# DATABEHANDLERAVTALE

I henhold til personopplysningsloven,

EUs Personvernforordning 2016/679,

Helseregisterloven, Normen og

Pasientjournalloven

Mellom

---

[Virksomhetens navn]

Org.nr.: _____

*Behandlingsansvarlig*

og

Opus Systemer AS

Org.nr.: 971058676

*Databehandler*

## 1. Avtalens formål

1.1 Denne databehandleravtalen ("DBA") fastsetter partenes rettigheter og plikter når Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige som del av leveransene under Avtalen. DBA har som formål å sikre at partene etterlever Gjeldende personvernregler.

1.2 DBA består av dette dokumentet, samt Vedlegg 1-3. Vedleggene utgjør en integrert del av DBA.

1.3 Ved eventuell motstrid mellom DBA og Avtalen, har DBA forrang.

## 2. Definisjoner

2.1 "Personopplysninger", "behandling", "behandlingsansvarlig", "databehandler", "brudd på opplysningssikkerhet" og "helseopplysninger" skal forstås slik de er definert i personvernforordningen artikkel 4, helseregisterloven § 2 og pasientjournalloven § 2.

2.2 «Gjeldende personvernregler»: Den til enhver tid gjeldende versjon av EUs personvernforordning (2016/679) ("personvernforordningen"), samt lov om behandling av personopplysninger av 15.06. 2018 (personopplysningsloven) med tilhørende forskrifter mv., samt eventuell annen relevant lovgivning slik som lov om helseregistre og behandling av helseregistre av 20.juni 2014 nr. 43 (helseregisterloven) og lov om behandling av helseopplysninger ved ytelse av helsehjelp av 20.juni 2014 nr. 42 (pasientjournalloven).

2.3 «Avtalen»: En eller flere avtaler mellom Behandlingsansvarlig og Databehandler om bruk og tjenester knyttet til tannlegeprogrammet Opus Dental som leveres av Databehandler og som innebærer behandling av personopplysninger. DBA kan gjelde flere underliggende avtaler.

2.4 «Underdatabehandler»: Annen virksomhet som benyttes av Databehandler som underleverandør til behandling av personopplysninger under DBA.

2.5 For personvernbegreper som ikke er definert i denne DBA gjelder definisjonene i personvernforordningen artikkel 4.

## 3. Behandlingens formål, opplysninger og behandlinger

3.1 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.

3.2 Nærmere beskrivelse av behandlingen, behandlingens formål og hvilke helse- og personopplysninger som omfattes, fremgår av Vedlegg 1 og 2.

## 4. Rammene for behandling av helse- og personopplysninger

4.1 Behandlingsansvarlig har til enhver tid full rådighet over de helse- og personopplysningene som Databehandler har anledning til å behandle etter denne DBA. Databehandler har ikke selvstendig råderett over helse- og personopplysningene, og kan ikke behandle disse til egne formål. Databehandler kan imidlertid anonymisere helse- og personopplysninger mottatt og behandlet på vegne av Behandlingsansvarlig, forutsatt at anonymiseringen gjennomføres på en måte som utelukker enhver mulighet for å identifisere enkeltpersoner. Det anonymiserte datamaterialet kan deretter benyttes til statistikk, analyser og for videreutvikling og forbedring av Databehandlers tjenestespekter.

4.2 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. Anonymiserte data, hvor det ikke er mulig å identifisere enkeltpersoner, er ikke å anse som helse- og personopplysninger, og vil derfor ikke omfattes av denne DBA og dermed heller ikke innsynsretten eller andre forhold knyttet til denne DBA.

## 5. Behandlingsansvarliges plikter

5.1 Behandlingsansvarlige har ansvaret for at behandlingen av personopplysninger skjer i samsvar med Gjeldende personvernregler. Behandlingsansvarlige skal i den forbindelse særskilt sørge for at:

i. behandlingen av personopplysninger er formålsbestemt og basert på et gyldig rettsgrunnlag;

ii. de registrerte har mottatt nødvendig informasjon om behandlingen av personopplysningene;

iii. Behandlingsansvarlig har gjennomført tilstrekkelige risikovurderinger; og

iv. Databehandler til enhver tid har tilstrekkelige instrukser og informasjon for å oppfylle sine plikter i henhold til DBA og Gjeldende personvernregler.

## 6. Databehandlers plikter

6.1 Databehandleren skal bare behandle personopplysninger etter dokumenterte instrukser fra den behandlingsansvarlige, og i samsvar med Gjeldende personvernregler og Norm for informasjonssikkerhet i helse- og omsorgstjenesten («Normen»), med mindre noe annet kreves av unionsretten eller medlemsstatenes nasjonale rett som Databehandleren er underlagt. Disse instruksene er spesifisert i Vedlegg 1-3.

6.2 Databehandleren skal omgående underrette den Behandlingsansvarlige dersom en instruks fra den Behandlingsansvarlige, etter Databehandlerens mening, er i strid med gjeldende personvernregler i unionsretten eller medlemsstatenes nasjonale rett.

6.3 Hvis annen behandling er nødvendig for å oppfylle forpliktelser som Databehandler er underlagt i henhold til gjeldende rett, skal Databehandleren underrette den Behandlingsansvarlige så langt dette er tillat ved lov, jf. personvernforordningen artikkel 28 (3) (a).

## 7. Tekniske, organisatoriske og sikkerhetsmessige tiltak

7.1 Personvernforordningen artikkel 32 fastslår at, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål 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.

7.2 Den Behandlingsansvarlige skal vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør og gjennomføre tiltak for å imøtegå disse risikoene. Avhengig av relevans kan tiltakene omfatte:

- pseudonymisering og kryptering av personopplysninger
- evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene
- evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse
- en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er

7.3 Ifølge personvernforordningen artikkel 32 skal databehandleren – uavhengig av den behandlingsansvarlige – også vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør, og gjennomføre tiltak for å imøtegå risikoene. Med henblikk på denne vurderingen skal den Behandlingsansvarlige stille den nødvendige informasjonen til rådighet for Databehandleren som gjør vedkommende i stand til å identifisere og vurdere slike risikoer.

