Mal:

Databehandleravtale

i henhold til personopplysningsloven og EU personvernforordning 2016/679

om behandling av person- og helseopplysninger

mellom

Databehandlingsansvarlig, org.nr. ... ...
(" databehandlingsansvarlige")

og

Databehandler, org. nr. ... ...
("databehandler")

NB!

Tekst i klammeparentes markert med gul mark-up må erstattes med det som gjelder for den aktuelle avtalen – denne røde teksten fjernes.

1. Avtalens bakgrunn og formål

Denne avtalen gjelder for tjenesteoppdrag som omfatter behandling av person- og helseopplysninger som er tilgjengelig på utstyr og/eller løsning som eies, leies eller på annen måte disponeres av den behandlingsansvarlige/dataansvarlige. Avtalen skal regulere rettigheter og plikter mellom behandlingsansvarlig/dataansvarlig og databehandler.

Formålet er å regulere hvordan databehandleren skal behandle person- og helseopplysninger på vegne av den behandlingsansvarlige/dataansvarlig, jf. personopplysningsloven§ 1, jf. personvernforordningen art 28 nr. 3.

Avtalen skal videre sikre at partene ivaretar tilfredsstillende informasjonssikkerhet og ivaretar vern av den registrertes rettigheter.

Avtalen skal sikre at opplysningene ikke brukes urettmessig og at konfidensialitet, integritet -, tilgjengelighet og robusthet ivaretas i behandlingssystemene under oppdraget.

2. Forholdet til andre avtaler

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten ("Normen") er bindende for databehandler som omhandler helseopplysninger (Dette avsnittet strykes dersom det ikke skal behandles helseopplysninger).

Denne avtalen supplerer andre avtaler som er inngått mellom partene, for eksempel kjøps- og leieavtaler, tjenestenivåavtaler (SLA), serviceavtaler, oppdragsavtaler og avtale om tilgang til utstyr.

I tilfelle konflikt mellom denne avtalen og avtaler som nevnt i avsnitt ovenfor, skal denne avtalen gjelde når det gjelder behandling av personopplysninger.

3. Tilgang til person- og helseopplysninger

Databehandleren gis tilgang til person- og helseopplysninger enten ved personlig oppmøte og bruk av utstyret til den databehandlingsansvarlige eller ved fjerntilgang. I begge tilfeller gjelder tilgangen for et spesifisert databehandleroppdrag. Tilgangen skal ikke benyttes til andre formål.

Helse Vest IKT AS er ansvarlig for etablering og drift av fjerntilgang over datanettverket. Leverandøren skal følge de krav Helse Vest IKT AS stiller til brukere av fjerntilgang.

4. Omfang for behandling av person- og helseopplysninger

Tjeneste-/oppdragsavtalen (sett inn navn) innebærer at databehandler behandler personopplysninger på vegne av behandlingsansvarlig/dataansvarlig. I vedlegg 1 til denne avtalen fremkommer det nærmere hva selve behandlingen som databehandler gjør på vegne av behandlingsansvarlig/dataansvarlig.

Personopplysninger skal kun benyttes til de formålene som følger av denne avtalen, Tjeneste/oppdragsavtalen og senere skriftlige avtaler mellom partene i den utstrekning det er strengt nødvendig for å gjennomføre og imøtekomme kravene i avtalene.

Formålet med og varigheten av behandlingen er nærmere beskrevet i vedlegg 1. Videre beskrives selve behandlingen som utføres, hvilke helse- og personopplysninger som skal behandles, kategorier av de registrerte og behandlingens art i vedlegg 1. Eventuelt senere endringer skal fremgå av vedlegg 1.

Databehandleren skal ikke behandle person- og helseopplysninger på annen måte enn det som er avtalt skriftlig med den databehandlingsansvarlige.

Databehandler kan ikke benytte tredjepart (underleverandører) i sin behandling av personopplysninger for Databehandlingsansvarlig, uten at dette på forhånd er skriftlig avtalt med Databehandlingsansvarlig. Dersom tredjepart engasjeres, er Databehandler ansvarlig for utførelsen på samme måte som om han selv stod for utførelsen.

