Avtale om kommunens bruk av Modia arbeidsrettet oppfølging til behandling av personopplysninger etter sosialtjenesteloven

Databehandleravtale

mellom

Lindås kommune
(Behandlingsansvarlig)

og

Arbeids- og velferdsdirektoratet
(Databehandler)

Sign.: NEB/ TM

1. Avtalens hensikt og formål

Denne avtalen («databehandleravtalen») er en del av avtale om bruk av Modia Arbeidsrettet Oppfølging («samarbeidsavtalen») datert 16.05.2018 mellom Lindås kommune og Arbeids- og velferdsetaten ved NAV Hordaland.

Databehandleravtalen inngås mellom Hordaland kommune som «behandlingsansvarlig» og Arbeids- og velferdsetaten ved Arbeids- og velferdsdirektoratet som «databehandleren», der begge utgjør en «part», samlet benevnt som «partene».

Formålet med denne databehandleravtalen er å fastlegge partenes rettigheter og plikter vedrørende databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige i henhold til den inngåtte samarbeidsavtalen.

Med unntak for det som er spesifisert her, skal samarbeidsavtalens betingelser gjelde. I tilfelle uoverensstemmelse mellom samarbeidsavtalen og denne databehandleravtalen når det gjelder forhold spesifikt knyttet til behandling av personopplysninger, skal databehandleravtalen gis forrang.

2. Definisjoner

I denne databehandleravtalen skal følgende ord og uttrykk ha den betydning som er angitt nedenfor.

«Behandlingsansvarlig»: En fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett.

«**Databehandler**»: En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

«**Underdatabehandler**»: En annen databehandler som databehandler engasjerer for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige.

"**Personopplysninger**": Enhver opplysning om en identifisert eller identifiserbar fysisk person ("den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.

«Brudd på personopplysningssikkerheten»: Et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

«Behandling»: Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring. Det omfatter også tilgang til å se på personopplysningene, aksessere, samt aksessering fra annen lokasjon (fjernaksess), og eller mulighet til å aksessere personopplysninger, selv om denne muligheten ikke faktisk benyttes, både fra fjern og nær lokasjon.

"**Gjeldende personvernregler**": Gjeldende lover og regler om personvern, inkludert personopplysningsloven og GDPR (fra og med 25. mai 2018).

"**Standardklausuler**": Standardklausuler («Standard Contractual Clauses / EU Model Clauses») for overføring av personopplysninger til databehandlere etablert i tredjeland, etablert ved EU-kommisjonens vedtak av 5. februar 2010 og/eller som etablert av EU-kommisjonen eller en relevant tilsynsautoritet i henhold til GDPR artikkel 28(7) eller 28(8).

"**GDPR**": EUs personvernforordning 2016/679 (General Data protection Regulation).

"**Tredjestat**": Et land utenfor EØS som EU-kommisjonen ikke har fastslått sikrer et tilstrekkelig beskyttelsesnivå.

For øvrig skal ord og uttrykk ha samme mening som de er tillagt i GDPR.

3 Databehandlingens formål og omfang

Denne databehandleravtalen gjelder alle personopplysninger som databehandleren behandler på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstillinger, lagring, utlevering eller kombinasjoner av disse.

Databehandlingens formål og art, typen personopplysninger som behandles, samt kategorier av registrerte fremgår av denne avtalens Vedlegg 1 om databehandlingens omfang.

4 Databehandlers generelle plikter

Databehandleren garanterer å ha gjennomført egnede tekniske og organisatoriske tiltak som sikrer at behandlingen av personopplysningene oppfyller kravene i henhold til gjeldende personvernregler og ivaretar de registrertes rettigheter, og at disse tiltakene vil etterleves i hele avtaleperioden.

Databehandleren skal behandle personopplysningene utelukkende for det formål og innenfor det omfang som er angitt i Vedlegg 1, og for øvrig i samsvar med det som er avtalt mellom partene i samarbeidsavtalen og denne databehandleravtalen med vedlegg.

Databehandleren skal omgående underrette den behandlingsansvarlige skriftlig hvis den har rimelig grunn til å tro at

- (i) en instruks fra den behandlingsansvarlige kan medføre at databehandleren bryter med gjeldende personvernlovgivning, eller

- (ii) gjeldende rett i EØS-området krever at databehandleren behandler personopplysninger utover omfanget av den behandlingsansvarliges dokumenterte instrukser, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal databehandleren underrette den behandlingsansvarlige så snart retten tillater det).
- I tilfelle av (i) eller (ii) skal partene i god tro diskutere hvordan problemet kan løses uten at det negativt påvirker vernet av de registrertes rettigheter.

