

**AVTALE OM BEHANDLING AV PERSONOPPLYSNINGER
I DE DIGITALE TJENESTENE FOR DE
KOMMUNALE SOSIALE TJENESTENE**

Databehandleravtale

mellom

Eksempel kommune
som behandlingsansvarlig

og

Arbeids- og velferdsdirektoratet
som databehandler

INNHOLDSFORTEGNELSE:

1	Formålet med denne databehandleravtalen	3
2	Definisjoner	3
3	Omfang av behandlingen.....	4
4	Generelle plikter	5
5	Bistand til behandlingsansvarlig	5
6	Tekniske og organisatoriske sikkerhetstiltak	6
7	Taushetsplikt.....	6
8	Bruk av underdatabehandlere	6
9	Overføring av personopplysninger til tredjeland	7
10	Melding om brudd på personopplysningssikkerheten	7
11	Revisjon.....	8
12	Varighet og opphør.....	9
13	Lovvalg og verneting.....	9
14	Kontaktpersoner	9
15	Signering av avtalen og ikrafttredelse.....	9
16	Om vedlegg.....	9

1 FORMÅLET MED DENNE DATABEHANDLERAVTALEN

1. Denne avtalen («databehandleravtalen») er en del av samarbeidsavtale om digitale tjenester for de kommunale sosiale tjenestene («samarbeidsavtalen») mellom Eksempel 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 i forbindelse med samarbeidsavtalen.
4. I tilfelle uoverensstemmelse mellom samarbeidsavtalen og databehandleravtalen når det gjelder forhold spesifikt knyttet til personvern, skal databehandleravtalen gis forrang.
5. Databehandleravtalen har tre vedlegg. Vedleggene er en del av databehandleravtalen. Partene kan inngå nye vedlegg til databehandleravtalen for nye digitale tjenester.
6. Vedlegg 1 inneholder en beskrivelse av tekniske og organisatoriske sikkerhetstiltak.
7. Vedlegg 2 inneholder en oversikt over godkjente underdatabehandlere.
8. Vedlegg 3 inneholder en beskrivelse av behandlingens omfang, formål og hensikt, type personopplysninger og kategorier av registrerte for den digitale tjenesten «søknad om økonomisk sosialhjelp».

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 ny personvernforordning (GDPR).
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 generert i forbindelse med samarbeidsavtalen.
2. Databehandlingens formål og art, type personopplysninger som behandles, samt kategorier av registrerte fremgår av vedlegg 3 med videre.
3. Databehandler har ikke selvstendig råderett over personopplysningene og kan ikke bruke opplysningene til andre formål enn det som fremgår av vedlegg 3 med videre, og skal ellers behandle personopplysningene i samsvar med behandlingsansvarliges dokumenterte instruksjoner.

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 etterleveres 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 instruks.

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 adferdsnormer 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 ivaretagelse 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 1.
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 sosialtjenesteloven § 44, 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 2.
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 instruksjoner 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 36 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 personopplysningsikkerheten. Databehandler skal avstå fra å informere allmennheten eller tredjepart om brudd på personopplysningsikkerheten.

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 jevnlig 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 samarbeidsavtalen 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 parter underskrift og gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig i forbindelse med samarbeidsavtalen.
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 vernetting. Dette gjelder også etter opphør av databehandleravtalen.

14 KONTAKTPERSONER

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

Hos behandlingsansvarlig: _____

Navn:
e-post:

Hos databehandler: _____

Navn:
e-post:

15 SIGNERING AV AVTALEN OG IKRAFTTREDELSE

Avtalen trer i kraft fra det tidspunkt begge partene har signert databehandleravtalen og samarbeidsavtalen elektronisk. Det samme gjelder for avtalenes vedlegg. Nye vedlegg til avtalen må også signeres elektronisk av begge parter før de er gyldige.

16 OM VEDLEGG

Databehandleravtalen inneholder alltid minimum tre vedlegg.