5. Rammen for behandling av helse- og personopplysninger

Behandlingsansvarlig har til enhver tid full rådighet over de helse- og personopplysningene som Databehandler har anledning til å behandle etter denne Avtalen. Databehandler har ikke selvstendig råderett over helse- og personopplysningene, og kan ikke behandle disse til egne formål.

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i helse- og personopplysningene som behandles hos Databehandleren.

6. Behandlingsansvarliges/dataansvarliges plikter

Behandlingsansvarlig skal etterleve de forpliktelser som fremkommer av personopplysningsloven, personvernforordningen, relevant helselovgivning og annen særlovgivning, samt denne avtalen.

7. Databehandlers plikter

7.1 Generelt

Databehandler forplikter seg til å behandle helse- og personopplysninger kun i samsvar med all relevant lov og regelverk, denne Avtalen, Tjeneste/oppdragsavtalen, Behandlingsansvarliges dokumenterte instruksjoner og andre gjeldende avtaler mellom partene, samt "Normen". Databehandler skal ikke ved noen handling eller unnlatelse, sette Behandlingsansvarlig i en slik situasjon at Behandlingsansvarlig bryter noen bestemmelse i gjeldende lov og regelverk.

Databehandler skal ikke:

a. behandle helse- og personopplysninger for andre formål eller i større grad enn det som følger av denne Avtalen med vedlegg;
b. behandle helse- og personopplysninger utover det som er nødvendig for å oppfylle Databehandlers forpliktelser i henhold til de til enhver tid gjeldende avtaler;
c. utlevere, overlate eller overføre helse- og personopplysninger i noen form på eget initiativ med mindre det er avtalt på forhånd med Behandlingsansvarlig eller Behandlingsansvarlig har godkjent dette skriftlig;
d. samle inn fra eller overføre helse- og personopplysninger til en tredjepart;
e. behandle helse- og personopplysninger de får tilgang eller adgang til gjennom oppdraget fra Behandlingsansvarlig på annen måte enn hva som er angitt i denne Avtalen med vedlegg.

Databehandler skal:

a. ha løpende kontroll på alle kategorier av behandlingsaktiviteter utført på vegne av Behandlingsansvarlig;
b. gi Behandlingsansvarlig tilgang til og innsyn i helse- og personopplysninger som behandles hos Databehandleren;
c. føre og vedlikehold en oversikt over alle opplysninger og behandlinger eller dersom det er relevant, protokoll over sine egne behandlingsaktiviteter i henhold til personvernforordningen artikkel 30;
d. treffe alle rimelige tiltak for å sikre at helse- og personopplysningene til enhver tid er korrekte og oppdaterte;
e. etablere rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen og slette informasjon i henhold til fastsatte rutiner og retningslinjer fra den behandlingsansvarlige/dataansvarlige;
f. ha rutiner for og teknisk mulighet til å begrense behandlingen av den registrertes helse- og personopplysninger dersom den registrerte ønsker det med hjemmel i gjeldende lovgivning;
g. påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Behandlingsansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;
h. sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Databehandlers løsninger. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter;
i. gi Behandlingsansvarlig nødvendig bistand slik at Behandlingsansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;
j. samarbeide med og bistå Behandlingsansvarlig ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger fra den registrerte med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III;

k. omgående underrette den Behandlingsansvarlige dersom Databehandler mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;

l. bistå Behandlingsansvarlig for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet.

7.2 Tekniske, organisatoriske og sikkerhetsmessige tiltak

Databehandler plikter å treffe og gjennomføre alle nødvendige og adekvate planlagte og systematiske tekniske, organisatoriske og sikkerhetsmessige tiltak slik at det til enhver tid er tilfredsstillende informasjonssikkerhet ved behandling av helse- og personopplysninger.

