

DATABEHANDLERAVTALE

I henhold til personopplysningsloven,
EUs Personvernforordning 2016/679,
Helseregisterloven og
Pasientjournalloven
Mellom

[Virksomhetens navn]

Org.nr.: _____

Behandlingsansvarlig

og

Opus Systemer AS

Org.nr.: 971058676

Databehandler

1. Om avtalen

Denne databehandleravtalen (heretter omtalt som "Avtalen") regulerer rettigheter og plikter mellom Behandlingsansvarlig og Databehandler (heretter omtalt som "partene") etter:

Lov om behandling av personopplysninger av 15.juni 2018 nr. 38 (personopplysningsloven);

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen");

Lov om helseregistre og behandling av helseregistre 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 endrer eller erstatter disse.

Ved motstrid mellom Avtalens regulering og de rammer som følger av personopplysningslovgivningen eller relevant helselovgivningen, viker Avtalens regulering.

Definisjoner

Begrepene "personopplysninger", "behandling", "behandlingsansvarlig", "databehandler", "brudd på opplysningssikkerhet" og "helseopplysninger" skal forstås slik de er definert i personvernforordningen § 4, helseregisterloven § 2 og pasientjournalloven § 2 som gjeldende.

"Avvik": brudd på opplysningssikkerhet og bruk av informasjonssystemet i strid med fastlagte rutiner.

Bruk av informasjonssystemet som ikke er i samsvar med instruksjoner fra Behandlingsansvarlig eller gjeldende personvernlovgivning skal behandles som avvik.

Avtalens bakgrunn og formål

Denne Avtalen er inngått mellom partene og skisserer de generelle vilkårene for den behandling av helse- og personopplysninger som Databehandler utfører på vegne av Behandlingsansvarlig.

Formålet med Avtalen er å sikre behandlingen av helse- og personopplysninger på vegne av Behandlingsansvarlig slik at helse- og personopplysningene ikke brukes urettmessig eller kommer uberettigede i hende.

Omfang

Denne Avtalen kommer til anvendelse på all behandling av helse- og personopplysninger som Databehandler foretar på grunnlag av AVTALE OM LISENS, BRUKSRETT OG VEDLIKEHOLD FOR TANNLEGEPROGRAMMET OPUS DENTAL. (heretter omtalt som "Tjeneste/oppdragsavtalen"). I tilfelle konflikt mellom denne Avtalen og Tjeneste/oppdragsavtalen, skal denne Avtalen gjelde. Tjenester som inngår i denne Avtalen er de tjenester som inngår i Tjeneste/oppdragsavtalen og som innebærer behandling av helse- og personopplysninger.

Denne Avtalen vil i tillegg gjelde for ytterligere behandling av helse- og personopplysninger basert på eventuelle skriftlige avtaler mellom partene som inngås i løpet av denne Avtalens virksomhetsperiode og som innebærer at

Databehandler behandler helse- og personopplysninger på vegne av Behandlingsansvarlig (heretter omtalt som "senere skriftlige avtaler mellom partene").

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.

Behandlingens formål, opplysninger og behandlinger

Formålet med og varigheten av behandling av helse- og personopplysninger, hvilke helse- og personopplysninger som behandles, kategorier av de registrerte og behandlingens art er angitt i Vedlegg 1.

Nærmere beskrivelse av behandlingen, behandlingens formål og hvilke helse- og personopplysninger som omfattes fremgår av Tjeneste/oppdragsavtalen og senere skriftlige avtaler mellom partene.

Rammene 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.

Behandlingsansvarliges plikter

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

Databehandlers plikter

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 "Norm for informasjonssikkerhet i helse- og omsorgstjenesten". 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, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene;
- 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 eller Behandlingsansvarlig har godkjent dette skriftlig;
- 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, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene.

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;
- 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 Databehandlerens løsninger, der dette er mulig teknisk sett.
- i. gi Behandlingsansvarlig nødvendig bistand i de tilfeller hvor databehandler har tilgang til behandlingsansvarliges data, slik at Behandlingsansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;
- j. samarbeide med og bistå Behandlingsansvarlig i form av sitt oppdrag hvor databehandler har fått tilgang til sensitive data, 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 fra Behandlingsansvarlig er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;
- l. bistå Behandlingsansvarlig i databehandlerens oppdrag/leveranse av tjenester hvor databehandler har tilgang til behandlingsansvarliges data, å sørge for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet.