5. Bistand til den behandlingsansvarlige

Databehandler plikter å bistå den behandlingsansvarlige ved ivaretakelse av den registrertes rettigheter etter GDPR kapittel 3, som anmodninger om informasjon, innsyn, korrigering, sletting, begrensning av behandlingen, dataportabilitet, innsigelser, og det å ikke være underlagt automatiserte individuelle avgjørelser herunder profilering. Databehandleren skal umiddelbart videresende til den behandlingsansvarlige forespørsler eller klager som den eventuelt mottar fra den registrerte.

Med hensyn til behandlingens art og den informasjon som er tilgjengelig for databehandleren, skal databehandleren bistå den behandlingsansvarlige med forpliktelsene i henhold til GDPR artikkel 32 til 36, herunder forpliktelsene til datasikkerhet (som nærmere beskrevet i kap. 6), melding om brudd på personopplysningssikkerhet (som nærmere beskrevet i kap. 10), vurdering av personvernkonsekvenser, samt forhåndsdrøftinger.

Databehandleren skal ikke kommunisere direkte med tilsynsmyndigheter med mindre dette er forhåndsgodkjent av den behandlingsansvarlige. Databehandleren skal også umiddelbart videresende eventuelle forespørsler fra en tilsynsmyndighet som gjelder inspeksjoner, undersøkelser, eller tilgang til eller informasjon om personopplysninger, med mindre loven forbyr det (i så fall skal databehandleren underrette den behandlingsansvarlige så snart loven tillater det).

6. Sikkerhetstiltak

Databehandleren skal gjennomføre egnede tekniske og organisatoriske sikkerhetstiltak for å beskytte personopplysninger som omfattes av denne avtalen mot utilsiktet eller ulovlig tilintetgjøring, tap, endring, ikke-autorisert utlevering eller tilgang. Databehandleren skal som et minimum gjennomføre de tiltakene som er påkrevd i henhold til GDPR artikkel 32.

Databehandleren skal ikke utlevere personopplysninger til tredjeparter uten skriftlig forhåndsgodkjennelse fra den behandlingsansvarlige, med unntak for eventuelt godkjente underdatabehandlere (se kap. 8) i den utstrekning de har behov for opplysningene for å kunne utføre sine oppgaver.

7. Taushetsplikt

Databehandlers ansatte som er autorisert og andre som er opptrer på databehandlers vegne til å behandle personopplysninger, har taushetsplikt om informasjon og personopplysninger som vedkommende får tilgang til i henhold til denne avtalen. Taushetsplikten omfatter også ansatte hos underdatabehandler som utfører oppdrag for databehandler for å kunne levere tjenesten.

Reglene om taushetsplikt i sosialtjenesteloven § 44, arbeids- og velferdsforvaltningslovens § 7, jf. forvaltningsloven §§ 13 til 13 e, kommer til anvendelse for partene i denne avtalen og andre som partene svarer for. Taushetsplikten gjelder også opplysninger om fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bosted og arbeidssted. Om nødvendig skal det undertegnes taushetserklæring.

Taushetsplikten gjelder også etter avtalens opphør. Ansatte og andre som fratrer sin tjeneste hos databehandler skal pålegges taushet også etter fratredelse om forhold som nevnt ovenfor.

Dersom en del av databehandleroppdraget omfatter utlevering av adresseinformasjon til andre, så skal graderte adresser (adressesperre med kode 6 og 7 i folkeregisteret) ikke utleveres.

8. Ansvar for bruk av underdatabehandler

Databehandleren kan kun engasjere underdatabehandler etter særlig skriftlig tillatelse fra den behandlingsansvarlige. Denne tillatelsen skal foreligge før behandlingen av personopplysninger starter.

Databehandleren skal inngå skriftlig avtale med hver underdatabehandler som pålegger egne forpliktelser med hensyn til vern av personopplysninger. Databehandleren har fullt ansvar for underleverandørenes utførelse av sine forpliktelser på samme måte som om databehandler selv sto for utførelsen.

Samtlige som på vegne av databehandler utfører oppdrag der behandling av de aktuelle personopplysningene inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

Godkjente underdatabehandler skal angis i Vedlegg 3 om godkjente underdatabehandlere.

9. Overføring av personopplysninger til utlandet - tredjestat

Databehandleren kan kun overføre personopplysninger til en tredjestat eller en internasjonal organisasjon etter dokumenterte instrukser fra den behandlingsansvarlige. Databehandler kan imidlertid gjøre dette hvis det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal databehandler underrette den behandlingsansvarlige om nevnte rettslige krav før overføringen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal databehandleren underrette den behandlingsansvarlige så snart retten tillater dette).