Databehandleren skal:

a. etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av helse- og personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personopplysningslovgivningens bestemmelser, herunder kravene etter personvernforordningen artikkel 32, og gjeldende helselovgivning. Dette omfatter blant annet, alt etter hva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til eller spredning av data så vel som enhver annen bruk av helse- og personopplysninger som ikke er i overensstemmelse med denne Avtalen, og tiltak for å gjenopprette tilgjengelighet og tilgang til opplysningene ved hendelser;

b. ha gode og hensiktsmessige internkontrollrutiner;

c. ha rutiner for autorisasjon og styring som sikrer at bare de av Databehandlers medarbeidere som har reelt behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for gjennomføring av Tjeneste/oppdragsavtalen får slik tilgang. Tilgangsnivået skal være i henhold til reelt behov knyttet til å gjennomføre oppdraget;

d. etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten og følge opp avvik, som skal omfatte blant annet rutiner for avviksmelding, gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentakelse. På forespørsel, skal Databehandler gi Behandlingsansvarlig tilgang til relevant sikkerhetsdokumentasjon og systemene som benyttes for behandling av helse- og personopplysninger;

e. avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på opplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos Databehandler;

f. ved mistanke om eller konstatering av avvik, omgående varsle Behandlingsansvarlig. I varselet opplyses avviket med forklaring om årsak, tidsrom og tidspunktet avviket ble oppdaget, kategoriene av og omtrentlig antall registrerte som er berørt, kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt, navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes, antatte konsekvenser av avviket og hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt for å håndtere avviket;

g. dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;

h. omgående varsle Behandlingsansvarlig ved uautorisert utlevering av personopplysninger;

i. registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som gjøres skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos Databehandler, underleverandører og Behandlingsansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det Tjeneste/oppdragsavtalen spesifiserer;

j. bistå Behandlingsansvarlig med å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 32–34, dvs:
   - sikkerhet ved behandlingen;
   - melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten;
   - underretning av den registrerte om brudd på personopplysningssikkerheten;

k. i forbindelse med sikkerhetsrevisjon som utføres av Behandlingsansvarlig eller en tredjepart utpekt av Behandlingsansvarlig, framlegge interne revisjonsrapporter, interne prosedyrer, rutiner,

sikkerhetsarkitektur, risiko og sårbarhetsanalyser med tiltak og andre dokumenter av betydning for revisjonen;

l. varsle Behandlingsansvarlig om alle forhold som medfører endring i risikobildet;

m. innhente godkjenning av Behandlingsansvarlig før gjennomføring av enhver endring av databehandlingen hos Databehandler som har eller kan ha betydning for informasjonssikkerheten.

Nærmere krav til Databehandlerens informasjonssikkerhet er angitt i **Vedlegg 2** (hvis relevant).

Ved brudd på denne avtalen eller på bestemmelsene i personopplysningslovgivningen, helselovgivningen eller annen relevant lovgivning kan Behandlingsansvarlig kreve endringer i behandlingsmåten eller pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandler skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for Behandlingsansvarlig.

8. Bruk av underleverandør

Behandlingsansvarlig tillater at Databehandler benytter underleverandører for oppfyllelse av forpliktelsene under Avtalen. Databehandler benytter underleverandører som angitt i **Vedlegg 3** for de der angitte tjenester og bekrefter at det er ingen andre underleverandører som benyttes.

Databehandler skal:

a. sikre at underleverandøren påtar seg tilsvarende forpliktelser som Databehandler under Avtalen og gjeldende lovgivning;

b. sørge for at underleverandører kun behandler personopplysninger i samsvar med denne Avtalen og ikke i større utstrekning enn det som er nødvendig for å oppfylle den aktuelle tjenesten som underleverandøren leverer;

c. holde en oppdatert liste over identiteten og stedlig plassering av underleverandører som angitt i **Vedlegg 3**. Oppdatert liste skal være tilgjengelig for Behandlingsansvarlig;

d. gjennomføre en risikovurdering av bruk av underleverandør og betydningen for tjenesten før det inngås avtale med underleverandør og på Behandlingsansvarliges forespørsel, dele vurderingen med Behandlingsansvarlig;

e. på Behandlingsansvarliges forespørsel, legge frem kopi av avtalen(e) som er inngått med underleverandørene (med unntak av merkantile betingelser). Slike avtaler skal senest være inngått før underleverandørene starter med behandling av helse- og personopplysninger;

