**Databehandleravtale**

mellom

Oslo kommune

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Behandlingsansvarlig

og

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Databehandler

# Avtalens hensikt

Avtalens hensikt er å regulere partenes rettigheter og plikter som følger av Europaparlaments- og rådsforordning (EU) 2016/679 (GDPR) og lov om behandling av personopplysninger av 15. juni 2018 nr. 38 (personopplysningsloven) med tilhørende forskrifter.

Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer Databehandlers bruk av personopplysninger på vegne av den Behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

I denne avtalen gjelder de definisjoner som følger av GDPR art. 4.

# Rangordning

Ved motstrid går Databehandleravtalens bestemmelser foran Databehandlers eventuelle egne personvernvilkår og andre aktuelle vilkår som inngår i eller påvirker avtaleforholdet mellom Behandlingsansvarlig og Databehandler, herunder avtaler mellom Databehandler og dennes underleverandører eller samarbeidspartnere.

# Behandling av personopplysninger

## Formål

[Her beskrives kort formålet med behandlingen knyttet opp til den konkrete avtale.]

## Typer personopplysninger som behandles

* + Personnumre, navn, adresse, telefonnumre
	+ Særlige kategorier av personopplysninger som opplysninger om helseforhold, religiøs overbevisning, etnisk opprinnelse

Oppramsingen er ikke uttømmende og ved tvil om informasjon er personopplysninger, herunder særlige kategorier av personopplysninger, skal Databehandler ta kontakt med Behandlingsansvarlig.

## Kategorier av registrerte

* Behandlingsansvarliges tjenestemottakere

## Behandlingens art

* + Enhver operasjon eller rekke av operasjoner som gjøres, enten automatisert eller ikke, herunder, men ikke begrenset til, innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring. Disse behandlingstypene kan også gjennomføres i kombinasjon.

## Rådighet over data

* + Databehandler har ikke råderett over personopplysningene og kan dermed heller ikke behandle disse til egne formål. Det er kun den Behandlingsansvarliges formål som skal ligge til grunn for enhver behandling. Opplysningene kan kun utleveres til behandlingsansvarlig og den/de han bemyndiger som mottaker.
	+ Opplysningene skal lagres i så lang tid som formålet med avtalen tilsier, og slik at Behandlingsansvarlig får benyttet seg av opplysningene i henhold til formålet. Dette enten i original form eller som aggregerte, sammenstilte opplysninger. Opplysningene skal ikke lagres for fremtidig bruk i arkivinstans.

# Partenes rettigheter og plikter

Databehandler skal følge de rutiner og instrukser for behandlingen som Behandlingsansvarlig til enhver tid har bestemt skal gjelde.

Databehandler plikter å gi Behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at Behandlingsansvarlig kan ivareta sitt eget ansvar etter regelverket. Databehandler plikter å informere Behandlingsansvarlig hvis det foretas endringer i sikkerhetsdokumentasjonen.

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Databehandler, herunder ansatte hos Databehandler, har taushetsplikt om personopplysninger som vedkommende får tilgang til i henhold til denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

## Sikkerhetskopiering og speiling av opplysninger

Databehandler skal ta regelmessig sikkerhetskopi.

Dersom Databehandler benytter underleverandør skal Databehandler sikre at underleverandør tar sikkerhetskopier.

Databehandler lagrer sikkerhetskopi logisk adskilt fra originaldataene.

## Innsyn, korrigering og sletting av personopplysninger

Behandlingsansvarlig vil behandle anmodninger om innsyn fra de registrerte og andre. Databehandler skal imidlertid bistå den Behandlingsansvarlige ved behov.

Korrigering og sletting av personopplysninger skal utføres av Databehandler etter avtale med den Behandlingsansvarlige, og etter avtalte rutiner.

## Ulike behandlingsansvarlige

Databehandler skal sikre at personopplysninger som behandles på vegne av Behandlingsansvarlig etter denne avtalen ikke sammenblandes med personopplysninger som behandles på vegne av andre behandlingsansvarlige.

## Overføring av data til utlandet

Personopplysninger kan ikke uten skriftlig godkjennelse fra behandlingsansvarlig overføres til land utenfor EØS eller utenfor de EU-godkjente mottakerstater. Denne begrensningen gjelder også overføring til servicesenter eller andre funksjoner som ligger utenfor EØS-området eller utenfor de EU-godkjente mottakerstater. Begrensningen innebærer også at opplysningene ikke skal kunne aksesseres av personer eller systemer i land utenfor EØS eller utenfor de EU-godkjente mottakerstater. Personopplysninger kan likevel overføres til og aksesseres fra USA forutsatt at databehandler til en hver tid er sertifisert etter EU-U.S. Privacy Shield.

## Dataportabilitet

Data kan overføres til tredjeparter etter skriftlig samtykke fra behandlingsansvarlig. Ved behov skal det signeres en ny databehandleravtale med den nye databehandleren før behandlingen av personopplysningene starter.

