



Nordland
FYLKESKOMMUNE

DATABEHANDLERAVTALE

Mellom

Nordland fylkeskommune, org. nr. 964982953 («Behandlingsansvarlig»)

og

[INNTA DATABEHANDLER], org. nr. [xxx xxx xxx] («Databehandler»)

Datert: **xx.xx.20xx**

MÅ UTARBEIDES KONKRET FOR HVER HOVEDAVTALE

1. Avtalens bakgrunn

Behandlingsansvarlig og Databehandler, (i fellesskap «Partene»), har inngått avtale(r) om [sett inn beskrivelse av leveranse i Hovedavtalen(e) hvis relevant] («Hovedavtalen»). Denne databehandleravtalen, (heretter «Avtalen»), er inngått mellom Partene og inneholder de generelle vilkårene for den behandling av personopplysninger som Databehandler utfører på vegne av Behandlingsansvarlig. Avtalen regulerer rettigheter og forpliktelser til behandling av personopplysninger ved oppfyllelse av Hovedavtalen. Avtalen utgjør en del av Hovedavtalen. Avtalen regulerer Behandlingsansvarliges rettigheter og forpliktelser som *behandlingsansvarlig* og Databehandlers rettigheter og forpliktelser som *databehandler* når Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig.

2. Avtalens formål

Avtalen skal sikre at personopplysninger behandles i samsvar med de til enhver tid gjeldende krav til behandling av personopplysninger, herunder EU forordning 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger («Personvernforordningen») og personopplysningsloven med tilhørende forskrifter (i fellesskap «Personvernlovgivningen»).

Begreper og definisjoner benyttet i Avtalen skal forstås på samme måte som i Personvernlovgivningen.

Avtalen har som formål å regulere Partenes rettigheter og plikter på en slik måte at Personvernlovgivningen overholdes. Ved tvil skal det tolkningsalternativet som ligger nærmest Personvernlovgivningens normalordning velges, se særlig prinsippene for behandling av personopplysninger i Personvernforordningen Artikkel 5. Databehandler skal behandle personopplysningene på den måte som er beskrevet i Avtalen, samt på annen måte etter skriftlig instruks fra eller skriftlig avtale med Behandlingsansvarlig.

Avtalen innebærer ingen endringer i de kommersielle betingelsene i Hovedavtalen. Overholdelse av Avtalen gir heller ikke partene krav på ytterligere vederlag utover det som fremkommer av Hovedavtalen. Overholdelse av Personvernlovgivningen anses priset inn i Tjenesten med mindre annet er skriftlig avtalt mellom partene.

Formålet med behandlingen, behandlingens art, de typer personopplysninger som skal behandles og kategorier av registrerte følger av Vedlegg 1 til Avtalen.

3. Omfang

Denne Avtalen kommer til anvendelse på all behandling av personopplysninger som Databehandler foretar i forbindelse med Hovedavtalen.

Denne Avtalen vil også gjelde for ytterligere behandling av personopplysninger basert på eventuelle skriftlige avtaler mellom partene som inngås i løpet av Avtalens varighetsperiode og som innebærer at Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig (heretter omtalt som «senere skriftlige avtaler mellom Partene»).

Databehandler skal ikke behandle personopplysninger som Databehandler får tilgang til i forbindelse med Hovedavtalen i større grad enn det som er nødvendig for å oppfylle Hovedavtalen, Avtalen, skriftlige instruksjoner og eventuelle senere skriftlige avtaler mellom Partene. Begrensningen i dette avsnittet gjelder ikke for personopplysninger som Databehandler er rettslig forpliktet til å behandle (for eksempel for å etterleve forpliktelser i

bokføringsloven). Før Databehandler eventuelt behandler personopplysninger den har fått tilgang til som følge av Hovedavtalen for å etterleve sine rettslige forpliktelser, skal Databehandler underrette Behandlingsansvarlig. Databehandler sin plikt til å varsle Behandlingsansvarlig gjelder likevel ikke hvor slik varsling er forbudt i medhold av Personvernlovgivningen eller annen norsk lov.