f. underrette Behandlingsansvarlig om eventuelle planer om å benytte andre underleverandører eller skifte ut underleverandører. Slike bytter skal varsles i god tid slik at Behandlingsansvarlig gis mulighet til å motsette seg endringen. Ved bytte av underleverandør skal **Vedlegg 3** oppdateres og oversendes Behandlingsansvarliges kontaktperson;

g. sikre at Behandlingsansvarlig og tilsynsmyndighetene har samme rett til innsyn og kontroll med behandling av personopplysninger hos en underleverandør som Behandlingsansvarlig har overfor Databehandler etter Avtalens punkt 11;

h. ved opphør av Avtalen, sikre at underleverandører oppfyller plikten til å slette eller forsvarlig destruere alle helse- og personopplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene som framgår av Avtalens punkt 12 på samme måte som Databehandler så langt det ikke strider mot andre lovbestemmelser.

Databehandler er til enhver tid fullt ut ansvarlig overfor Behandlingsansvarlig for alt arbeid som utføres av underleverandører og for underleverandørenes etterlevelse av bestemmelsene i denne Avtalen.

Tilgang til helse- og personopplysninger for tredjeparter krever konkret avtale utover denne Avtalen mellom partene for alle andre enn Databehandlers underleverandører.

9. Overføring av personopplysninger til utlandet

Partene i denne Avtalen er enige om at ingen av helse- og personopplysningene som behandles under denne Avtalen skal føres ut av Norge, med mindre det er særskilt avtalt mellom partene. I tillegg skal helse- og personopplysninger være plassert på servere i Norge (jf. arkivloven § 9 bokstav b). Eventuelle unntak som innebærer overføring til utlandet skal godkjennes eksplisitt av Behandlingsansvarlig før behandlingen starter.

Databehandler bekrefter at ingen av underleverandørene overfører helse- og personopplysninger som omfattes av denne Avtalen til utlandet, med unntak for slike overføringer som er angitt i Vedlegg 3. Dette omfatter også fjerntilgang fra utlandet.

Bruk av underleverandører som overfører helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal avtales skriftlig med Behandlingsansvarlig på forhånd. Ved overføring av helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal Databehandler benytte godkjente EU-overføringsmekanismer.

Ved overføring til utlandet, uavhengig av om det er innenfor EU/EØS eller utenfor EU/EØS (tredjeland), skal Databehandler gi nødvendig dokumentasjon om sikkerhet, risiko og etterlevelsesnivå knyttet til aktuelle underleverandører slik at Behandlingsansvarlig får nødvendig informasjon for å kunne gjennomføre en særskilt risikovurdering. Behandlingsansvarlig kan nekte samtykke til den aktuelle overføringen basert på spesifikke risikoer som fremkommer av Behandlingsansvarliges egen risikovurdering.

10. Taushetsplikt

Databehandlers ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger i henhold til denne Avtalen med vedlegg og Tjeneste/oppdragsavtale (heretter omtalt som «personer som er autorisert til å behandle personopplysningene»), er underlagt taushetsplikt etter denne Avtalen og gjeldende regelverk. Personer som er autorisert til å behandle personopplysningene forplikter seg til å behandle opplysningene fortrolig. Det samme gjelder eventuelle underleverandører.

Databehandler skal påse at alle som behandler personopplysninger under avtalen er kjent med taushetsplikten.

Ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger skal ha undertegnet taushetserklæring. Bestemmelsen gjelder tilsvarende for underleverandører.

Taushetsplikten gjelder også etter avtalens opphør.

11. Innsyn, verifikasjon og revisjon

Behandlingsansvarlig kan til enhver tid kreve innsyn i og verifikasjon av Databehandlers behandling av personopplysninger tilhørende Behandlingsansvarlig, herunder innsyn i og verifikasjon av dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og Databehandlers system for internkontroll.

Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen som utføres av Databehandler på vegne av Behandlingsansvarlig, og øvrige innsynsrettigheter nedfelt i lov. Hvis Behandlingsansvarlig ber om innsyn skal generell informasjon fra revisjonen gjøres tilgjengelig for andre behandlingsansvarlige som benytter samme tjeneste hos Databehandler.