7.4 Databehandleren skal også bistå den Behandlingsansvarlige med å overholde den Behandlingsansvarliges plikter etter personvernforordningen artikkel 32, ved blant annet å stille til den behandlingsansvarliges rådighet nødvendig informasjon om de tekniske og organisatoriske sikkerhetstiltakene som Databehandleren allerede har gjennomført i henhold til personvernforordningen artikkel 32, samt all annen informasjon som er nødvendig for at den Behandlingsansvarlige skal kunne overholde sine plikter etter personvernforordningen artikkel 32. Nærmere krav til Databehandlerens informasjonssikkerhet er angitt i Vedlegg 2.

## 8. Melding om brudd på personopplysningssikkerheten

8.1 Ved brudd på personopplysningssikkerheten skal Databehandleren underrette den Behandlingsansvarlige om bruddet uten ugrunnet opphold etter å ha fått kjennskap til det.

8.2 Databehandlerens underretning til den Behandlingsansvarlige skal om mulig skje innen 48 timer etter at Databehandleren har fått kjennskap til bruddet på personopplysningssikkerheten, slik at den Behandlingsansvarlige kan overholde sin forpliktelse til å melde bruddet til den kompetente tilsynsmyndigheten, jf. personvernforordningen artikkel 33.

8.3 I overensstemmelse med DBA punkt 12.3 bokstav a skal Databehandleren bistå den Behandlingsansvarlige med å melde bruddet til den kompetente tilsynsmyndigheten. Det innebærer at Databehandleren skal bistå med å fremskaffe informasjon listet opp nedenfor, som ifølge personvernforordningen artikkel 33 nummer 3 skal fremgå av den Behandlingsansvarliges melding av bruddet til den kompetente tilsynsmyndigheten:

a. arten av bruddet på personopplysningssikkerheten, 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 konsekvenser av bruddet på personopplysningssikkerheten

c. de tiltak som den Behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

8.4 Partene skal i Vedlegg 2 oppgi all informasjon som Databehandleren skal fremskaffe når vedkommende bistår den Behandlingsansvarlige med å melde brudd på personopplysningssikkerheten til den kompetente tilsynsmyndigheten.

## 9. Bruk av underdatabehandlere

9.1 Databehandleren skal oppfylle betingelsene som er fastsatt i personvernforordningen artikkel 28 nummer 2 og nummer 4 for å gjøre bruk av en annen databehandler (en underdatabehandler). Databehandleren må således ikke bruke en underdatabehandler for å oppfylle DBA uten på forhånd å ha innhentet en generell skriftlig godkjennelse fra den Behandlingsansvarlige.

9.2 Databehandleren har den Behandlingsansvarliges generelle godkjennelse til å benytte underdatabehandlere. Listen over underdatabehandlere som den Behandlingsansvarlige allerede har godkjent fremgår av Vedlegg 3.

9.3 Når Databehandleren engasjerer en underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den Behandlingsansvarlige, skal underleverandøren pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i denne DBA, ved hjelp av en 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 DBA og gjeldende personvernregler.

Databehandleren er derfor ansvarlig for å kreve at underdatabehandleren som minimum overholder databehandlerens forpliktelser etter denne DBA og personvernforordningen.

9.4 En kopi av slik underdatabehandleravtale og eventuelle etterfølgende endringer skal ved den Behandlingsansvarliges anmodning sendes til den Behandlingsansvarlige, som på denne måten har mulighet for å sørge for at underdatabehandleren er pålagt de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i denne DBA. Kommersielle bestemmelser som ikke påvirker det personopplysningsvernrettslige innholdet av underdatabehandleravtalen, er ikke underlagt kravet om kopi til den Behandlingsansvarlige.

9.5 Databehandleren skal i underdatabehandleravtalen inkludere den Behandlingsansvarlige som begunstiget tredjepart i tilfelle databehandleren går konkurs, slik at den Behandlingsansvarlige kan tre inn i databehandlerens rettigheter og gjøre dem gjeldende overfor underdatabehandler, hvilket for eksempel setter den Behandlingsansvarlige i stand til å instruere underdatabehandleren om å slette eller tilbakeføre personopplysningene.

9.6 Hvis underdatabehandleren ikke oppfyller sine personopplysningsvernforpliktelser blir Databehandleren ansvarlig overfor den Behandlingsansvarlige når det gjelder oppfyllelse av underdatabehandlerens forpliktelser. Dette påvirker ikke de registrertes rettigheter etter personvernforordningen - særlig de nedfestet i personvernforordningen artikkel 79 og 82 - overfor den behandlingsansvarlige og databehandleren, herunder underdatabehandleren.

## 10. Overføring til tredjeland

10.1 Databehandleren kan kun overføre personopplysninger til tredjeland eller internasjonale organisasjoner etter dokumentert instruks fra den Behandlingsansvarlige, og slik overføring skal alltid skje i overensstemmelse med personvernforordningen kapittel V.

10.2 Hvis overføring av personopplysninger til tredjeland eller internasjonale organisasjoner, som databehandleren ikke er blitt instruert av den Behandlingsansvarlige om å gjennomføre, kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som Databehandleren er underlagt, skal Databehandleren underrette den Behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning.

10.3 Uten dokumentert instruks fra den Behandlingsansvarlige kan Databehandleren innenfor rammene av denne DBA således ikke:

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

b. overlate behandling av personopplysninger til en underdatabehandler i et tredjeland

c. behandle personopplysningene i et tredjeland

10.4 Den Behandlingsansvarliges instruks når det gjelder overføring av personopplysninger til et tredjeland, herunder det eventuelle overføringsgrunnlaget i personvernforordningen kapittel V som overføringen er basert på, skal angis i Vedlegg 2.