Vedlegg nr. 1 om tekniske og organisatoriske sikkerhetstiltak.

Vedlegg nr. 2 om godkjente underdatabehandlere.

Vedlegg nr. 3 om databehandlingens omfang for den digitale tjenesten «søknad om økonomisk sosialhjelp».

Nye vedlegg til avtalen må signeres elektronisk av begge parter før de er gyldige.

EKSEMPEL

VEDLEGG 1:

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.

EKSEMPEL

VEDLEGG 2:

GODKJENTE UNDERDATABEHANDLERE

Selskapets navn	Selskapets adresse	Behandlingssted	Beskrivelse av hvilken type behandling

Per 10.12.2018 benytter Arbeids- og velferdsdirektoratet ingen underdatabehandlere, jf. personvernforordningen artikkel 28 punkt 4.

VEDLEGG 3:

DATABEHANDLINGENS OMFANG FOR DEN DIGITALE TJENESTEN «SØKNAD OM ØKONOMISK SOSIALHJELP»

Behandlingens formål

Behandling av personopplysninger som omfattes av denne databehandleravtalen er til bruk i den digitale tjenesten «søknad om økonomisk sosialhjelp».

Formålet med løsningen er å gi innbyggerne i kommunen bedre service, gi innbyggerne mulighet til å søke om økonomisk sosialhjelp digitalt og sette NAV-kontoret i stand til å komme raskere i gang med søknadsbehandlingen.

Formålet med behandlingen av personopplysningene er at innbyggerne får søkt og vurdert sitt behov for økonomisk stønad etter sosialtjenestelovens §§ 18 og 19.

Dette gjøres ved at innbyggerne i kommunen får tilbud om å benytte seg av en digital søknad ved å logge seg inn på Ditt NAV via nav.no. Løsningen forutsetter at bruker logger inn med sikker identifisering på nivå 4.

Arbeids- og velferdsdirektoratet kan som databehandler bare behandle personopplysningen i henhold til de formål som er bestemt av kommunen som behandlingsansvarlig og i samsvar med de vilkår som fremgår av avtalene med vedlegg.

Behandlingens art og hensikt

Samle inn og behandle personopplysninger med hjemmel i sosialtjenesteloven, for søkere av tjenesten «økonomisk sosialhjelp», gjennom Arbeids- og velferdsdirektoratet sitt nettsted nav.no.

Hensikten er å tilby og forvalte en digital søknad for tjenesten «økonomisk sosialhjelp».

Kategorier av registrerte

Søkere av økonomisk stønad etter sosialtjenesteloven §§ 18 og 19.

Typen personopplysninger

Navn, fødselsnummer/d-nummer, statsborgerskap, sivilstatus, opplysninger om barn, opplysninger om forsørgelsesplikt, opplysninger om samvær med barn, folkeregistrertadresse, oppholdsadresse, postadresse, telefonnummer, kontonummer, opplysninger om arbeid, opplysninger om utdanning, opplysninger om bosituasjon, opplysninger om økonomi eksempelvis inntekter, utgifter og formue, opplysninger om hva det søkes om og begrunnelse gitt i fritekstfelt, variabler som angir diverse statuser. Eksempler på variabler er: Start dato, stop dato, endret dato, løpenummer, tidsstempel, boolsk variabel med videre.

Komplett liste over personopplysninger finnes i den til enhver tid gjeldende personvernkonsekvensvurdering for tjenesten, og på nettstedet:

<https://github.com/navikt/soknadsosialhjelp-filformat>

Type sensitive personopplysninger

Som følge av at løsningen åpner for at både bruker kan skrive i fritekstfelt og laste opp vedlegg kan behandlingen omfatte opplysninger om rase, etnisk opprinnelse, politisk oppfatning, religion, fagforeningsmedlemskap, helseopplysninger, opplysninger om straffedommer og lovovertrедelser.

EKSEMPEL