4. Databehandlers plikter

Databehandler skal ikke:

- a. behandle personopplysninger for andre formål eller i større grad enn det som følger av denne Avtalen, Hovedavtalen og eventuelle senere skriftlige avtaler mellom Partene;
- b. utlevere, overlate eller overføre personopplysninger i noen form på eget initiativ med mindre det er avtalt på forhånd med Behandlingsansvarlig eller Behandlingsansvarlig har godkjent dette skriftlig;
- c. samle inn fra eller overføre personopplysninger til en tredjepart uten eksplisitt skriftlig instruks fra Behandlingsansvarlig. Dersom Databehandler mottar henvendelser fra tredjeparter, herunder registrerte og tilsynsmyndigheter, skal Databehandler videreformidle henvendelsen til Behandlingsansvarlig så raskt som mulig. Med mindre annet er skriftlig avtalt, og så langt det er mulig, skal Behandlingsansvarlig selv ha kontakten med tredjeparter.

Databehandler skal:

- a. gjøre tilgjengelig all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i artikkel 28 er oppfylt, samt forpliktelser i dette punkt 4, bidra til revisjoner, herunder inspeksjoner, som gjennomføres av Behandlingsansvarlig eller en annen representant på fullmakt fra Behandlingsansvarlig. Dette omfatter også å gi tilgang til sikkerhetsdokumentasjon. Behandlingsansvarlig vurderer selv om hvor ofte det er nødvendig å be om tilsyn.
- b. føre protokoll (logg) over behandlingsaktiviteter denne utfører på vegne av Behandlingsansvarlig, som skal inneholde minimum den informasjon som er pålagt etter Personvernforordningen Artikkel 30. Den Behandlingsansvarlige kan til enhver tid kreve oversendt kopi av slik protokoll;
- c. gi Behandlingsansvarlig tilgang og innsyn i personopplysninger som behandles hos Databehandleren;
- d. samarbeide med og bistå Behandlingsansvarlig ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger fra den registrerte med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III;
- e. gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under Avtalen oppfyller kravene i Personvernlovgivningen, herunder kravene om informasjonssikkerhet i Personvernforordningen Artikkel 32.
- f. bistå Behandlingsansvarlig med vurdering av personvernkonsekvenser og forhåndsdrøftinger i Personvernforordningen Artikkel 35 og 36.
- g. sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Databehandlers løsninger dersom dette er relevant. Dette inkluderer å bygge inn

funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter;

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

Databehandlers bistand med ovennevnte punkter skal gjøres kostnadsfritt.

5. Taushetsplikt

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Databehandler skal sikre at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt. Databehandler skal etter anmodning fra Behandlingsansvarlig dokumentere at de autoriserte personene er underlagt slik taushetsplikt. Databehandler skal sikre at kun autoriserte personer har tilgang til personopplysningene, og at tilgangene fratas dersom autorisasjonen utløper eller av andre grunner ikke lenger gjelder for personene. Databehandler skal kun autorisere personer som av nødvendige grunner må ha tilgang til personopplysningene.

Partene har i tillegg taushetsplikt om konfidensiell informasjon knyttet til hverandres virksomhet som er formidlet i forbindelse med Hovedavtalen, Avtalen, skriftlige instruksjoner og eventuelle senere skriftlige avtaler mellom Partene.

Taushetsplikten gjelder også etter Avtalens opphør.

6. Behandlingsansvarliges rettigheter og plikter

Det er den Behandlingsansvarliges rett og plikt å bestemme hvilke formål og hvilke hjelpemidler som kan brukes i behandlingen. Behandlingsansvarlig bekrefter at dennes behandling av personopplysninger i forbindelse med Hovedavtalen er i samsvar med Personvernlovgivningen, herunder at Behandlingsansvarlig har det/de nødvendige behandlingsgrunnlagene for å behandle personopplysningene.

7. Bruk av underdatabehandler

Databehandler skal kun benytte underleverandør(er) til behandling av personopplysninger («Underdatabehandler» og «Underdatabehandlere») som er skriftlig godkjent av Behandlingsansvarlig på forhånd og som har bekreftet å gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne Avtalen oppfyller kravene i Personvernlovgivningen. Underdatabehandler skal pålegges de samme forpliktelsene som Databehandler med hensyn til vern av personopplysninger som er fastsatt i Avtalen.