## 11. Konfidensialitet

11.1 Databehandleren kan bare gi tilgang til personopplysninger som behandles på den Behandlingsansvarliges vegne til personer underlagt Databehandlerens instruksjonsmyndighet som har forpliktet seg til konfidensialitet eller er underlagt en passende lovbestemt taushetsplikt, og bare i det nødvendige omfang.

11.2 Listen av personer som har fått tilgang skal gjennomgås fortløpende. På bakgrunn av en slik gjennomgang kan tilgangen til personopplysninger stenges, dersom den ikke lenger er nødvendig, og personopplysningene skal deretter ikke lenger være tilgjengelig for disse personene.

11.3 Databehandleren skal etter anmodning fra den Behandlingsansvarlige kunne påvise at de aktuelle

personene underlagt Databehandlerens instruksjonsmyndighet er underlagt ovennevnte taushetsplikt.

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

11.5 Taushetsplikten gjelder også etter Avtalens opphør.

## 12. Bistand til den behandlingsansvarlige

12.1 Databehandleren bistår, idet det tas hensyn til behandlingens art og i den grad det er mulig, ved hjelp av egnede tekniske og organisatoriske tiltak, den Behandlingsansvarlige med å oppfylle vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III.

12.2 Dette innebærer at Databehandleren så langt det er mulig skal bistå den Behandlingsansvarlige i den Behandlingsansvarlige oppfyllelse av:

a. opplysningsplikten ved innsamling av personopplysninger fra den registrerte
b. opplysningsplikten dersom personopplysninger ikke er blitt samlet inn fra den registrerte
c. den registrertes rett til innsyn
d. retten til retting
e. retten til sletting («retten til å bli glemt»)
f. retten til begrensning av behandling
g. underretningsplikten i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling
h. retten til dataportabilitet
i. retten til å protestere
j. retten til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisk behandling, herunder profilering

12.3 I tillegg til Databehandlerens forpliktelse til å bistå den Behandlingsansvarlige i henhold til DBA 7.4, bistår Databehandleren også, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for Databehandleren, den Behandlingsansvarlige med:

a. den Behandlingsansvarliges forpliktelse ved brudd på personopplysningssikkerheten til uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet på personopplysningssikkerheten til den kompetente tilsynsmyndigheten, Datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter
b. den Behandlingsansvarliges forpliktelse til uten ugrunnet opphold å underrette den registrerte om bruddet på personopplysningssikkerheten når det er sannsynlig at bruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter
c. den Behandlingsansvarliges forpliktelse til før behandlingen å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (vurdering av personvernkonsekvenser)
d. den Behandlingsansvarliges forpliktelse til å rådføre seg med den kompetente tilsynsmyndigheten, Datatilsynet, før behandlingen dersom en vurdering av personvernkonsekvenser tilsier at behandlingen vil medføre en høy risiko dersom den Behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.

12.4 Partene skal i Vedlegg 2 oppgi de egnede tekniske og organisatoriske tiltakene gjennom hvilke Databehandleren skal bistå den Behandlingsansvarlige, samt omfanget og utstrekningen av den

påkrevde bistanden.

## 13. Revisjon

13.1 Databehandleren skal stille til den Behandlingsansvarliges disposisjon all informasjon som er nødvendig for å påvise etterlevelse av forpliktelsene etter personvernforordningen artikkel 28 og denne DBA. Videre skal Databehandleren muliggjøre og bidra til revisjoner, herunder inspeksjoner, som utføres av den Behandlingsansvarlige eller en annen revisor som er bemyndiget av den Behandlingsansvarlige.

13.2 Prosedyrene for den Behandlingsansvarliges revisjoner, herunder innsyn og inspeksjoner, av Databehandleren er spesifisert i Vedlegg 2. Databehandleren forplikter seg til å gi tilsynsmyndighetene, som etter gjeldende lovgivning har tilgang til den Behandlingsansvarliges eller Databehandlerens lokaler, eller representanter som opptrer på slike tilsynsmyndigheters vegne, adgang til Databehandlerens fysiske lokaler ved presentasjon av behørig legitimasjon.

## 14. Varighet og opphør

14.1 Denne DBA gjelder fra den er signert av partene og gjelder så lenge databehandlertjenestene varer. Reglene om oppsigelse i Avtalen gjelder tilsvarende for DBA, så langt de passer. DBA kan ikke sies opp så lenge Avtalen består med mindre den avløses av en ny databehandleravtale.

## 15. Sletting og returnering av opplysninger

15.1 Ved opphør av DBA 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 prisliste som Databehandler har for slike oppdrag.

15.2 Senest to måneder etter at opplysningene er overført til Behandlingsansvarlig, skal Databehandler slette alle personopplysningene som denne har mottatt og behandlet på vegne av Behandlingsansvarlig, med mindre annet er skriftlig avtalt mellom partene.

15.3 Databehandler skal gi Behandlingsansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over.

## 16. Endring av avtale

16.1 Databehandler har rett til å endre, tilpasse eller oppdatere denne DBA, dersom det er nødvendig som følge av endringer i tjenestene som leveres mellom partene, teknologiske oppdateringer, endring eller utvikling i behandlingsaktivitetene, eller for å sikre etterlevelse av gjeldende personvernlovgivning, bindende retningslinjer eller rettskraftige domstolsavgjørelser. Databehandler skal varsle Behandlingsansvarlig skriftlig i rimelig tid før slike endringer trer i kraft.

16.2 Hver av partene kan for øvrig foreslå andre endringer i denne DBA. Endringer trer ikke i kraft før de er skriftlig avtalt mellom partene.