Dersom bruk av en godkjent underdatabehandler krever overføring av personopplysninger til en tredjestat, og slike overføringer er godkjent av databehandleren, gir den behandlingsansvarlige databehandleren fullmakt til å inngå standardklausuler i uendret form med underleverandør på vegne av den behandlingsansvarlige dersom dette er nødvendig for å tilfredsstille krav etter gjeldende personvernregler. Så snart en slik avtale er inngått skal

underdatabehandler fremlegge en kopi av denne for den behandlingsansvarlige. Alle slike standardklausuler skal automatisk opphøre ved opphøret av denne databehandleravtalen.

10. Brudd på personopplysningssikkerheten (avvik)

Databehandleren skal gi skriftlig melding til den behandlingsansvarlige om eventuelle brudd på denne databehandleravtalen eller personopplysningssikkerheten. Meldingen skal gis senest 36 timer etter at databehandleren ble oppmerksom på bruddet.

Melding om brudd på personopplysningssikkerheten må minst, i den grad det er relevant:

a) beskrive arten av bruddet, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt;
b) inneholde, når det er mulig, de berørte registrertes identitet;
c) inneholde navn og kontaktinformasjon til personvernombudet eller et annet kontaktpunkt hos databehandleren for ytterligere innhenting av informasjon;
d) beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten;
e) beskrive de tiltak som er truffet eller foreslått for å håndtere bruddet, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger;
f) inkludere annen informasjon som kreves for at den behandlingsansvarlige kan overholde gjeldende personvernregler.

Databehandleren skal så snart som mulig gjennomføre alle tiltak som beskrevet i punkt e. ovenfor, samt gjennomføre alle de tiltak som med rimelighet kreves for å unngå at det senere oppstår lignende brudd på personopplysningssikkerheten. Databehandleren skal tillate den behandlingsansvarlige å undersøke, fastlegge årsaken til og å verifisere de tiltak som er gjennomført eller foreslått av den behandlingsansvarlige for å håndtere bruddet på personopplysningssikkerheten. Databehandleren skal, så langt det er mulig, rådføre seg med den behandlingsansvarlige med hensyn til de tiltak som skal gjennomføres samt overveie innspill fra den behandlingsansvarlige i den forbindelse.

Kun den behandlingsansvarlige har rett til å informere den relevante tilsynsmuligheten og de berørte registrerte om brudd på personopplysningssikkerheten. Databehandleren skal avstå fra å informere allmennheten eller tredjepart om brudd på personopplysningssikkerheten.

11. Revisjon

Databehandleren skal dokumentere, samt gjøre tilgjengelig for den behandlingsansvarlige, informasjon som er nødvendig for å påvise etterlevelse av denne databehandleravtalen og gjeldende personvernregler.

Databehandleren skal muliggjøre og bidra ved revisjoner av databehandlerens behandlingsaktiviteter som utføres av den behandlingsansvarlige eller av annen inspektør på fullmakt fra den behandlingsansvarlige. Databehandleren skal også muliggjøre og bidra ved revisjoner fra tilsynsmyndigheter.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandler, skal den behandlingsansvarlige informeres om dette og ha tilgang til oppsummering av revisjonsrapportene.

12. Ansvarsbegrensning

Databehandleren skal holde den behandlingsansvarlige skadesløs fra eventuelle kostnader (herunder rimelige saksomkostninger) og tap som følge av et krav fra en tredjepart (inkludert tilsynsmyndigheter og registrerte) om at behandlingen av personopplysningene innebærer brudd på gjeldende personvernregler, og kravet skyldes databehandlerens mislighold av sine forpliktelser i denne databehandleravtalen, herunder behandling av personopplysninger utover den behandlingsansvarliges skriftlige instrukser.

Skadesløsholdelsen er betinget av (i) at den behandlingsansvarlige umiddelbart varsler databehandleren om kravet, og (ii) at databehandleren får mulighet til å samarbeide med den behandlingsansvarlige i forsvaret mot og oppgjøret av kravet.

13. Endringshåndtering

Ved endringer i lover, forskrifter og lignende med relevans for databehandleravtalen, skal det vurderes om denne databehandleravtalen må revideres.

Tekniske eller andre sikkerhetsmessige endringer kan medføre at databehandleravtalen må endres. Dette vurderes fortløpende av partene. Slike endringer skal varsles den andre part uten ugrunnet opphold.

Endringer av databehandleravtalen skal avtales skriftlig og legges ved som vedlegg til denne avtalen.

14. Avtalens varighet og oppsigelse

Denne databehandleravtalen gjelder så lenge databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige i forbindelse med samarbeidsavtalen.

Ved opphør eller oppsigelse av databehandleravtalen skal databehandleren, dersom den behandlingsansvarlige ønsker det, slette eller tilbakelevere alle personopplysninger til den behandlingsansvarlige og slette eksisterende kopier, og skriftlig dokumentere overfor den behandlingsansvarlige at dette er gjort, med mindre gjeldende rett i EØS-området krever at databehandleren lagrer personopplysningene (i så fall skal databehandleren besørge sikker lagring, men ikke aktivt behandle, personopplysningene, og skal slette personopplysningene så snart loven tillater dette).