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 (skytjenester), 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 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/opplevingsavtalen spesifiserer; i.h.h.t. lovens krav - Normen
- j. sørge for at Databehandlers behandling av data som tilhører Behandlingsansvarlig ivaretar de samme pliktene som Behandlingsansvarlig har med å sikre overholdelse av forpliktelsene i personvernforordningen artikkelene 32–34, i forbindelse med databehandlers behandling av person og helseopplysninger 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 økning av risikobildet;
- m. innhente godkjenning av Behandlingsansvarlig før gjennomføring av enhver endring av databehandlingen hos Databehandler som har eller kan påvirke informasjonssikkerheten i negativ retning.

Nærmere krav til Databehandlerens informasjonssikkerhet er angitt i **Vedlegg 2**.

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.

Bruk av underleverandør

Behandlingsansvarlig tillater at Databehandler benytter underleverandører for oppfyllelse av forpliktelsene under Avtalen. Databehandler benytter pr dags dato underleverandører som angitt i **Vedlegg 3** for de der angitte tjenester. Databehandler har rett til fritt å legge til eller bytte ut underleverandører som etterkommer de samme kravene som stilles til Databehandleren i denne avtalen gitt i bokstav a-b under

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 på forespørsel;
- 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 databehandleravtalen 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. 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 12;
- g. 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 13 på samme måte som Databehandler så langt det ikke strider mot andre lovbestemmelser.

Databehandlerens sikring dekkes opp på slik måte som beskrevet i punkt a-g.

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.

Overføring av personopplysninger til utlandet

Personopplysninger skal kun overføres til land utenfor EU/EØS (tredjeland) etter instruks fra den Behandlingsansvarlige. Databehandleren skal altså ikke overføre eller la personer i tredjeland på noen måte få tilgang til personopplysninger uten at den Behandlingsansvarlige på forhånd eksplisitt har godkjent dette skriftlig og gitt instruks om overføring eller tilgang. Samtykke og instruks må dekke hvilke land opplysningene skal kunne overføres til. Overføring til tredjeland forutsetter, selv med samtykke og instruks, at de krav til sikkerhet og vern av de registrertes rettigheter som følger av personopplysningsloven og annet regelverk er ivarettatt.

Taushetsplikt

Databehandlers ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av personopplysninger i henhold til denne Avtalen, Tjeneste/oppdragsavtale og senere skriftlige avtaler mellom partene (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.

Partene har i tillegg taushetsplikt om konfidensiell informasjon knyttet til hverandres virksomhet, som er formidlet i forbindelse med oppdraget.

Partene plikter å ta de forholdsregler som er nødvendige for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

Taushetsplikten gjelder også etter Avtalens opphør.

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 på forespørsel.

Behandlingsansvarlig skal gi Databehandler varsel i rimelig tid ved krav om innsyn og kontroll, vanligvis minst 30 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.

Varighet og opphør

Denne Avtalen gjelder fra den er signert av partene og gjelder til Avtalen og alle gjeldende avtaler mellom partene, som innebærer at Databehandler skal behandle helse- og personopplysninger på vegne av Behandlingsansvarlig, er opphørt.

Ved opphør av Avtalen skal Databehandler tilrettelegge for og medvirke til tilbakeføring av alle opplysninger som Databehandler har mottatt og behandlet på vegne av Behandlingsansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje. Databehandler kan kreve dekket kostnader som påløper ved slike overføringer etter den til enhver gjeldende prislister som Databehandler har for slike oppdrag.

Etter at alle opplysningene er overført til Behandlingsansvarlig og bekreftet mottatt av denne, skal Databehandler irreversibelt slette eller forsvarlig destruere alle opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer, med mindre ufravikelige rettsregler krever at helse- og personopplysningene fortsatt lagres.

Databehandler skal gi Behandlingsansvarlig skriftlig bekreftelse på at opplysningene er overført, slettet eller utilgjengeliggjort som angitt over.

Se for øvrig vedlegg 2 punkt 8.

Endring av avtale

I tilfelle endringer i gjeldende lovverk, endelig dom som gir en annen tolkning av gjeldende lov, eller endringer i tjenester i Tjeneste/oppdragsavtalen som krever endringer av denne Avtalen, skal partene samarbeide for å oppdatere Avtalen tilsvarende.