16.3 Dersom en endring medfører merarbeid for Databehandler, har Databehandler krav på godtgjørelse. Dersom endringen kun får betydning for Behandlingsansvarlig og ikke øvrige kunder, vil slik godtgjørelse beregnes på grunnlag av medgått tid og Databehandlers til enhver tid gjeldende timepriser, med mindre annet er skriftlig avtalt mellom partene. Dersom det gjøres endringer med betydning for alle kunder, vil kostnadene kunne bli fordelt på kundene gjennom prisøkning av tjenesten eller på annen måte. Godtgjørelse for endringer som initieres av Behandlingsansvarlig og som ikke er regulert av punkt 8 eller 9 i Vedlegg 2, skal fastsettes etter nærmere avtale mellom partene.

## 17. Meddelelser

17.1 Meddelelser, underretting, varsel eller annen kommunikasjon mellom Behandlingsansvarlig og

Databehandler skal gis skriftlig.

## 18. Lovvalg og verneting

18.1 DBA er underlagt norsk rett og partene vedtar Oslo tingrett som verneting.

*****

| For Databehandler | For Behandlingsansvarlig |
|---|---|
| Opus Systemer AS | _____<br>VIRKSOMHETENS NAVN |
| _____<br>NAVN<br>_____<br>Underskrift | _____<br>NAVN<br>_____<br>Underskrift |

DBA signeres i to eksemplarer, en til hver part.

## VEDLEGG

**Vedlegg 1**: Behandlingens formål

**Vedlegg 2:** Instruks for behandling av personopplysninger

**Vedlegg 3**: Godkjente underdatabehandlere

## VEDLEGG 1 – OPPLYSNINGER OM BEHANDLINGEN

### 1. Formålet med behandlingen og hvordan opplysningene behandles

Databehandleren har utviklet- og tilbyr bruk av tannlegeprogrammet Opus Dental med tilhørende tjenester («Journalsystemet»). Journalsystemet tilbys som en stasjonær løsning eller som en skytjeneste. Journalsystemet innbefatter ulike moduler og tjenester, herunder også applikasjoner levert fra 3. parter.

Det overordnede formålet med behandlingen er drift og vedlikehold av Journalsystemet, herunder tilrettelegging for Behandlingsansvarlig sin bruk av Journalsystemet. Dette omfatter teknisk håndtering og lagring av pasientjournaler, digitale funksjoner som meldingsutveksling, pasientportal og rapportering, samt teknisk og operasjonell support. Databehandleren bistår i tillegg med håndtering av data, som overføring, sletting og konvertering av helse- og personopplysninger, og tilrettelegger for integrasjoner med applikasjoner som inngår i journalsystemet samt øvrige systemer som den behandlingsansvarlige benytter. Databehandler tilbyr også rådgivning og veiledning.

Det avtalte formålet inkluderer også databehandlerens anonymisering av personopplysninger som omfattes av Journalsystemet, for statistikk, analyser og for videreutvikling og forbedring av Databehandlers tjenestespekter.

Personopplysningene behandles så lenge det er nødvendig og påkrevd i henhold til gjeldende avtale mellom databehandler og behandlingsansvarlig.

### 2. Hvordan opplysningene behandles

Den avtalte behandlingen omfatter innsamling og registrering av informasjon gjennom Journalsystemet, samt behandling av slike opplysninger for det formål å kunne levere Journalsystemet med den funksjonalitet som ligger i tjenesten til enhver tid, herunder drift, vedlikehold, support, lagring, rapportering, anonymisering og sletting, samt også utvikling og system- og tjeneste-forbedringer.

### 3. Typer av opplysninger

Følgende helse- og personopplysninger behandles:

| Personopplysninger | Registrerte |
|---|---|
| ID- og kontaktinformasjon, informasjon om timebestilling og fakturering, samt helseopplysninger (fra helseskjema, resepter, bilder, journal, kommunikasjon med Helfo og helsepersonell, henvisninger, epikriser, sykemeldinger, helseregisteret, Folkeregisteret, etc.) | Pasienter |
| ID- og kontaktinformasjon, samt opplysninger relatert til håndtering og oppfølging av pasienten. | Foresatte, fullmektiger/verger for pasienter |

| | |
|---|---|
| ID- og kontaktinformasjon, ansattnummer, brukerlogger og systemaktivitet, tilgangsrettigheter, påloggingsdata og administrativ og arbeidsrelatert informasjon | Ansatte hos behandlingsansvarlig, tidligere ansatte og ansatte i samarbeidende selskaper |
| ID- og kontaktinformasjon, stillingsbetegnelse, kommunikasjonsdata, og avtale- og fakturarelaterte opplysninger | Leverandører, samarbeidspartnere, organisasjoner og deres ansatte |

## VEDLEGG 2 – INSTRUKS FOR BEHANDLING AV PERSONOPPLYSNINGER

### 1. Bakgrunn

Dette vedlegget regulerer krav til informasjonssikkerhet og tilhørende tekniske og organisatoriske tiltak som Databehandler skal iverksette ved behandling av helse- og personopplysninger på vegne av Behandlingsansvarlig. Bestemmelsene tar utgangspunkt i personopplysningsloven, personvernforordningen (EU 2016/679), samt gjeldende helselovgivning.

### 2. Informasjonssikkerhet

Behandlingen av personopplysninger for den behandlingsansvarlige omfatter både alminnelige personopplysninger og særskilte kategorier personopplysninger, samt konfidensiell informasjon knyttet til den behandlingsansvarliges ansatte og pasienter.

Ettersom personopplysningene som oppgis i forbindelse med behandlingsansvarliges journalsystem sannsynligvis vil innebære behandling av helseopplysninger, er det avtalt at, hensyntatt behandlingens art, omfang, kontekst og formål og risikoen for varierende sannsynlighet og alvorlighetsgrad for fysiske personers rettigheter og friheter, sikkerhetstiltakene må gjenspeile et høyt sikkerhetsnivå.

