarlig for egne formål, og utover de formål som fremkommer av Databehandleravtalen eller Tjenesteavtalen.

Dersom Databehandler er pålagt mer omfattende Behandling gjennom lov eller tilsvarende pålegg fra offentlig myndighet forplikter Databehandler seg til å varsle Datansvarlig, samt sikre videre konfidensialitet og sikkerhet i henhold til Databehandleravtalen.

4.3 Kategorier av Personopplysninger og datasubjekter

I forbindelse med oppfyllelse av Tjenesteavtalen, vil Databehandler Behandle følgende Personopplysninger:

I tilknytning til leveransen av tjenester som angitt i Tjenesteavtalen, kan Databehandler få tilgang til Personopplysninger. Dette kan være navn (på pasienter og ansatte), fødselsnummer, telefonnummer, e-postadresse og type undersøkelse. I tillegg kan Databehandler, spesielt tekniske ressurser hos Databehandler som utfører tekniske tjenester i Dataansvarlig sine lokaler, få tilgang til kategorier av personopplysninger som klinisk informasjon om pasienter (diagnose, medisinske data, bilder o.l.).

Personopplysningen vil gjelde følgende type personer;
☒ Ansatt
☐ Leverandør
☒ Pasient
☐ Pårørende
☒ Tidligere ansatt
☐ Innleide konsulenter
☐ Andre, spesifiser:

4.4 Området for Behandlingen

Databehandler skal kun Behandle Personopplysninger innenfor det geografiske området som følger av Tjenesteavtalen, eller det som er avtalt mellom Partene for øvrig.

Eventuell overførsel skal møte de krav til sikkerhet og vern av de registrertes rettigheter som følger av Databehandleravtalen og i henhold til Personvernregelverket.

Område for behandling
Norge: JA

EU/EØS-land, hvilke: **JA, alle EU/EØS-land.**

Tredjeland som er godkjent av Europakommisjonen: **JA, Storbritannia.**

Andre land: **NEI.**

4.5 Behandlingens varighet

Behandlingen er ikke tidsbegrenset og varer inntil avtalen sies opp av en av partene.

5 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.

6 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 GDPR, og vil bli oppsummert og oppdatert i Databehandlers til enhver tid gjeldende oversikt.

6.1 Rangordning

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

7 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 enhver lov og forskrift som erstatter disse, herunder lov som implementerer EUs Personvernforordning 2016/679 (GDPR) i norsk rett, samlet benevnt «*Personvernlovgivningen»*

b) Normen[1]

c) regionalt[2] og internt[3] styringssystem for informasjonssikkerhet, og

d) denne Databehandleravtale

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

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) umiddelbart varsle Databehandler hvis en instruksjon er i strid med Personvernregelverket.

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

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.

8 Krav til Databehandlerens informasjonssikkerhet

8.1 Overordnede krav

Databehandler skal til enhver tid oppfylle de krav til informasjonssikkerhet som følger av Personvernlovgivningen, denne Databehandleravtale, regionalt- og internt styringssystem for informasjonssikkerhet, og 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

d) forhindre at datasystemer som Behandler Personopplysninger blir brukt eller gir tilgang til Personopplysninger til personer som ikke er autorisert, inkludert tilgang til å lese, kopiere, endre eller slette Personopplysninger uten autorisasjon.

e) sikre at all tilgang og bruk av systemet hendelsesregistreres i tråd med Personvernregelverket herunder også krav til hendelsesregistrering ved fjernaksess.

f) pseudonymisere og kryptere Personopplysninger, herunder kryptere datakommunikasjon som inneholder særlige kategorier av personopplysninger, herunder blant annet helse- og personopplysninger, i henhold til gjeldende regelverk dersom slike for eksempel skal overføres til eksterne nettverk.

8.2 Databehandlerens tiltak

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

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.

8.3 Krav til teknisk sikkerhet

Det følger av regionalt styringssystem for informasjonssikkerhet at følgende minimumskrav til teknisk sikkerhet skal være implementert, der det er relevant:

a) Kun autoriserte medarbeidere skal ha tilgang til Personopplysninger, og tilgang til tjenester og opplysninger i nettverket skal være basert på individuelle brukerkoder og passord.

b) All tilgang til Personopplysninger skal logges

c) 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

d) 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

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

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

8.4 Krav til adgangskontroll

Databehandler skal ha rutiner for tilgangsautorisasjon og -styring som sikrer at bare de av Databehandlerens medarbeidere som 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 en 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 overfør til andre en registrerts 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.

8.5 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.

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.

8.6 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.

9 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 også varsles samtidig.

9.1 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

10 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.

10.1 Vesentlig mislighold

Ved vesentlig mislighold kan Databehandleravtalen heves med umiddelbar virkning.

Følgende skal alltid regnes som vesentlig mislighold:

a) Avvik eller svikt i informasjonssikkerhet som medfører at Personopplysninger kommer på avveie eller uberettigede i hende hos tredjepart, korrumperes eller på annen måte beskadiges.
b) Manglende etterlevelse av sikkerhets- og informasjonskrav, samt uttrykkelige instrukser gitt i henhold til denne Underdatabehandleravtale.
c) Overføring av person- eller helseopplysninger til tredjepart uten uttrykkelig avtale.
d) Manglende lukking av definerte avvik i Underdatabehandlers informasjonssikkerhet.

11 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 konfidensielle opplysninger, noens personlige forhold, 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.

12 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.

13 Overføring

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

13.1 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

14 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.

15 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.

16 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 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.

Dersom det foreligger lovpålagt videre Behandling av Personopplysninger etter at Databehandleravtalen er opphørt, er Databehandler forpliktet til å Behandle disse Personopplysningene kostnadsfritt.

17 Mislighold

Mislighold reguleres fullt ut av Tjenesteavtalens bestemmelser om dette.

18 Tvisteløsning

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

19 Undertegning

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

Sted: _____, den _____/_____/_____.

_____	_____
Dataansvarlig (signatur)	Databehandler (signatur)
_____	_____
(med trykte bokstaver)	(med trykte bokstaver)
Stilling: _____	Stilling: _____