Avtalens Vedlegg 3 skal være mottatt og skriftlig godkjent av Behandlingsansvarlig før data kan overføres til og behandles av den enkelte Underdatabehandler.

Behandlingsansvarlig har rett til å underkjenne valg av Underdatabehandler på saklig grunnlag.

Dersom Databehandler velger å beholde Underdatabehandler på tross av slik underkjennelse, skal Databehandler skriftlig varsle Behandlingsansvarlig. Behandlingsansvarlig har rett til å si opp Hovedavtalen og eventuelle senere inngåtte avtaler mellom Partene. Ved en eventuell oppsigelse, skal Databehandler refundere alle

forhåndsbetalte beløp knyttet til Hovedavtalen og eventuelle senere inngåtte avtaler mellom Partene som skulle leveres etter oppsigelsens ikrafttredelsesdato.

Dersom Databehandler beholder en Underdatabehandler som Behandlingsansvarlig har innsigelse mot, plikter Databehandler å sørge for at Underdatabehandleren ikke mottar personopplysninger som Databehandler behandler på vegne av Behandlingsansvarlig. På tidspunktet for Avtalens inngåelse, har Behandlingsansvarlig godkjent de Underdatabehandlere som fremgår av Avtalens Vedlegg 2. Databehandler skal påse at det til enhver tid eksisterer en oppdatert liste over godkjente Underdatabehandlere med tilsvarende informasjon som i Vedlegg 2. Den oppdaterte listen skal være tilgjengelig for Behandlingsansvarlig på forespørsel.

Overfor Behandlingsansvarlig er Databehandler fullt ut ansvarlig for alle forhold knyttet til bruk av Underdatabehandler, uavhengig av godkjenning fra Behandlingsansvarlig. Dersom Underdatabehandler ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger og kravene i Avtalen, skal Databehandler overfor Behandlingsansvarlig ha fullt ansvar for at Underdatabehandler oppfyller sine forpliktelser.

Databehandler er forpliktet til å sikre at avtalen med Underdatabehandler gir Behandlingsansvarlig rett til å gjøre krav direkte gjeldende mot Underdatabehandleren dersom Behandlingsansvarlig lider økonomisk tap som følge av Underdatabehandlerens mislighold.

8. Sikkerhet og avvik

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter Personvernlovgivningen. Databehandleren skal kunne dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på den Behandlingsansvarliges forespørsel.

Databehandler skal sørge for at det gjennomføres årlige sikkerhetsrevisjoner, fortrinnsvis ved hjelp av en tredjepart. Revisjonen bør omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak. Før gjennomføring av slik revisjon skal Behandlingsansvarlig og Databehandler avtale fordeling av ressurser og kostnader forbundet med revisjonen.

Rapport med resultat av revisjonen skal oversendes til Behandlingsansvarlig. På bakgrunn av rapporten skal Databehandler av eget tiltak iverksette utbedringer for å avhjelpe eventuelle mangler og feil i informasjonssikkerheten.

I tillegg til nevnte kontroll kan Behandlingsansvarlig avtale med Databehandler at Behandlingsansvarlig selv gjennomfører sikkerhetsrevisjon for egen kostnad. Behandlingsansvarlig, eller dennes representant, skal under Databehandlers tilsyn gis tilgang til både datasystemer og lokaler, samt mulighet til å intervju Databehandlers personell som er autorisert for arbeid med Behandlingsansvarliges systemer.

I tilfelle sikkerhets- eller personvernbrudd, skal Databehandler varsle den Behandlingsansvarlige uten ugrunnet opphold, slik at Behandlingsansvarlig kan oppfylle sitt krav etter Artikkel 33 og 34, og melde avviket innen 72 timer til Datatilsynet og umiddelbart ved høy risiko til den registrerte. Melding om brudd skal minimum inneholde:

1. Beskrivelse av 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 personopplysningstyper som er berørt,

2. Navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes,
3. Beskrivelse av de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
4. Beskrivelse av de tiltak som er truffet eller foreslått for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Dersom ikke alle opplysninger kan gis i første melding, skal opplysningene gis trinnvis så snart de foreligger.