Databehandler har da rett og plikt til å fatte vedtak om hvilke tekniske og organisatoriske sikkerhetstiltak som skal iverksettes for å etablere nødvendig (og avtalt) sikkerhetsnivå, og databehandler kan fortløpende endre iverksatte sikkerhetstiltak innenfor disse rammene.

Databehandleren må imidlertid – under alle omstendigheter og som et minimum – gjennomføre **følgende tiltak avtalt med behandlingsansvarlig:**

| Tema | Krav |
|---|---|
| Norm for informasjonssikkerhet i helse- og omsorgssektoren | Følge gjeldende krav i Norm for informasjonssikkerhet i helse- og omsorgssektoren (Normen). |
| Sikring av data | Ha systemer og rutiner som beskytter data under transport, bruk og lagring, slik at informasjonens konfidensialitet og integritet blir ivaretatt. |
| Internkontroll | Føre og vedlikeholde en oversikt over alle opplysninger og behandlinger eller dersom det er relevant, protokoll over sine egne behandlingsaktiviteter i henhold til personvernforordningen artikkel 30. |
| Autentisering | Sikre at all tilgang til tjenesten forutsetter tjenstlig behov og skal være rollebasert på brukernivå. Autentisering av brukere gjøres ved bruk av flerfaktorautentisering. |

| | |
|---|---|
| Tjenestenektangrep | Sørge for at systemene er beskyttet med antivirusprogram og brannmur, i tillegg til at de skal være gjenstand for regelmessige oppdateringer. |
| Logging og sporbarhet | Sørge for at alle oppslag som foretas registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos databehandler, underleverandører og Behandlingsansvarlig). |
| Redundans og skalering | Ha en infrastruktur som sikrer kapasitet og oppetid i tråd med avtalt tjenestenivå gjennom tiltak som redundans og skalering. |
| Backup og restore | Ha forsvarlige backup- og restorerutiner som testes og evalueres regelmessig. |
| Kryptering ved lagring | Kryptere data ved lagring. |
| Kryptering i kommunikasjon | Kryptere data under kommunikasjon og overføring. |

## 3. Bistand til behandlingsansvarlig

Databehandleren skal i den grad det er mulig – i det nedenfor beskrevne omfang og utstrekning – bistå den behandlingsansvarlige i samsvar med DBA ved å gjennomføre følgende tekniske og organisatoriske tiltak:

- Prosedyrer eller tekniske løsninger for å hjelpe den behandlingsansvarlige med å hente ut informasjon i et lett lesbart format som lar den behandlingsansvarlige redigere innholdet ved tilgangsforespørsler.
- Prosedyrer og tekniske løsninger for retting eller sletting av personopplysninger.
- Prosedyrer eller tekniske løsninger som tillater flagging av utvalgte personopplysninger for begrensning av behandling.
- Prosedyrer for å informere eventuelle underdatabehandlere om retting eller sletting av personopplysninger og etablering eller opphevelse av begrensninger for behandling.
- Prosedyrer for å sikre at beslutninger om videre behandling av mottatte varsler alltid tas av en fysisk person, slik at slike avgjørelser ikke kun baseres på automatisert behandling.

## 4. Sletting og oppbevaring

Ved opphør av databehandlertjenestene skal databehandleren slette og levere tilbake personopplysningene i overensstemmelse med DBA punkt 15.

## 5. Instruks for overføring av personopplysninger til tredjeland

Behandlingsansvarlig har godkjent at personopplysninger kan overføres til tredjeland (land utenfor EØS), herunder til underleverandører som benyttes av databehandler, forutsatt at ett av følgende overføringsgrunnlag i henhold til personvernforordningen kapittel V er oppfylt:

- Det foreligger en adekvansbeslutning fra EU-kommisjonen i henhold til artikkel 45, som fastslår at mottakerlandet har et tilstrekkelig beskyttelsesnivå.
- Det er inngått standard personvernbestemmelser (SCC) vedtatt av EU-kommisjonen i henhold til artikkel 46 nr. 2 bokstav c.
- Det benyttes bindende virksomhetsregler (BCR) godkjent i henhold til artikkel 47, dersom overføringen skjer internt i en konsernstruktur.
- Det foreligger et gyldig unntak i henhold til artikkel 49, for eksempel uttrykkelig samtykke fra den registrerte eller at overføringen er nødvendig for oppfyllelse av en kontrakt.

Ved bruk av SCC eller andre garantier i henhold til artikkel 46, skal databehandler utføre en overføringsvurdering (Transfer Impact Assessment – TIA) for å vurdere om lovgivningen i mottakerlandet tillater effektiv etterlevelse av garantiene. Resultatet skal dokumenteres og gjøres tilgjengelig for behandlingsansvarlig på forespørsel.

Ved bruk av underdatabehandleren Haselt benyttes SCC som overføringsgrunnlag. Dette er regulert i databehandleravtalen mellom Haselt og databehandler.

## 6. Underretning om brudd

Databehandler skal umiddelbart underrette behandlingsansvarlig dersom:

- Det skjer brudd på personopplysningssikkerheten
- Databehandler mener at en instruks fra behandlingsansvarlig er i strid med gjeldende regelverk
- Det skjer et forsøk på ikke- autorisert tilgang

I slike tilfeller skal databehandler utarbeide en beskrivelse av hendelsen, som blant annet skal inkludere tidspunktet for når hendelsen inntraff, hvordan den ble oppdaget, og hvilke systemer eller tjenester som er berørt eller kunne ha blitt berørt. Det skal også opplyses hvilke typer personopplysninger som er involvert, herunder om det dreier seg om særlige kategorier av opplysninger, og dersom relevant, et estimat over antall registrerte og datasett som er påvirket.

