Databehandleravtale

mellom

Helsedirektoratet ("**Behandlingsansvarlig**")

(org.nr. xxx xxx xxx)

og

[Selskap] ("**Databehandler**")

(org.nr. xxx xxx xxx)

hver for seg også benevnt "**Part**" og i fellesskap "**Partene**"

1. BAKGRUNN

I henhold til pasient- og brukerrettighetsloven § 2-1b fjerde ledd har pasienter som ikke har fått nødvendig helsehjelp innen fastsatt frist rett til nødvendig helsehjelp uten opphold, om nødvendig fra privat tjenesteyter eller tjenesteyter utenfor riket.

I henhold til pasient- og brukerrettighetsloven § 2-2 annet ledd skal spesialisthelsetjenesten kontakte Helfo dersom pasienten ikke kan tilbys nødvendig helsehjelp innen fristen. I henhold til prioriteringsforskriften § 6 skal Helfo uten opphold skaffe pasienten et tilbud fra offentlig tjenesteyter eller om nødvendig fra privat tjenesteyter i riket eller om nødvendig i utlandet.

Helfo er Helsedirektoratets ytre etat, og forvalter stønad og bidrag etter Folketrygdloven kap. 5, i tillegg til å ha ansvar for tjenester som fastlegebytte, utstedelse av frikort og pasientformidling ved fristbrudd. Helsedirektoratet er eier av de nødvendige systemløsningene som tas i bruk for å videreformidle pasienter ved fristbrudd.

Helsedirektoratet har utviklet en digital løsning for varsling av fristbrudd fra spesialisthelsetjenesten til Helfo, heretter omtalt som Fristbruddsportalen. All informasjonsutveksling, kommunikasjon og saksbehandling foregår i Fristbruddsportalen. Selve arkiveringen av opplysningene skjer i eSaks/360.

2. AVTALENS FORMÅL

Databehandling i saksbehandlingssystemet Fristbruddsportalen har sin hjemmel i pasientjournalloven, og Helsedirektoratet er Behandlingsansvarlig for behandling av Personopplysninger i tilknytning til varsling av fristbrudd og videreformidling av

pasienter. [Selskap] vil behandle Personopplysninger på vegne av Helsedirektoratet for det formål å yte nødvendig helsehjelp til pasienter som ikke mottar helsehjelp fra den offentlige spesialisthelsetjenesten innen lovpålagt frist.

Partene har inngått [Rammeavtale – sett inn <navn på Hovedavtalen>, <org.nr.>, <varighet på Hovedavtalen> med mulighet for prolongering x <år><mnd>] ("**Hovedavtalen**") datert [dato]. Denne Databehandleravtalen ("**Databehandleravtalen**") regulerer all Behandling av Personopplysninger som skjer under og i tilknytning til Hovedavtalen. Databehandleren skal utelukkende Behandle de typer Personopplysninger som forutsettes av Hovedavtalen, og bare i den utstrekning det er nødvendig for å oppfylle Hovedavtalen.

Formålene med Behandlingen, kategorier av Personopplysninger og berørte Registrerte er angitt i vedlegg 1 til denne Databehandleravtalen.

3. VIRKEOMRÅDE

Denne Databehandleravtalen regulerer Partenes rettigheter og plikter i tilknytning til Databehandlers Behandling av Personopplysninger på vegne av Behandlingsansvarlig.

Databehandleravtalen skal sikre at Personopplysninger, inkludert Helseopplysninger, behandles i samsvar med:

- EUs personverndirektiv 95/46 som er implementert i norsk lov gjennom personopplysningsloven (lov av 14. april 2000 nr. 31) og personopplysningsforskriften (forskrift av 15. desember 2000 nr. 1265);

- Den nye norske personopplysningsloven som implementerer EUs personvernforordning (Regulation 2016/679) fra tidspunktet den trer i kraft;

- Den til enhver tid gjeldende versjon av Norm for informasjonssikkerhet i helse- og omsorgstjenesten (Normen) og

- Andre lover, forskrifter og retningslinjer som regulerer behandling av Personopplysninger og som gjelder i Norge.

Listen ovenfor benevnes heretter som "**Gjeldende Personvernlovgivning**".

4. DEFINISJONER

Begreper som er skrevet med stor forbokstav i denne Databehandleravtalen skal tolkes i samsvar med definisjoner som er gitt i Gjeldende Personvernlovgivning, med mindre annet fremkommer eksplisitt.

5. BEHANDLINGSANSVARLIGES PLIKTER

Behandlingsansvarlig er ansvarlig for at det foreligger et rettslig grunnlag for Behandling av Personopplysninger i tilknytning til Hovedavtalen og i henhold til denne Databehandleravtalen.