Behandlingsansvarlig skal så vidt mulig gi Databehandler varsel i rimelig tid ved krav om innsyn og kontroll, vanligvis minst 30 dagers varsel. For krav om dokumentinnsyn bør det gis minst 14 dagers varsel. Behandlingsansvarlig skal medvirke til at innsyn og kontroll kan koordineres mellom flere behandlingsansvarlige som får levert tjenester fra Databehandler. Innsyn og kontroll kan gjennomføres av Behandlingsansvarlig eller tredjepart som Behandlingsansvarlig utpeker. Databehandler kan kreve dekket dokumenterte merkostnader som påløper ved slike revisjoner.

Databehandler skal gi Datatilsynet og annen relevant tilsynsmyndighet tilgang og innsyn i behandlingen av helse- og personopplysninger slik det følger av relevant lovgivning.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes Databehandler eller dennes underleverandører skal korrigeres uten kostnad for Behandlingsansvarlig. Databehandler skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

12. Varighet og opphør

Denne avtalen gjelder fra den er signert av begge parter og til behandlingen av helse- og personopplysninger opphører. Når behandlings av helse- og personopplysninger opphører skal Databehandler tilrettelegge for og medvirke til overføring av alle opplysninger som Databehandler har behandlet på vegne av behandlingsansvarlig/dataansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysningene er overført til og bekreftet mottatt av Databehandlingsansvarlig, skal Databehandler slette opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer.

Databehandler skal gi Databehandlingsansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over

13. Avtalebrudd(mislighold) og erstatning for økonomiske utlegg

Avtalebrudd foreligger dersom en part ikke oppfyller sine forpliktelser etter avtalen, og dette ikke skyldes forhold som den andre parten har ansvaret eller risikoen for. Den som vil påberope seg avtalebrudd må meddele dette til den annen part med skriftlig begrunnelse, uten ugrunnet opphold etter at det aktuelle forholdet ble kjent.

Dersom en part i vesentlig grad misligholder sine forpliktelser etter avtalen kan den andre parten heve avtalen. Den som ønsker å heve skal i skriftlig varsel sette en rimelig frist for retting av forholdet. Av varselet skal det fremgå at avtalen vil bli hevet dersom forholdet ikke er rettet innen fristen.

Overtredelse av taushetsplikt vil alltid anses som vesentlig mislighold.

Dersom avtalebrudd fører til økonomisk tap i form av økte utgifter eller reduserte inntekter, kan den skadelidte parten kreve at motparten dekker tapet.

14. Meddelelser og kontaktpersoner

Alle meddelelser som gis i henhold til denne avtalen skal være skriftlige. Andre språk enn norsk kan bare brukes dersom det er avtalt.

Avsender plikter å vurdere om meddelelsen har et slikt innhold at den skal unntas offentlighet på grunn av personopplysninger eller næringsopplysninger, jf. forvaltningsloven §§ 13 flg.

Følgende kontaktpersoner er oppnevnt i forbindelse med avtalen.

For den databehandlingsansvarlige: Navn, rolle, kontaktinformasjon

For databehandleren: Navn, rolle, kontaktinformasjon

Skifte av kontaktperson skal så snart som mulig meddeles skriftlig til den andre parten.

15. Rettsvalg og verneting

Denne avtalen reguleres av norsk rett.

Partene skal søke å løse tvister gjennom forhandlinger. Tvister som ikke er løst innen 60 dager etter at en part har satt frem krav om forhandlinger, kan hver av partene bringe inn for de ordinære domstoler. <…..Tingrett> vedtas som verneting.

16. Undertegning

Denne avtalen undertegnes i to eksemplarer og partene beholder ett hver.

_____	_____
Sted og dato	Sted og dato
_____	_____
Databehandlingsansvarlig Stilling og navn	Databehandler Stilling og navn

VEDLEGG 1 – BEHANDLINGENS FORMÅL, OPPLYSNINGER OG BEHANDLINGER

Tabellene oppdateres fortløpende og dateres.