Videre skal databehandler gi en vurdering av de sannsynlige konsekvensene for de registrerte, herunder mulige risikoer for deres rettigheter og friheter. Det skal også redegjøres for hvilke tekniske og organisatoriske tiltak som er iverksatt for å begrense skadevirkningene og for å forhindre at lignende hendelser oppstår i fremtiden.

Relevante logger og annen dokumentasjon som kan belyse hendelsen, skal gjøres tilgjengelig for behandlingsansvarlig. I tillegg skal navn og kontaktinformasjon til en ansvarlig kontaktperson hos databehandler oppgis, slik at denne kan bistå i eventuell dialog med tilsynsmyndigheten.

## 7. Prosedyrer for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av behandlingen av personopplysninger som er overlatt til databehandleren

I samsvar med artikkel 24 og 28 i GDPR har den behandlingsansvarlige rett og plikt til å føre tilsyn med databehandleren og den behandling av personopplysninger som skjer på vegne av den behandlingsansvarlige.

Den behandlingsansvarliges tilsyn med databehandleren kan utføres ved at behandlingsansvarlig utfører en egenkontroll, skriftlig veiledning, eller fysisk inspeksjon.

Ved egenkontroll skal den behandlingsansvarlige gis innsyn i og tilgang til helse- og personopplysninger so behandles hos databehandleren på vegne av behandlingsansvarlig, samt annen samt annen dokumentasjon som er nødvendig for å gjennomføre egenrevisjon.

Ved skriftlig tilsyn og fysiske inspeksjoner kan den behandlingsansvarlige velge å gjennomføre en revisjon enten som en skriftlig revisjon eller ved fysisk inspeksjon. Revisjonen kan utføres av behandlingsansvarlig selv og/eller i samarbeid med tredjepart. En revisjon skal baseres på de sikkerhetstiltak som er avtalt mellom partene, databehandlerens etterlevelse av instruksen, herunder bruk av underbehandlere, og oppfyllelse av avtalt bistand til behandlingsansvarlig.

Ved forespørsel om gjennomføring av skriftlig tilsyn eller fysisk kontroll skal det til enhver tid gjeldende skjema fra databehandler benyttes.

Prosedyre og rapportering for skriftlig tilsyn eller fysisk inspeksjon:

- Den behandlingsansvarlige fyller ut tilsynsskjemaet.
- Den behandlingsansvarlige sender det utfylte skjemaet til databehandleren på e-post og ber om gjennomføring av revisjonen og/eller inspeksjonen.
- Databehandler bekrefter mottak og oppgir siste dato for gjennomføring av re-visjon og/eller inspeksjon.
- Utførelse av revisjon og/eller inspeksjon finner sted.
- Behandlingsansvarlig skal utarbeide en rapport, som deretter sendes til databehandler. Rapporten skal utarbeides på grunnlag av databehandlers mal for dette formålet.
- Databehandleren gjennomgår rapportutkastet og kommenterer eventuelle observasjoner fra behandlingsansvarlig (kan gjentas flere ganger).
- Sluttrapporten avsluttes av behandlingsansvarlig.
- Tilsynet er avsluttet.

Ved fysisk inspeksjon skal den behandlingsansvarlige/eller representant for den be-handlingsansvarlige som deltar i inspeksjonen være underlagt databehandlerens generelle sikkerhetstiltak og signere en konfidensialitetsavtale databehandleren i samsvar med vanlig praksis.

Den behandlingsansvarlige eller dennes representant kan da gis adgang til å foreta fysiske inspeksjoner av lokalene hvor databehandleren utfører behandlingen av personopplysninger samt de systemer som brukes til eller i forbindelse med behandlingen.

## 8. Prosedyrer for revisjoner, herunder inspeksjoner, av behandlingen av personopplysninger som er overlatt til underdatabehandleren

Databehandleren skal for egen regning gjennomføre årlig kontroll av underdatabehandleres overholdelse av GDPR, personvernregelverket for øvrig og DBA, når det gjelder de behandlingsaktivitetene som utføres av en underdatabehandler for databehandleren.

Tilsyn med underbehandlerne som benyttes av databehandleren utføres således av databehandleren, som fastsetter fremgangsmåte og hyppighet.

Den behandlingsansvarlige kan imidlertid – dersom det anses nødvendig – velge å iverksette og/eller delta i et skriftlig tilsyn eller en fysisk inspeksjon hos underdatabehandleren. Dette kan bli aktuelt dersom behandlingsansvarlig vurderer at databehandlers inspeksjon av underdatabehandler ikke har gitt behandlingsansvarlig tilstrekkelig sikkerhet for at behandlingen hos underdatabehandler er utført i samsvar med GDPR, personvernregelverket for øvrig og DBA. Tilsyn med underdatabehandler skal utføres i henhold til underdatabehandlers fastsatte vilkår for tilsyn og kontroll.

Enhver deltakelse fra den behandlingsansvarliges side i en revisjon eller inspeksjon av underdatabehandleren, skal ikke endre det faktum at databehandleren skal forbli ansvarlig for underdatabehandlerens overholdelse av GDPR, personvernregelverket for øvrig og DBA.

Den behandlingsansvarliges initiativ og/eller deltakelse i revisjon eller tilsyn i relasjon til en underdatabehandler skal gjøres i samsvar med prosedyren fastsatt i punkt 7.

Databehandler og underdatabehandler skal ha rett til godtgjørelse for den behandlingsansvarliges utøvelse av tilsyn og revisjon hos underdatabehandler når den behandlingsansvarlige har igangsatt og/eller deltatt i slikt tilsyn eller revisjon. Godtgjørelsen skal beregnes på grunnlag av medgått arbeidstid og gjeldende timepriser for databehandler og underbehandler, pluss dekke eventuelle kostnader som påløper i den forbindelse.

