AVTALE OM WEBSAK – SYSTEM FOR ELEKTRONISK ADMINISTRATIV SAKSBEHANDLING OG ARKIV

Databehandleravtale

mellom

kommune
som Behandlingsansvarlig

og

Arbeids- og velferdsdirektoratet (NAV)
som Databehandler

Sted og dato:	Sted og dato:
For Behandlingsansvarlig	For Databehandler
_____	_____
kommune	Arbeids- og velferdsdirektoratet

Avtalen undertegnes i to eksemplarer, ett til hver part.

INNHOLDSFORTEGNELSE:

1 FORMÅLET MED DENNE DATABEHANDLERAVTALEN

1. Denne avtalen ("Databehandleravtalen") gjelder kommunalt ansattes tilgang til, og bruk av, WebSak. Avtalen er inngått mellom [redacted] kommune («Behandlingsansvarlig») og Arbeids- og velferdsdirektoratet ("Databehandler"), der begge utgjør en "Part", samlet benevnt som "Partene".

2. Databehandleravtalens hensikt er å regulere rettigheter og plikter i henhold til Europaparlamentets- og rådsforordning (EU) 2016 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, samt om oppheving av direktiv 95/46/EF (generell personvernforordning/ General Data Protection Regulation).

3. Databehandleravtalen regulerer Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig.

4. Databehandleravtalen har tre vedlegg. Vedleggene er en del av Databehandleravtalen.

5. Vedlegg 1 inneholder en beskrivelse av behandlingens omfang, formål og hensikt, type personopplysninger og kategorier av registrerte.

6. Vedlegg 2 inneholder en beskrivelse av tekniske og organisatoriske sikkerhetstiltak.

7. Vedlegg 3 inneholder en oversikt over godkjente underdatabehandlere.

2 DEFINISJONER

I Databehandleravtalen skal følgende ord og uttrykk ha denne betydning:

1. «**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 eller flere identifikatorer. Slike identifikatorer kan f.eks. være 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, se artikkel 4 nr. 1.

2. **«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. Se artikkel 4 nr. 1.

3. **«Brudd på personopplysningssikkerheten»:** 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, se artikkel 4 nr. 12.

4. «**Underdatabehandler»**: En annen databehandler eller flere (underleverandører) som Databehandler engasjerer for å utføre spesifikke behandlingsaktiviteter på vegne av Behandlingsansvarlig.

5. **«Gjeldende personvernregler»**: Gjeldende lover og regler om personvern, inkludert ny personopplysningslov og GDPR (fra og med ikrafttredelsestidspunkt).

6. «**GDPR»**: General Data Protection Regulation. Europaparlamentets- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning).

7. «**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).

8. «**Tredjestat»**: Et land utenfor EØS som EU-kommisjonen ikke har fastslått at sikrer et tilstrekkelig beskyttelsesnivå.

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

3 OMFANG AV BEHANDLINGEN

1. Databehandleravtalen gjelder alle personopplysninger som Databehandler har mottatt, er gitt tilgang til eller har genert i forbindelse med Hovedavtalen.

2. Databehandlingens formål og art, type personopplysninger som behandles, samt kategorier av registrerte fremgår av Vedlegg 1.

3. Databehandler har ikke selvstendig råderett over personopplysningene og kan ikke bruke opplysningene til andre formål enn det som fremgår av Vedlegg 1, og skal ellers behandle personopplysningene i samsvar med Behandlingsansvarliges dokumenterte instrukser.

4 GENERELLE PLIKTER

1. Databehandler plikter å ha gjennomført egnede tekniske og organisatoriske tiltak som sikrer at behandlingen av personopplysningene er i samsvar med kravene etter gjeldende personvernregler, og at disse tiltakene etterleves i hele avtaleperioden.

2. Databehandler skal omgående varsle Behandlingsansvarlig skriftlig hvis Databehandler har rimelig grunn til å tro at:

    (i) en instruks fra Behandlingsansvarlig kan medføre at Databehandler bryter med gjeldende personvernlovgivning, eller

(ii) gjeldende rett i EØS-området krever at Databehandler behandler personopplysninger utover omfanget av Behandlingsansvarliges dokumenterte instrukser.