[*dato/måned/år*]

A. Formålet med og varigheten av behandlingen

Formålet med og varigheten av behandling av helse- og personopplysninger er: [*husk at hver behandling må være knyttet til spesifikke og uttrykkelig angitt formål – se eksempel nedenfor*]

Dato (fra/til)	Navn på tjeneste	Formålet med behandlingen	Varigheten av behandlingen
<Fyll ut>	Filoverføringstjenesten	Overføre større datamengder	Til formålet er oppnådd
<Fyll ut>	Vedlikehold av system	Drift og forvaltning	I avtaleperioden
<Fyll ut>	Produktutvikling	Bedret funksjonalitet etc	I avtaleperioden
<Fyll ut>	Fillagring	Lagring av filer og databaser	I avtaleperioden
<Fyll ut>	<Fyll ut>	<Fyll ut>	<Fyll ut>

B. Behandling av helse- og personopplysninger

Det følger av personvernforordningen art 4 nr.2 at med «behandling» menes**:** «*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*»

Følgende behandlinger av personopplysninger omfattes av Avtalen: *[se eksempler nedenfor]*

Behandling	Behandlingsaktiviteter
Innsamling	<Fyll ut hvis relevant>
Registrering	<Fyll ut hvis relevant>
Organisering	<Fyll ut hvis relevant>
Strukturering	<Fyll ut hvis relevant>
Lagring	<Fyll ut hvis relevant>
Tilpasning eller endring	<Fyll ut hvis relevant>
Gjenfinning	<Fyll ut hvis relevant>
Sammenstilling	<Fyll ut hvis relevant>
Sletting eller tilintetgjøring	<Fyll ut hvis relevant>
Utlevering/Overføring	<Fyll ut hvis relevant>
Andre former for tilgjengeliggjøring	<Fyll ut hvis relevant>
<Andre relevante behandlinger>	<Fyll ut>

C. Typer av opplysninger

Følgende helse- og personopplysninger behandles: *[her listes opp hvilke helse- og personopplysninger som omfattes – se eksempler nedenfor – fyll ut det som passer]*

Personopplysninger
Navn
Fødselsnummer
Bosted
<Andre opplysninger – fyll ut>

Helseopplysninger
Legemiddelbruk
Diagnoseopplysninger
Opplysninger fra helseregistre
<Andre opplysninger – fyll ut>

D. Kategorier av registrerte

Følgende kategorier av personer behandles det opplysninger om (registrerte): [her listes opp hvilke kategorier av registrerte som omfattes – se eksempler nedenfor]

Kategorier av registrerte		
Pasienter	Helsepersonell	Leverandører
Barn	Ansatte	Nøkkelpersoner
Foreldre	Tidligere ansatte	<Fyll ut>
Fullmektiger	Ansatte i samarbeidende firma	

VEDLEGG 2 – DETALJERTE KRAV TIL INFORMASJONSSIKKERHET

[her listes opp detaljerte krav til informasjonssikkerhet – se eksempler nedenfor – fyll ut det som er relevant]

[*dato/måned/år*]

Nr.	Tema	Krav
1.	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)
2.	Sikring av data	Databehandler skal ha mekanismer for data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet.
3.	Autentisering	Ved tilgang til data ved tjenstlig behov skal det benyttes personlige brukernavn med passord. Databehandler skal ha etablert passordpolicy.
4.	Tjenestenektangrep	<Fyll ut hvis relevant>
5.	Logging og sporbarhet	<Fyll ut hvis relevant>
6.	Redundans og skalering	<Fyll ut hvis relevant>
7.	Testdata	<Fyll ut hvis relevant>
8.	Sletting og tilbakelevering	<Fyll ut hvis relevant>
9.	Lagringstid	<Fyll ut hvis relevant>
10.	Backup og restore	<Fyll ut hvis relevant>
11.	Kryptering ved lagring	<Fyll ut hvis relevant>
12.	Kryptering i kommunikasjon	<Fyll ut hvis relevant>
13.	<Annet>	
14.		
15.		

VEDLEGG 3 – UNDERLEVERANDØRER

[her listes opp hvilke underleverandører som benyttes av Databehandler – se eksempler nedenfor]

Tabellene oppdateres fortløpende.

[*dato/måned/år*]

Navn på underleverandør	Leveranseområde	Stedlig plassering
ABC	Datasenter, hosting	Stockholm, Sverige
DEF	IT-supporttjenester	Oslo, Norge
XYZ	Backup	Paris, Frankrike