## 9. Kostnader ved bistand

### 9.1 Bistand

Databehandleren skal ha rett til godtgjørelse for bistand i henhold til de bistandstjenester som er avtalt i DBA punkt 12.

Godtgjørelsen beregnes på grunnlag av medgått arbeidstid og databehandlers gjeldende timepriser, med tillegg av eventuelle positive kostnader som påløper, inkludert kostnader som skal betales av databehandleren for bistand fra underbehandlere.

Dersom databehandlers bistand fører til krav om innskjerping av de sikkerhetstiltak som er fremgår av DBA, skal databehandleren, så langt det er mulig, iverksette slike ekstra sikkerhetstiltak etter skriftlig avtale med den behandlingsansvarlige, forutsatt at databehandler mottar godtgjørelse for dette.

### 9.2 Gjennomføring av andre sikkerhetstiltak

Dersom den behandlingsansvarliges krav eller databehandlers løpende vurderinger fører til en skjerping av kravene til sikkerhetstiltak i forhold til det som er avtalt, skal databehandleren iverksette og gjennomføre slike ytterligere sikkerhetstiltak som er avtalt med den behandlingsansvarlige, forutsatt at databehandler mottar godtgjørelse for dette.

### 9.3 Tilsyn og revisjon

Databehandler skal ha krav på godtgjørelse for den behandlingsansvarliges utøvelse av tilsyn og revisjon hos databehandleren. Godtgjørelsen skal beregnes på grunnlag av medgått arbeidstid og databehandlers gjeldende timepriser. I tillegg kan databehandler kreve dekket eventuelle kostnader som påløper, herunder kostnader som er påløpt i forbindelse med bistand fra underdatabehandlere.

## 10. Ansvar

### 10.1 Mislighold og erstatning

Databehandleren er kun ansvarlig for overtredelsesgebyrer, erstatningskrav, sanksjoner eller andre økonomiske tap som følge av brudd på DBA og gjeldende personvernregler, i den utstrekning bruddet utelukkende skyldes forhold databehandleren selv er ansvarlig for. Databehandlerens ansvar er begrenset til dokumenterte direkte tap og omfatter ikke indirekte tap, herunder tapt fortjeneste, med mindre annet følger av ufravikelig lovgivning.

Databehandleren har rett til å kreve erstatning for økonomisk tap som følge av behandlingsansvarliges mislighold av DBA og gjeldende personvernregler, herunder både brudd og unnlatelser, forsømmelser eller passivitet. Dette inkluderer, men er ikke begrenset til, overtredelsesgebyrer, tredjepartskrav, håndtering av klager, myndighetsdialog og andre konsekvenser av forhold som kan tilskrives behandlingsansvarlig. Retten til erstatning gjelder også dersom databehandleren blir holdt ansvarlig overfor registrerte, eller tilsynsmyndigheter for forhold som skyldes behandlingsansvarliges forhold.

Dersom en av partene blir ilagt overtredelsesgebyr, erstatningsplikt eller annen sanksjon som følge av forhold den andre parten er ansvarlig for, kan den påkrevde parten kreve regress for hele eller deler av det økonomiske tapet.

Databehandlers totale ansvar for forhold knyttet til DBA og/eller GDPR er uansett begrenset til NOK 50 000,-.

### 10.2 Krav fra registrerte

Dersom databehandler har utbetalt erstatning, kompensasjon eller andre beløp til registrerte med hjemmel i GDPR artikkel 82 eller annet rettslig grunnlag, og det forhold som utløste kravet ikke helt eller delvis kan tilskrives databehandlerens handlinger eller unnlatelser, skal databehandler ha ubetinget rett til fullt regresskrav overfor behandlingsansvarlig for det totale beløp som er utbetalt.

### 10.3 Varslingsplikt

Partene forplikter seg til å varsle hverandre uten ugrunnet opphold dersom det oppstår forhold som kan utløse sanksjoner, erstatningskrav eller annen form for ansvar. Partene skal samarbeide lojalt for å håndtere slike situasjoner, inkludert informasjonsutveksling, dokumentasjon og dialog med relevante myndigheter.

## VEDLEGG 3 – GODKJENTE UNDERDATABEHANDLERE

### 1. Underdatabehandlere

Den behandlingsansvarlige godkjenner bruken av følgende underdatabehandlere:

| Navn på underdatabehandler | Beskrivelse av behandlingen | Stedlig plassering |
|---|---|---|
| HF DATA SERVICE, | Leverer tjenester innenfor utvikling, support og implementeringsarbeid knyttet til behandlingsansvarliges skylagringssystem og eventuelle tilleggsfunksjoner, samt databaser.<br><br>Underdatabehandler behandler personopplysninger som angitt i Vedlegg 1 punkt 3.<br><br>Personopplysningene behandles ved at ansatte hos underdatabehandler får midlertidig tilgang til behandlingsansvarliges databaser, skylagringssystem og tilleggsfunksjoner i den grad det er nødvendig for å utføre ovennevnte oppgaver. | Tromsø, Norge |
| Microsoft Corporation | Leverandør og administrasjon, teknisk integrasjon og support av Microsofttjenester, som bl.a. CRM, MS360, Sharepoint og Azure.<br><br>Underdatabehandler behandler personopplysninger som angitt til i Vedlegg 1 punkt 3.<br><br>Personopplysningene innsamles, registreres og lagres i Microsoft Azure, inkludert Microsoft Dynamics CRM, hvor supporthenvendelser registreres og håndteres for å sikre effektiv kundeservice og oppfølging. | Stavanger Norge og EU/EØS |
| Visma Enterprise AS | Leverandør av regnskaps- og lønnssystem, samt Vismalink.<br><br>Behandlingen inkluderer innsamling, lagring, registrering og overføring av personopplysninger som er nødvendige for å levere regnskaps- og lønnstjenester til behandlingsansvarlig.<br><br>Visma Link benyttes som en tjeneste for sikker kommunikasjon mellom helseaktører via Norsk Helsenett, hvor personopplysninger overføres kryptert.<br><br>Underdatabehandler behandler navn, tlf.nr, postadresse, mailadresse, kontonummer til behandlingsansvarliges kunder og ansatte. Navn og kontaktinfo til ansatte hos behandlingsansvarlig som bruker systemet. Samt person- og helseopplysninger som deles via Visma Link med Norsk Helsenett. | EU/EØS, inkludert Norge, Sverige og Nederland |