I tilfelle av (i) eller (ii) skal Partene diskutere hvordan problemet kan løses uten at de registrertes rettigheter blir krenket.

3. Hvis Databehandler er underlagt godkjente adferdsnormer etter GDPR artikkel 40 eller en godkjent sertifiseringsmekanisme etter GDPR artikkel 42, garanterer Databehandler at den vil etterleve slike atferdsnormer eller sertifiseringsmekanismer.

4. Dersom Databehandler er underlagt plikt om protokollføring som fremgår av GDPR artikkel 30 skal Databehandler føre skriftlig protokoll over alle kategorier av behandlingsaktiviteter som utøves på vegne av Behandlingsansvarlig.

5 BISTAND TIL BEHANDLINGSANSVARLIG

1. Databehandler plikter å bistå Behandlingsansvarlig ved ivaretakelse av registrertes rettigheter etter GDPR kapittel III som inkluderer:
   a) retten til informasjon ved innsamling av personopplysninger fra den registrerte
   b) retten til informasjon hvis opplysningene innhentes fra andre enn registrerte
   c) retten til å kreve innsyn i egne personopplysninger
   d) retten til å kreve korrigering eller sletting av egne opplysninger
   e) retten til å kreve at behandlingen av egne personopplysninger begrenses
   f) retten til dataportabilitet
   g) retten til innsigelse
   h) retten til å motsette seg automatiske avgjørelser inkludert profilering

   Databehandler skal umiddelbart videresende til Behandlingsansvarlig forespørsler eller klager som Databehandler eventuelt mottar fra den registrerte.

2. Databehandleren skal så langt det er mulig bistå Behandlingsansvarlig med forpliktelsene etter GDPR artikkel 32 til 36, herunder forpliktelsene til datasikkerhet (se avtalens punkt 6), melding om brudd på personopplysningssikkerhet (se avtalens punkt 10), vurdering av personvernkonsekvenser samt forhåndsdrøftinger med Datatilsynet.

6 TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

1. Databehandler skal gjennomføre egnede tekniske, fysiske og organisatoriske sikkerhetstiltak for å beskytte personopplysninger som omfattes av Databehandleravtalen mot utilsiktet eller ulovlig tilintetgjøring, tap, endring og ikke-autorisert utlevering eller tilgang. Databehandleren skal som et minimum gjennomføre de tiltakene som er påkrevd i henhold til GDPR artikkel 32, samt de tiltak som er angitt eller referert til i Vedlegg 2.

2. Databehandler skal ikke utlevere personopplysninger til tredjeparter uten skriftlig forhåndsgodkjenning fra Behandlingsansvarlig. Unntak gjelder for eventuelle godkjente underdatabehandlere (se avtalens punkt 8) når de har behov for opplysningene for å kunne utføre sine oppgaver.

3. Databehandler sikrer, at kun de personer som er autorisert til å behandle personopplysninger, har tilgang til personopplysningene som behandles på vegne av Behandlingsansvarlig.

7 TAUSHETSPLIKT

1. Databehandlers ansatte og andre som opptrer på Databehandlers vegne, har taushetsplikt om informasjon og personopplysninger som vedkommende får tilgang til etter Databehandleravtalen. Taushetsplikten omfatter også ansatte hos underdatabehandler som utfører oppdrag for Databehandler for å kunne levere tjenesten.

2. Ansatte og andre hos Databehandler pålegges taushetsplikt etter reglene i arbeids- og velferdsforvaltningsloven § 7, jf. forvaltningsloven §§ 13 til 13 e. Taushetsplikten omfatter også opplysninger om fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bosted og arbeidssted, jf. arbeids- og velferdsforvaltningsloven § 7, første ledd. NAVs taushetsplikterklæring skal undertegnes.

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

8 BRUK AV UNDERDATABEHANDLERE

1. Databehandler kan kun engasjere underdatabehandlere etter forutgående skriftlig tillatelse fra Behandlingsansvarlig. Godkjente underdatabehandlere er oppført i Vedlegg 3.

2. Databehandler skal kun engasjere underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at databehandlingen oppfyller kravene etter gjeldende personvernregler. Databehandler skal gjennomføre kontroller av underdatabehandlere for å verifisere deres databeskyttelsesnivå. Databehandler skal kunne fremlegge rapporter fra slik kontroller for Behandlingsansvarlig.