6. DATABEHANDLERENS PLIKTER

6.1 Etterlevelse av regelverket

Databehandleren skal etterleve Gjeldende Personvernlovgivning gjennom hele avtaleperioden, jf. pkt. 9.

Databehandleren skal ikke, verken ved handling eller unnlatelse, sette Behandlingsansvarlig i en situasjon hvor denne misligholder noen av bestemmelsene i Gjeldende Personvernlovgivning.

Databehandleren skal samarbeide med og yte rimelig bistand til Behandlingsansvarlig for å sikre at Behandlingsansvarlig oppfyller kravene i Gjeldende Personvernlovgivning, herunder men ikke begrenset til, bistand knyttet til oppfyllelse av Registrertes rettigheter og gjennomføringen av "Vurdering av personvernkonsekvenser" dersom relevant.

Behandlingsansvarlig har rett til innsyn i all informasjon som Databehandleren besitter på vegne av Behandlingsansvarlig, og Databehandler plikter å gi Behandlingsansvarlig tilgang til systemer som benyttes for Behandling av Personopplysninger under Hovedavtalen med mindre annet er avtalt eller følger av bindende lovgivning.

Databehandleren skal opptre i samsvar med Behandlingsansvarliges til enhver tid gjeldende rutiner og instrukser for Behandling av Personopplysninger.

6.2 Bruksbegrensninger

Databehandleren skal ikke behandle Personopplysninger utover det som kreves for å oppfylle sine forpliktelser overfor Behandlingsansvarlig i henhold til Hovedavtalen.

Databehandleren skal påse at Personopplysninger ikke utleveres til utenforstående med mindre Behandlingsansvarlig har gitt instruks om dette eller i tilfeller hvor det er pålagt ved lov.

Databehandleren får ingen rettigheter til Personopplysninger som utleveres fra Behandlingsansvarlig til Databehandleren i henhold til Hovedavtalen.

Databehandleren skal påse at alle Personopplysninger som Behandles på vegne av Behandlingsansvarlig holdes separat fra andre data som Databehandleren Behandler.

6.3 Informasjonssikkerhet

Databehandleren skal ved hjelp av organisatoriske og tekniske tiltak sørge for et sikkerhetsnivå som står i forhold til den risikoen Behandlingen representerer og som ellers tilfredsstiller krav i Gjeldende Personvernlovgivning.

Databehandleren skal på forespørsel fra Behandlingsansvarlig fremvise dokumentasjon på de tiltak som er implementert for de datasystemer som benyttes for behandling av Personopplysninger. Dokumentasjon skal også dekke rutiner for bruk av informasjonssystemet og annen informasjon av vesentlig betydning for informasjonssikkerheten.

Spesifikke sikkerhetskrav som får anvendelse for Databehandler er opplistet i Vedlegg 1.

6.4 Avvik

Bruk av informasjonssystemet som ikke er i samsvar med etablerte rutiner, instrukser fra Behandlingsansvarlig eller Gjeldende Personvernlovgivning, inkludert brudd på personopplysningssikkerheten og andre sikkerhetsbrudd, skal behandles som avvik.

Databehandleren skal ha på plass rutiner og systematiske prosesser for å følge opp avvik, som skal omfatte gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentakelse.

Databehandleren skal uten ugrunnet opphold etter at avviket ble oppdaget, rapportere avviket til Behandlingsansvarlig. Meldingen skal inneholde den informasjonen som er påkrevet i henhold til Gjeldende Personvernlovgivning. Databehandleren skal også yte rimelig bistand til Behandlingsansvarlig slik at Behandlingsansvarlig settes i stand til å oppfylle sine forpliktelser til å rapportere avviket videre til tilsynsmyndigheter og Registrerte, samt til å svare på eventuelle henvendelser fra tilsynsmyndigheter eller Registrerte.

6.5 Varslingsplikt

Databehandleren skal uten ugrunnet opphold etter å ha blitt klar over det aktuelle forholdet, skriftlig varsle Behandlingsansvarlig om:

(i) Enhver mistanke om at instrukser fra Behandlingsansvarlig krenker Gjeldende Personvernlovgivning;
(ii) Enhver hendelse som vesentlig hindrer Databehandlers nåtidige eller fremtidige evne til å utføre behandlingen av Personopplysninger i samsvar med denne Databehandleravtalen;
(iii) Enhver forespørsel fra myndigheter om utlevering av Personopplysninger som behandles i henhold til Databehandleravtalen, unntatt dersom slik varsling er eksplisitt forbudt i henhold til preseptorisk lovgivning;
(iv) Enhver mistanke eller oppdagelse av (a) sikkerhetsbrudd som resulterer i tilfeldig eller ulovlig ødeleggelse, tap, endring, uautorisert utlevering av eller tilgang til Personopplysninger som er sendt, lagret eller på annen måte behandlet av Databehandler under Databehandleravtalen, eller (b) annen manglende etterlevelse av Databehandlers forpliktelser; og
(v) Enhver forespørsel om innsyn i Personopplysninger som er mottatt direkte fra Registrerte eller fra tredjeparter.