| | | |
|---|---|---|
| Flexon AS | Leverer tjenester innen utvikling, support og implementeringsarbeid knyttet til integrasjon/samhandling mellom Journalsystemet og 3. parts regnskapssystemer.<br><br>Personopplysninger behandles ved at regnskapsopplysninger tilhørende Behandlingsansvarlig og deres pasienter/brukere overføres til et eksternt regnskapssystem for bokføring og videre behandling.<br><br>Underdatabehandler behandler navn, tlf.nr, postadresse, mailadresse, kontonummer til behandlingsansvarliges kunder og ansatte. Navn og kontaktinfo til ansatte hos behandlingsansvarlig som bruker systemet. Samt person- og helseopplysninger som er tilgjengelig i Journalsystemet. | Asker, Norge |
| Haselt | Teknisk støtte, utvikling, analyser og vedlikehold av skytjenesten. Tilgangen til skytjenesten er begrenset til fjerntilgang. Slik adgang gis kun i den grad det er nødvendig for å utføre teknisk støtte, utvikling eller vedlikehold av tjenesten, og etter forespørsel fra databehandler. Det ytes dermed ingen daglige tjenester fra underdatabehandler som en del av leveransen til behandlingsansvarlig. Underdatabehandler skal ikke gjøre noen fysiske overføringer av persondata ut av Journalsystemet.<br><br>Ved eventuell tilgang har underdatabehandler midlertidig tilgang til personopplysninger som angitt i Vedlegg 1 punkt 3. | Skopje, Nord Makedonia |
| Planmeca OY | Drift av interne IT-tjenester.<br><br>Personopplysninger behandles i forbindelse med drift av intern IT-infrastruktur hos Databehandler. Underdatabehandler vil i den forbindelse kunne få tilgang til personopplysninger som en del av drifts- og vedlikeholdsoppgavene de utfører.<br><br>Underdatabehandler behandler personopplysninger som angitt i Vedlegg 1 punkt 3. | Finland |
| Puzzel AS | Telefonsystem for kundehåndtering knyttet til support tjenester.<br><br>Personopplysninger behandles når behandlingsansvarlig tar kontakt via telefonsystemet for support, ved at samtaler loggføres og kontaktinformasjon registreres for å kunne håndtere henvendelser på en sikker og effektiv måte.<br><br>Underdatabehandler behandler navn, tlf.nr, e-postadresse, og annen kontaktinformasjon tilhørende behandlingsansvarlig og deres ansatte. | U/EØS, inkludert Norge. |

| | | |
|---|---|---|
| Norsk Helsenett | Forvalter og drifter Helsenettet, som er et kommunikasjonssystem mellom virksomheter i helse- og omsorgssektoren og virksomheten innenfor helse- og omsorgsforvaltningen.<br><br>Personopplysninger overføres, registreres og lagres i Norsk Helsenett ved elektronisk kommunikasjon mellom helseaktører.<br><br>Underdatabehandler behandler personopplysninger som angitt i Vedlegg 1 punkt 3. | Norge |
| Link Mobility AS | Leverandør av SMS- tjeneste.<br><br>Personopplysninger samles inn, lagres og registreres for å sende meldinger fra journalsystemet til pasienter og eventuelt andre brukere av systemet (foresatte og fullmektiger, samt ansatte hos behandlingsansvarlig).<br><br>Underdatabehandler behandler navn, og tlf. nr. til pasienter og andre brukere, i tillegg til opplysninger som fremgår av SMSen (tidspunkt for timeavtale og navn på behandler/helsepersonell). | EU/EØS, inkludert Norge. |
| 21st Century Mobile Solutions AB | Leverandør av SMS- tjeneste.<br><br>Personopplysninger samles inn, lagres og registreres for å sende meldinger fra journalsystemet til pasienter og eventuelt andre brukere av systemet (foresatte og fullmektiger, samt ansatte hos behandlingsansvarlig).<br><br>Underdatabehandler behandler navn, og tlf. nr. til pasienter og andre brukere, i tillegg til opplysninger som fremgår av SMSen (tidspunkt for timeavtale og navn på behandler/helsepersonell). | EU/EØS, inkludert, Sverige. |

Ved inngåelsen av DBA har den behandlingsansvarlige godkjent bruken av ovennevnte underdatabehandlere for den behandlingsaktiviteten som er beskrevet for vedkommende. Den behandlingsansvarlige har gitt generelt samtykke til bruk av underdatabehandlere, men databehandler må varsle om bruk av nye databehandlere eller andre endringer i henhold til punkt 2 nedenfor.

## 2. Varsel for godkjennelse av underdatabehandlere

Databehandler skal varsle behandlingsansvarlig skriftlig om planlagte endringer knyttet til tillegg eller utskifting av underdatabehandlere. Varsel skal, så langt det er mulig, gis minimum 14 dager før endringen trer i kraft.

Den behandlingsansvarlige aksepterer uavhengig av ovenstående at det kan være spesielle tilfeller hvor det kan være et konkret behov for at endringer skjer med kortere varsel eller umiddelbart. I slike tilfeller vil databehandler varsle behandlingsansvarlig om endringen så snart som mulig.

Dersom den behandlingsansvarlige har innsigelser eller spørsmål til varslede endringer, skal meddeles skriftlig til databehandler senest i 7 dager etter at varselet er mottatt.