3. Databehandler plikter å forelegge disse avtalene for Behandlingsansvarlig etter forespørsel.

4. Databehandler plikter å inngå skriftlig avtale med hver underdatabehandler som regulerer underdatabehandlers behandling av personopplysninger og pålegges å ivareta alle plikter som Databehandleren selv er underlagt etter denne Databehandleravtalen.

5. Databehandler har fullt ansvar for underdatabehandlers utførelse av sine forpliktelser på samme måte som om Databehandler selv sto for utførelsen.

6. 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 disse.

9 OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJELAND

1. Databehandler kan kun overføre personopplysninger til et tredjeland eller en internasjonal organisasjon etter dokumenterte instrukser fra Behandlingsansvarlig.

2. Unntak kan skje dersom det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandler underrette Behandlingsansvarlig om nevnte rettslige krav før overføringen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette Behandlingsansvarlig så snart retten tillater dette).

10 MELDING OM BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN

1. Databehandler skal gi skriftlig melding til Behandlingsansvarlig om eventuelle brudd på Databehandleravtalen eller personopplysningssikkerheten.

2. Melding skal gis uten unødvendig forsinkelse og senest innen 24 timer etter at Databehandler ble oppmerksom på bruddet, slik at Behandlingsansvarlig har mulighet til å melde bruddet til Datatilsynet innenfor tidsfristen på 72 timer.

3. Melding om brudd på personopplysningssikkerheten bør inneholde en beskrivelse av:
   a. arten av bruddet, herunder kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt,
   b. de berørte registrertes identitet,
   c. navn og kontaktinformasjon til Personvernombudet eller et annet kontaktpunkt hos Databehandler for ytterligere innhenting av informasjon,
   d. de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
   e. tiltak som er truffet eller foreslått for å håndtere bruddet, herunder tiltak for å redusere eventuelle skadevirkninger,
   f. annen informasjon som kreves for at Behandlingsansvarlig kan overholde gjeldende personvernregler.

   Databehandler skal så snart som mulig gjennomføre alle tiltak som beskrevet i punkt e ovenfor. I tillegg skal Databehandler gjennomføre alle de tiltak som med rimelighet kreves for å unngå at det senere oppstår lignende brudd på personopplysningssikkerheten. Databehandler skal, så langt det er mulig, rådføre seg med Behandlingsansvarlig om de tiltak som skal gjennomføres samt overveie innspill fra Behandlingsansvarlig i den forbindelse.

4. Kun Behandlingsansvarlig har rett til å rapportere til Datatilsynet og til de berørte registrerte om brudd på personopplysningssikkerheten. Databehandler skal avstå fra å informere allmennheten eller tredjepart om brudd på personopplysningssikkerheten.

11 REVISJON

1. Databehandler skal dokumentere og gjøre tilgjengelig for Behandlingsansvarlig, informasjon som er nødvendig for å påvise etterlevelse av Databehandleravtalen og gjeldende personvernregler.

2. Databehandler skal muliggjøre og bidra ved revisjoner av Databehandlers behandlingsaktiviteter som utføres av Behandlingsansvarlig eller av annen inspektør med fullmakt fra Behandlingsansvarlig. Databehandler skal også muliggjøre og bidra ved revisjoner fra tilsynsmyndigheter.

3. Databehandleren skal foreta jevnlige revisjoner av sine behandlingsaktiviteter. Dette kan Databehandler gjøre på egen hånd eller via annen inspektør med fullmakt fra Databehandler. Databehandleren skal oversende kopi av revisjonsrapporter fra slike revisjoner til Behandlingsansvarlig. Behandlingsansvarlig skal ha rett til å fremlegge slike revisjonsrapporter til sine eksterne revisorer og tilsynsmyndigheter.

4. Databehandler skal umiddelbart varsle Behandlingsansvarlig hvis den mottar forespørsel fra en myndighet om å utlevere personopplysninger som er behandlet under Databehandleravtalen. Med mindre loven krever det, skal Databehandler ikke etterkomme en slik forespørsel uten skriftlig forhåndsgodkjenning fra Behandlingsansvarlig.