Meddelelser

Meddelelser, underretting, varsel eller annen kommunikasjon mellom Behandlingsansvarlig og Databehandler skal gis skriftlig.

Lovvalg og vernetting


Avtalen er underlagt norsk rett og partene vedtar Asker og Bærum tingrett som vernetting. Dette gjelder også etter opphør av Avtalen.

Undertegning

DATABEHANDLERAVTALE

Denne Avtalen foreligger i to originaler, hvorav partene beholder et eksemplar hver.

Sted og dato:

Behandlingsansvarlig	Databehandler
	Opus Systemer AS
Navn:	Navn: Jarle B. Mathisen
Sign:	

VEDLEGG 1 – BEHANDLINGENS FORMÅL, OPPLYSNINGER OG BEHANDLINGER

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]*

Tjeneste	Formålet med behandlingen	Varigheten av behandlingen
Support/Konsulent	Veilede og bistå korrekt føring i EPJ systemet, feilretting, teknisk bistand osv.	Løpende i.h.h.t. Tjenesteavtalen og senere avtaler
API	Overføre data slik at de er tilgjengelig i Skyen for presentasjon i andre systemer som kundene benytter seg av i pasientbehandling	Til formålet er oppnådd - er regulert i en API avtale løpende
E-timebok	Selvbetjening for pasienten til å kunne administrere timebestillinger, ombestillinger, avbestilling av timeavtaler	Løpende er regulert i egen avtale for tjenesten (tilleggstjeneste)
Splitting skjøting	Flere baser sammen – eller fra hverandre	Databaser som er i besittelse av Databehandler beholdes så lenge det er behov for det i oppdraget, data slettes senest 2 måneder etter at oppdraget er avsluttet. Avslutning beregnes å inntreffe når Behandlingsansvarlig har kontrollert de leverte dataene.
Filoverføringstjeneste	Elektronisk overføring av databaser mellom databehandleransvarlig og Opus Systemer AS (databehandler) i forbindelse med ulike oppdrag/tjenester som skal utføres i databasene til behandlingsansvarlig. Regulert av eget rutineskriv.	Til formålet er oppnådd – fjernes så snart databasen er mottatt eller levert tilbake til databehandleransvarlig
Konvertering	Konverterer data fra andre EPJ systemer, evt andre systemer som har lagret pasient data inn til en database som kan anropes fra Opus Dental	Til formålet er oppnådd. Databaser som er i besittelse av Databehandler beholdes så lenge det er behov for det i oppdraget, data slettes senest 2 måneder etter at oppdraget

		er avsluttet. Avslutning beregnes å inntreffe når Behandlingsansvarlig har kontrollert de leverte dataene.
Skytjenester/Drift	Registrering av data EHR med tilleggstjenester i.h.h.t Tjeneste/oppdragsavtalen	Løpende for skytjenestene i.h.h.t Tjeneste/oppdragsavtalen

B. Behandling av helse- og personopplysninger

Følgende behandlinger omfattes av Avtalen: [her listes opp hvilke behandlinger av helse- og personopplysninger som omfattes – se eksempler nedenfor]

Behandling	Behandlingsaktiviteter
Support/Konsulent/Fjernsupport	Veileder og bistår korrekt føring i EPJ systemet, feilretter, teknisk bistand osv på telefon og via online påloggingstjeneste i.h.h. til rutineskriv. Registrerer CRM saker i internt kundesystem, slik at man kan følge opp kundesaker. Oppbevarer saksdokumentasjon i CRM systemet.
Skjøting/Splitting	Tar inn databaser kjører oppdatering av pas nr. skjøter, splitter, synkroniserer data
Konvertering	Konverterer data fra andre EPJ systemer, evt andre systemer som har lagret pasient data.
E-timebok	Registret data i skytjenesten er kontaktinformasjon til hver kunde med kontaktperson og etimebok nøkkel(API-nøkkel). Unikt for hver kunde. Løpende for skytjenestene i.h.h.t Tjeneste/oppdragsavtalen/tilleggsavtaler
Sletting eller tilintetgjøring	Databaser som er i besittelse av Databehandler i form av tjenester som blir levert, beholdes så lenge det er behov for det i oppdraget, data slettes senest 2 måneder etter at oppdraget er avsluttet. Avslutning beregnes å inntreffe når Behandlingsansvarlig har kontrollert de leverte dataene.