Den Behandlingsansvarlige har ansvaret for å sende melding til tilsynsmyndighet, og Databehandler skal ikke sende slik melding eller kontakte tilsynsmyndighet uten at den Behandlingsansvarlige har gitt skriftlig instruks om dette.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes Databehandler eller dennes Underdatabehandler skal korrigeres uten kostnad for Behandlingsansvarlig. Databehandler skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring, samt dokumentere overfor Behandlingsansvarlig når tiltak er utført.

9. Overføring til tredjeland og bruk av skytjenester

Personopplysninger skal kun overføres til tredjeland etter skriftlig instruks fra Behandlingsansvarlig. Databehandler skal således ikke overføre eller la personer i tredjeland på noen måte få tilgang til personopplysninger uten at Behandlingsansvarlig har eksplisitt godkjent dette skriftlig og gitt instruks om overføring eller tilgang på forhånd. Overføring av personopplysninger til / fra land utenfor EU / EØS, som ikke er godkjente av EU-kommisjonen på tidspunktet for overføringen, regnes som overføring til tredjeland.

Databehandler og eventuelle Underdatabehandlere kan ikke benytte skytjenester dersom dette kan føre til at personopplysninger behandles i tredjeland, uten at dette er særskilt godkjent av Behandlingsansvarlig.

Reguleringen om overføring til tredjeland og bruk av skytjenester gjelder både der personopplysninger lagres på en server i tredjeland og der serveren står i Norge, men personale i et tredjeland har tilgang til personopplysningene som Databehandler behandler på vegne av Behandlingsansvarlig. Tilsvarende gjelder for innlogging via skytjenester.

Samtykke og instruks må dekke hvilke land personopplysningene 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 Personvernlovgivningen er ivarettatt.

Spørsmål om overføring til tredjeland og bruk av skytjenester skal tas opp med Behandlingsansvarlig senest tre måneder før oppstart av slik behandling. Databehandler skal fremlegge en risikovurdering for overføring eller bruk av skytjeneste. En eventuell overføring til tredjeland eller bruk av skytjenester skal være basert på EUs Standardavtale for behandling av personopplysninger utenfor EU / EØS, med mindre Behandlingsansvarlig godkjenner et annet overføringsgrunnlag.

10. Avtalens varighet, pålegg om stans, plikter ved opphør/opsigelse

Avtalen gjelder så lenge Databehandler behandler (eller har tilgang til) personopplysninger på vegne av Behandlingsansvarlig etter Hovedavtalen eller senere skriftlige avtaler mellom

Partene. Hvis hovedavtale ikke er inngått, varer behandlingen til den sies opp av en av partene.

Ved brudd på denne Avtalen, skriftlige instruksjoner eller Personvernlovgivningen, kan Behandlingsansvarlig pålegge Databehandler å stoppe videre behandling av personopplysningene med øyeblikkelig virkning.

Databehandler skal, etter den Behandlingsansvarliges skriftlige instruksjon, slette eller tilbakelevere alle personopplysninger til Behandlingsansvarlig etter at Hovedavtalen eller senere skriftlige avtaler mellom Partene er opphørt. Databehandler skal slette eventuelle kopier av personopplysningene med mindre Databehandler har en rettslig forpliktelse til å fortsette behandlingen av personopplysningene. Plikten til å slette personopplysninger omfatter også eventuelle sikkerhetskopier, men hvor det er tilstrekkelig at personopplysningene overskrives i tråd med etablerte rutiner for sikkerhetskopiering.

Behandlingsansvarlig skal motta en skriftlig bekreftelse så snart som mulig fra Databehandler om at alle personopplysninger er returnert eller slettet i henhold til den Behandlingsansvarliges skriftlige instruksjoner og at Databehandler ikke har beholdt kopi, utskrifter eller andre former for personopplysninger i noen form.

11. Erstatningsansvar

Ved mislighold av vilkårene i denne avtalen som skyldes feil eller forsømmelser fra Databehandlers side, kan behandlingsansvarlig si opp avtalen med øyeblikkelig virkning. Databehandler vil fortsatt være pliktig til å tilbakelevere og slette personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 9.