15. Lovvalg og verneting

Databehandleravtalen er underlagt norsk rett og partene vedtar Oslo Tingrett som verneting. Dette gjelder også etter opphør av avtalen.

16. Kontaktpersoner

Alle meddelelser som gis etter denne avtalen skal være skriftlig og adressert til følgende kontaktpersoner:

Kontaktperson hos Behandlingsansvarlig:	**Kontaktperson hos Databehandler:**
Navn: Leni Dale	Navn: Ragnar Thorsteinsson
Telefon: 90854464	Telefon: 97030735
E-post:leni.dale@lindas.kommune.no	E-post: nav.forenklet.oppfolging-databehandleravtale@nav.no

[signaturfelt på neste side]

Databehandleravtalen er utarbeidet i 2 – to eksemplarer, hvorav partene har hvert sitt underskreven eksemplar.

******

For og på vegne av den behandlingsansvarlige ved Lindås kommune:

Signatur: Nils E. Buck

Navn:Nils-Erik Buck, IKT-leiar

Dato: 16.05.2018

For og på vegne av databehandleren ved Arbeids- og velferdsdirektoratet:

Signatur: Tormod Moland

Navn: TORMOD MOLAND

Dato: 28.6.16

VEDLEGG 1: DATABEHANDLINGENS OMFANG

Behandlingens formål

Den digitale aktivitetsplanen er et verktøy for den arbeidsrettede oppfølgingen i NAV, jf. NAV-loven § 14 a. Aktivitetsplanen er en samhandlingsflate der både bruker og veileder kan legge til aktiviteter og starte og gjennomføre dialog om aktivitetene.

Aktivitetsplanen er tilgjengelig for innbyggerne på selvbetjeningsløsningen «Ditt NAV» via nav.no. Tilgang til den digitale aktivitetsplanen, og selvbetjeningsløsningen, forutsetter at bruker logger inn med sikker identifisering på nivå 4.

Formålet med behandlingen av personopplysningene er at deltakere i kvalifiseringsprogrammet (KVP) (etter sosialtjenesteloven §§ 29 flg.) kan bruke *digital aktivitetsplan* til arbeidsrettet oppfølging.

Behandlingens art og hensikt

Behandle personopplysninger med hjemmel i sosialtjenesteloven, for deltakere i kvalifiseringsprogrammet, i Arbeids- og velferdsetatens fagsystem *Modia arbeidsrettet oppfølging*.

Hensikten er å drive, lagre og tilby et grensesnitt for digital dialog om arbeidsrettede oppfølgingen mellom deltakere i kvalifiseringsprogrammet og Arbeids- og velferdsforvaltningen.

Kategorier av registrerte

Deltakere i kvalifiseringsprogrammet.
Veileder i Arbeids- og velferdsforvaltningen.

Typen personopplysninger

Navn, fødselsnummer/d-nummer, adresse, ansatt-id, forskjellige opplysninger gitt i fritekstfelt og variabler som angir diverse statuser under oppfølgingsløpet. Eksempler på variabler er: Start dato, stop dato, endret dato, løpenummer, tidsstempel, bolsk flagg med videre.

Komplett liste over personopplysninger finnes i den til enhver tid gjeldende personverkonsekvensvurdering for tjenesten.

Type sensitive personopplysninger

Som følge av at løsningen åpner for at både bruker og veileder kan skrive i aktivitetsfelt kan behandlingen omfatte opplysninger om rase, etnisk opprinnelse, politisk oppfatning, religion, fagforeningsmedlemsskap, helseopplysninger, opplysninger om straffedommer og lovovertredelser

VEDLEGG 2: TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Databehandleren skal som et minimum gjennomføre alle de tiltak som fremkommer av Arbeids- og velferdsforvaltningens til enhver til gjeldende felles sikkerhetsnormer og samarbeidsavtalen. Databehandleren kan ikke uten skriftlig samtykke fra den behandlingsansvarlige gjøre endringer i disse tiltakene som reduserer graden av datasikkerhet. Databehandleren skal kontinuerlig arbeide for å forbedre sikkerhetstiltakene og sørge for at de oppdateres i takt med den teknologiske utviklingen.

VEDLEGG 3: GODKJENTE UNDERDATABEHANDLER

Selskapets navn	Selskapets adresse	Behandlingssted
Bekk Consulting (utvikling)	Akershusstranda 21,0150 Oslo	Oslo
Sopra Steria (utvikling)	Biskop Gunnerus gate 14a, 0185 Oslo	Oslo