<p>Utlevering/Overføring/Tilbakelevering</p>	<p>Elektronisk overføring av databaser mellom databehandleransvarlig og Opus Systemer AS(databehandler) i forbindelse med ulike oppdrag/tjenester som skal utføres i databasene til behandlingsansvarlig. Metoden som benyttes er regulert i eget rutineskriv for sikker overføring av pasientdata i henhold til dialog med datatilsynet.</p> <p>Andre metoder kan benyttes, dersom det innebærer høyere sikkerhet.</p>
<p>Opus skytjeneste</p>	<p>Drifning av Opus Dental skytjenester. Lagrer EHR data i MS SQL database til skytjenesten Opus Dental V8 og fremtidige versjoner. Gjelder dersom avtale om tilleggstjenesten er signert. Regulert i egen tjenesteavtale. Løpende for skytjenestene i.h.h.t Tjeneste/oppdragsavtalen/tilleggsavtaler</p>
<p>Utteksling av data til API</p>	<p>Via tilpasset rest API utveksles data og resultatene leveres som JSON eller XML, standard er JSON. Data utveksles på grunnlag av API anrop til tjenesten fra tredjepart. For å bruke API-funksjonene krever det en API-nøkkel levert av Opus som inngår i kallet. Hver funksjon kalles av adressen www.yourdomain.opusdentalonline.com. Løpende for skytjenestene i.h.h.t Tjeneste/oppdragsavtalen/tilleggsavtaler</p>

C. Typer av opplysninger

Følgende helse- og personopplysninger behandles: [her listes opp hvilke helse- og personopplysninger som omfattes – se eksempler nedenfor]

Personopplysninger	Helseopplysninger
Navn	EPJ – Alle føringer i EPJ som f.eks personalia, journal, timeavtaler, helseskjema, dokumenter inneholdende helseopplysninger, sendinger og svar til og fra Helfo, henvisinger epikriser, sykemeldinger etc.
Fødselsnummer	
Bosted	Opplysninger fra helseregistre, Helfo, Folkeregisteret, Kommunikasjonspartnere, som f.eks spesialister.
Telefon, epost, foresatte	

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
Voksne og Barn	Ansatte	Nøkkelpersoner
Foreldre	Tidligere ansatte	
Fullmektiger	Ansatte i samarbeidende firma	

VEDLEGG 2 – DETALJERTE KRAV TIL INFORMASJONSSIKKERHET

[her listes opp detaljerte krav til informasjonssikkerhet – se eksempler nedenfor]

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 å sikre 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	Antivirus, Win Update og brannmur.
5.	Logging og sporbarhet	Ved tilgang til data ved tjenstlig behov skal det benyttes personlige brukernavn med passord. Logging er standard for tilgangen.
6.	Redundans og skalering	Ingen
7.	Testdata	Databehandler er ikke i besittelse av testdata for Behandlingsansvarlig.
8.	Sletting og tilbakelevering	Databaser som er i besittelse av Databehandler beholdes så lenge det er behov for det i oppdraget, data slettes senest 2 måneder etter at oppdraget er avsluttet. Avslutning beregnes å inntreffe når Behandlingsansvarlig har kontrollert de leverte dataene (evalueringsperiode for å ivareta reklamasjoner).
9.	Lagringstid	Løpende for skytjenestene i.h.h.t Tjeneste/oppdragsavtalen . Databaser til skjøting – splitting, feilsøking og reparasjon -> se punkt 8.
10.	Backup og restore	For arbeidet Databehandler gjør følges rutiner for backup.
11.	Kryptering ved lagring	Ingen
12.	Kryptering i kommunikasjon	Visma Link – kryptering i.h.h.t. Lovkrav/ Normen

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
HF Dataservice	Skjøting splitting, feilsøking, retting, scripting i databaser, samt programmering	Tromsø, Norge
Oppu Systemer AS Norge Filial (Datterselskap)	Feilsøking, retting, scripting i databaser, samt programmering, E timebok	Malmø Sverige
Microsoft	Database I azure	Vest-Europa
Visma Link	Elektronisk meldingstjeneste – 2.linje programsupport- teknisk support – fjernpålogging.	Lokal installasjon på behandlingsansvarliges server