Databehandler skal varsle Behandlingsansvarlig uten ugrunnet opphold dersom Databehandler ikke er, eller ikke kommer til å være, i stand til å etterleve kravene i Databehandleravtalen. Ved mottak av et slikt varsel, skal Behandlingsansvarlig ha rett til, etter eget skjønn, enten å suspendere Databehandlers rett til å behandle Personopplysninger i henhold til Databehandleravtalen inntil Databehandler er i stand til å demonstrere etterlevelse, eller å si opp Databehandleravtalen med [10] dagers skriftlig varsel.

6.6 Sikkerhetsrevisjoner

Databehandleren skal minimum årlig foreta sikkerhetsrevisjoner av systemer og utstyr som benyttes for oppfyllelse av Hovedavtalen. Den behandlingsansvarlige skal kunne gis innsyn i sikkerhetsrevisjonen.

6.7 Bruk av underleverandører

Hvis Databehandler ønsker å engasjere en underleverandør skal Databehandler skriftlig varsle Behandlingsansvarlig om endringen minimum 3 måneder før den iverksettes. Behandlingsansvarlig skal svare på henvendelsen fra Databehandler senest 1 måned etter at skriftlig varsel er mottatt om endringen aksepteres eller ikke. Hvis Behandlingsansvarlig ikke aksepterer endringen, og Databehandler ikke med rimelighet kan tilby et annet alternativ, kan Behandlingsansvarlig si opp Hovedavtalen med umiddelbar virkning.

Dersom Databehandleren senere benytter underleverandører eller andre som ikke er ansatt hos Databehandleren, må det inngås avtale med den aktuelle Databehandleren hvor Databehandleren pålegges de samme plikter som er angitt i denne Databehandleravtalen. Databehandleren er fullt ut ansvarlig overfor Behandlingsansvarlig for handlinger eller unnlatelser begått av en underleverandør.

6.8 Overføring av personopplysninger

Databehandleren skal ikke overføre Personopplysninger til et land utenfor EØS-området, som ikke er ansett for å gi tilstrekkelig beskyttelse i henhold til Gjeldende Personvernlovgivning ("Tredjeland"), uten skriftlig forhåndssamtykke fra Behandlingsansvarlig.

6.9 Taushetsplikt

Databehandleren har taushetsplikt vedrørende Personopplysninger og andre data som Databehandleren Behandler i tilknytning til Hovedavtalen. Det betyr at Databehandleren ikke skal utlevere Personopplysninger eller andre data som Behandles under Hovedavtalen til tredjeparter uten Behandlingsansvarliges samtykke, med unntak av lovpålagt utlevering til myndigheter.

Databehandleren skal påse at alt personell, herunder hos underleverandører, er kjent med taushetsplikten under denne Databehandleravtalen. Dersom Databehandlers personell ikke er bundet av lovbestemt taushetsplikt, skal Databehandleren sørge for at aktuelt personell undertegner taushetserklæring.

Denne bestemmelsen gjelder også etter opphør av Databehandleravtalen og/eller Hovedavtalen.

7. MISLIGHOLD

Ved brudd på denne Databehandleravtalen eller Gjeldende Personvernlovgivning, skal Databehandleren umiddelbart stanse Behandlingen av Personopplysninger eller bestemte Behandlinger dersom Behandlingsansvarlig krever det.

Dersom Databehandler på et vesentlig punkt bryter denne Databehandleravtalen eller Gjeldende Personvernlovgivning, har Behandlingsansvarlig rett til å si opp Hovedavtalen med umiddelbar virkning.

8. SKADESLØSHOLDELSE

Hvis Behandlingsansvarlig blir holdt ansvarlig for et brudd på Gjeldende Personvernlovgivning, som er forårsaket av Databehandler og/eller dennes underleverandører, skal Databehandler holde Behandlingsansvarlig skadesløs for enhver kostnad, avgift, administrativ bot, skade, utgifter og/eller tap som har oppstått, forutsatt at:

a) Behandlingsansvarlig varsler Databehandler om kravet innen rimelig tid,
b) Databehandleren får kontroll over forsvaret av kravet og forhandlingene knyttet til en potensiell avgjørelse av kravet; og
c) Behandlingsansvarlig samarbeider med Databehandler i prosessen som knytter seg til forsvaret og avgjørelsen av kravet på Databehandlerens kostnad.