Databehandler er erstatningsansvarlig overfor de registrerte dersom feil eller forsømmelser hos databehandler påfører de registrerte økonomiske eller ikke-økonomiske tap som følge av at deres rettigheter eller personvern er krenket. Behandlingsansvarlig kan kreve erstatning for økonomiske tap som feil eller forsømmelser fra databehandlers side, inkludert mislighold av vilkårene i denne avtalen.

12. Øvrige plikter og rettigheter

Øvrige plikter og rettigheter følger av Hovedavtalen. Ved eventuell overdragelse av Hovedavtalen til andre parter, skal denne Avtalen overdras tilsvarende.

13. Endring av avtale

I tilfelle endring i gjeldende lovverk, rettskraftig dom som gir annen tolkning av Personvernlovgivningen, eller endringer i Hovedavtalen (eller senere skriftlige avtaler mellom Partene) som krever endringer av denne Avtalen, skal partene samarbeide for å oppdatere Avtalen tilsvarende.

14. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Salten tingrett som verneting. Dette gjelder også etter opphør av Avtalen.

15. Kontaktinformasjon

Alle henvendelser om denne avtalen rettes til:

Hos behandlingsansvarlig:

Navn:

Telefon:

E-post

Hos databehandler:

Navn:

Telefon:

E-post:

Avtalen foreligger i 2 – to originaler, hvorav partene beholder ett eksemplar hver.

For Databehandler:

Sted:

Dato:

For Behandlingsansvarlig:

Sted:

Dato:

Signatur:

Signatur

Vedlegg 1

Behandlingens formål: *[hver behandling skal ha klart definerte formål. Beskriv formål]*

Behandlingens art: *[Beskriv hva avtalen mellom Partene går ut på]*

Typer personopplysninger som skal behandles: *[her listes opp hvilke personopplysninger som omfattes, f.eks. navn, telefonnummer, fødselsnummer, helseopplysninger, e-postadresser o.l.]*

Kategorier av registrerte: *[her listes opp hvilke kategorier av registrerte som omfattes, f.eks. pasienter, barn, elever, foreldre, ansatte, tidligere ansatte, leverandører o.l.]*

Dataflyt *[her beskrives prosessen for dataflyt for de personopplysningene som Hovedavtalen og Avtalen regulerer) Beskrivelsen kan eventuelt dokumenteres som vedlegg til Avtalen]*

Frist for sletting eller tilbakelevering av personopplysninger som Avtalen regulerer *[Beskriv hvilke data som skal slettes og tidspunkt]*

Krav til arkivering av personopplysninger som Avtalen regulerer *[Beskriv hvilke data som er arkivpliktig]*

Vedlegg 3

Tiltredelseserklæring

Navn på selskap, organisasjonsnummer, tiltrer med dette Databehandleravtale inngått mellom Behandlingsansvarlig og Databehandler [dato xx.xx.xxxx], og betegnes som Underdatabehandler. Som Underdatabehandler til Databehandler eller noen av dennes underdatabehandlere, bekrefter vi å ha påtatt oss ansvar og forpliktelser i henhold til Databehandleravtale inngått xx.xx.xxxx, og tiltrer som Databehandler i Databehandleravtalens forstand.

Dersom Underdatabehandler etter dette vedlegg 3 benytter underdatabehandlere som skal behandle personopplysninger på vegne av Behandlingsansvarlig, blir underdatabehandleren også Databehandler i Databehandleravtalens forstand og skal tilsvarende undertegne på et likelydende bilag til Databehandleravtale.

Alle eventuelle underdatabehandlere har selvstendig ansvar og identiske forpliktelser for å oppfylle kravene i Databehandleravtalen som vi bekrefter å ha fått ulevert en kopi av. Denne avtale er i 3 – tre eksemplarer, hvorav partene har hvert sitt og hvor et eksemplar oversendes Behandlingsansvarlig i Hovedavtalen.

Sted:

Dato:

Sted:

Dato:

Databehandler

Underdatabehandler

Navn

Navn