5. Dersom en revisjon avdekker avvik fra forpliktelsene i Databehandleravtalen, skal Databehandler så snart som mulig avhjelpe slike avvik (og, hvis relevant, påse at den relevante underdatabehandler gjør det samme). Behandlingsansvarlig kan kreve at hele eller deler av behandlingsaktivitetene midlertidig opphører til vellykket utbedring er bekreftet. Ved særlig alvorlige brudd kan Behandlingsansvarlig kreve behandlingen stoppet, opplysningene tilbakeføres til Behandlingsansvarlig og terminere Hovedavtalen samt Databehandleravtalen.

6. Hver av partene dekker sine egne kostnader forbundet med en revisjon. Hvis en revisjon avdekker avvik fra forpliktelsene i Databehandleravtalen, skal alle kostnader forbundet med revisjonen dekkes av Databehandler, herunder Behandlingsansvarliges og eksterne revisorers relevante kostnader.

12 VARIGHET OG OPPHØR

1. Databehandleravtalen gjelder fra den er signert med begge Parters underskrift og gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig.

2. Behandlingsansvarlig kan ved brudd på Databehandleravtalen eller bestemmelsene i gjeldende personvernlovgivning pålegge Databehandler å stoppe den videre behandlingen av personopplysningene med øyeblikkelig virkning.

3. Ved opphør av Databehandleravtalen plikter Databehandler å slette eller tilbakelevere alle personopplysninger som forvaltes på vegne av Behandlingsansvarlig og som omfattes av Databehandleravtalen. Dette gjelder også eventuelle sikkerhetskopier. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysninger skal skje, herunder hvilket format som skal benyttes. Databehandler skal skriftlig bekrefte eller dokumentere at sletting er foretatt innen nærmere avtalt tidspunkt etter Databehandleravtalens opphør. Dokumentasjonen skal gjøres tilgjengelig for Behandlingsansvarlig.

13 LOVVALG OG VERNETING

Databehandleravtalen er underlagt norsk rett og Partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av Databehandleravtalen.

14 KONTAKTPERSONER

Alle meddelelser vedrørende Databehandleravtalen rettes skriftlig og adressert til følgende kontaktpersoner:

Hos Behandlingsansvarlig:	Hos Databehandler:
Navn	Boris Berger
Stilling	Seniorrådgiver
e-post	Boris.Berger@nav.no

15 VEDLEGG 1 DATABEHANDLINGENS OMFANG

Behandlingens formål

Formålet med behandling av personopplysninger er å legge til rette for at kommunale ledere og medarbeidere i partnerskapet mellom kommune og stat, skal kunne utøve administrativ saksbehandling og arkivering på statlig område. Dette innebærer bruk av Arbeids- og velferdsetatens system WebSak.

I tillegg kan personopplysningene brukes til å utarbeide analyser og rapportering på dette området.

Behandlingens art og hensikt
Behandlingen av personopplysninger om ansatte er hjemlet i Arbeidsmiljøloven. Dataene lagres på en skybasert plattform, og forvaltes av HR-avdelingen. Dataene holdes oppdaterte og endres av den enkelte leder, HR på fylke/styringsenhet samt NAV Økonomitjeneste.

Kategorier av registrerte
Kommunale ledere i NAV
Kommunale medarbeidere i NAV

Type personopplysninger
Navn, ansatt-ID, e-postadresse, nærmeste leder, geografisk arbeidssted og roller i WebSak.

Opplysningene er nødvendig for at de ansatte kan registreres som brukere i systemet og brukes kun til analyser og rapportering utover dette.

Type sensitive personopplysninger
Leder og medarbeider har en rekke fritekstfelt tilgjengelig, for eksempel feltet dokumentnavn. Fritekstfeltene skal ikke brukes til å oppføre sensitive personopplysninger, men Arbeids- og velferdsdirektoratet kan ikke garantere at dette ikke vil skje. Sentrale rutiner og veiledninger for riktig bruk av løsningen utarbeides og vedlikeholdes av Arbeids- og velferdsdirektoratet.

Spesifikke sletteregler
Ingen.

16 VEDLEGG 2 TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

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

17 VEDLEGG 3 GODKJENTE UNDERDATABEHANDLERE

Selskapets navn	Selskapets adresse	Behandlingssted
ACOS AS	Trollhaugmyra 15, 5353 Straume	Oslo