Databehandler skal ha bevisbyrden med hensyn til å bevise at Databehandler ikke har forårsaket bruddet på Gjeldende Personvernlovgivning.

9. VARIGHET OG OPPHØR

Denne Databehandleravtalen gjelder fra tidspunktet Hovedavtalen er signert av begge parter og opphører samtidig med Hovedavtalen, med unntak av bestemmelser som i henhold til Hovedavtalen eller Databehandleravtalen fortsatt skal gjelde.

Ved opphør av Databehandleravtalen skal Databehandleren og dennes underleverandører stoppe Behandlingen av Personopplysninger på vegne av Behandlingsansvarlig. Bevaring og sletting av data skal være i tråd med bestemmelsene i pasientjournalloven og tilhørende forskrift.

Databehandleren plikter å sjekke og dokumentere at ovennevnte krav også er overholdt av eventuelle godkjente underleverandører.

10. LOVVALG OG VERNETING

Databehandleravtalen er underlagt norsk rett.

Dersom Partene i tilfelle av en tvist ikke kan finne en løsning ved hjelp av forhandlinger, skal tvisten løses for de ordinære domstoler. Oslo tingrett avtales som verneting.

Sted/dato	Sted/dato
Signatur Behandlingsansvarlig	Signatur Databehandler
[navn, stilling, Selskap]	[navn, stilling, Selskap]
---	---

VEDLEGG 1

Dette vedlegget representerer Behandlingsansvarliges ytterligere instruksjoner til Databehandler i tilknytning til Databehandlers Behandling av Personopplysninger for Behandlingsansvarlig, og er en integrert del av Databehandleravtalen.

a) Behandlingens formål og karakter

- Helfo tildeler en pasient til avtaleparten
- Formidling av helseopplysninger

b) Kategorier av registrerte

- Pasienter med rett til nødvendig helsehjelp i spesialisthelsetjenesten etter pasient- og brukerrettighetsloven § 2-1b som ikke har fått oppfylt sine rettigheter innen fristen.

c) Kategorier av Personopplysninger

- Navn på pasient
- Fødselsnummer
- Telefonnummer
- Adresse (hentes fra PREG)
- Henvisning

d) Spesielle opplysningskategorier

- Helseopplysninger i form av datoer knyttet til henvisning, ICD-10 eller ICPC-2 kode, fritekstfelt for utfyllende informasjon til helseopplysninger, navn og arbeidssted på henviser, navn på pasientens opprinnelige behandlingssted, henvisning sendt til opprinnelig behandlingssted.

e) Særlige sikkerhetstiltak som får anvendelse for Databehandler

Databehandler skal ha på plass sikkerhetstiltak som er adekvate sett i forhold til den risikoen Behandlingen av Personopplysninger på vegne av Behandlingsansvarlig representerer. Dette inkluderer, blant annet, følgende tiltak og rutiner:

- Ha etablert en sikkerhetsorganisasjon med klare ansvarsområder;

- Kunne vise til en sikkerhetsstrategi;

- Kunne dokumentere at krav til personvern og konfidensialitet er oppfylt med hensyn til de ansatte og andre mottakere av Personopplysninger;

- Tilgangskontroll til systemer og data for å sikre at bare ansatte med et arbeidsrelatert behov for tilgang til Personopplysninger har tilgang

- Tilgangskontroll til bygninger og utstyr for å sørge for at bare ansatte med et arbeidsrelatert behov for tilgang, har tilgang;

- Benytte verktøy for virusbeskyttelse, spam-filtre og brannmurer når dette er nødvendig eller påkrevet;

- Logge alle kritiske systemoperasjoner;

- Kryptere kommunikasjon dersom det er nødvendig eller påkrevet i henhold til Gjeldende Personvernlovgivning. Helseopplysninger skal alltid krypteres ved forsendelse til annen mottaker.

- Ha etablerte prosedyrer for sletting og anonymisering av Personopplysninger;

- Ha etablerte prosedyrer for lagring og avhendelse av datamedium;

- Ha systemer for backup/gjenopprettingsprosess for alle kritiske systemer og gjenopprettingstester;

- Lære opp ansatte om informasjonssikkerhet og personvern; og

- Leverandørstyring vedrørende informasjonssikkerhetskrav.

Databehandler skal kunne dokumentere tiltakene som er opplistet ovenfor så langt Gjeldende Personvernlovgivning krever dette. Dokumentasjonen skal være tilgjengelig for Behandlingsansvarlig på forespørsel.