Den registrerte har rett til å motta personopplysninger vedkommende har gitt til Behandlingsansvarlig i et strukturert, alminnelig anvendt og maskinleselig format på de vilkår som følger av GDPR art. 20. Databehandler skal bistå med dette.

# Bruk av underleverandør

Dersom Databehandler benytter seg av underleverandør eller andre som ikke normalt er ansatt hos Databehandler forblir Databehandler ansvarlig for deres behandling av personopplysninger.

Dersom det skal benyttes underleverandør skal dette godkjennes skriftlig av behandlingsansvarlige før behandlingen av personopplysninger starter.

Oversikt over aktuelle underleverandører og samarbeidspartnere ved avtalens oppstart, som er godkjent av Behandlingsansvarlig, ligger som bilag 1 til denne avtale.

Databehandler kan ikke benytte andre underleverandører og samarbeidspartnere til oppfyllelse av avtaler med Behandlingsansvarlig uten skriftlig godkjennelse fra denne. Samtykke kan bare nektes på saklig grunnlag.

Databehandler plikter å ha nødvendige avtaler med underleverandøren for å sikre at underleverandørens behandling av personopplysninger er i tråd med denne avtalen. Slike avtaler skal være på plass før behandlingen av personopplysninger starter.

Samtlige aktører som på vegne av Databehandler utfører oppdrag der bruk av personopplysninger inngår skal være kjent med Databehandlers avtalemessige og lovmessige forpliktelser og påta seg å etterleve disse.

# Informasjonssikkerhet

Databehandler skal ha tilfredsstillende informasjonssikkerhet i tråd med GDPR art. 32. Databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen.

For å sikre fortrolighet skal databehandler sikre at informasjon kun er tilgjengelig for de som etter avtalen skal ha tilgang. Tilgangsstyringen hos databehandler skal være i samsvar med lovpålagte krav og i tråd med de krav som er stilt i avtalen(e) som omhandler Hjelpetiltak i barnevernstjenesten.

For å sikre integritet skal databehandler sikre at personopplysninger ikke endres uautorisert eller utilsiktet. Melding etter GDPR art. 33 skal skje ved at Databehandler melder avviket til Behandlingsansvarlig. Behandlingsansvarlig har ansvaret for at melding om brudd på personopplysningssikkerheten sendes Datatilsynet.

Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Rutiner og tiltak slik disse var ved etablering av avtalen, skal legges frem for Behandlingsansvarlig på forespørsel. Databehandler plikter skriftlig å varsle Behandlingsansvarlig når det foretas endringer i disse. Samtlige versjoner av dokumentasjonen skal i hele avtaleperioden være tilgjengelig på Behandlingsansvarliges eller aktuelle tilsynsmyndigheters forespørsel.

# Revisjoner

Behandlingsansvarlig skal avtale med Databehandler at det gjennomføres sikkerhetsrevisjoner jevnlig for systemer og lignende som omfattes av denne avtalen, men minimum én gang per år.

Sikkerhetsrevisjon skal omfatte gjennomgang av rutiner, stikkprøvekontroller, vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Revisjonen kan også omfatte mer omfattende stedlige kontroller og andre egnede kontrolltiltak. Resultatet fra sikkerhetsrevisjon skal dokumenteres og legges frem for den Behandlingsansvarlige.

Databehandler skal informere Behandlingsansvarlig om endrede informasjonssikkerhetstiltak.

# Avtalens varighet

Avtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig. Den gjelder videre så langt den passer for eventuelle personopplysninger som måtte forefinnes hos Databehandler etter avtalens utløp.

Ved brudd på denne avtale eller GDPR, kan Behandlingsansvarlig pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning

# Ved opphør av avtalen

Ved opphør av denne avtalen plikter Databehandler å tilbakelevere alle personopplysninger som er mottatt på vegne av den Behandlingsansvarlige og som omfattes av denne avtalen. Tilbakelevering skal skje til Behandlingsansvarlig eller den Behandlingsansvarlig utpeker.

Opplysningene må overføres på et medium og med tilhørende programvare som gjør det mulig å lese av dataene.

Databehandler skal foreta sikker sletting eller forsvarlig destruering av alle dokumenter, data, disketter, cd-er mv, som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier.

Databehandler skal skriftlig dokumentere at sikker sletting og/eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør. Meddelelse om sletting og destruksjon skal sendes til.

xx.xx@xxx.oslo.kommune.no, merket «*Meddelelse om sletting av data saksnummer xx.xxxx.xxx*»

Dersom Databehandler benytter underleverandør er Databehandler ansvarlig for at underleverandør foretar tilbakelevering og sletting eller forsvarlig destruering i tråd med beskrivelsen ovenfor.

# Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til: \_\_\_\_\_\_\_\_\_\_\_

og merkes «Databehandleravtale for Hjelpetiltak i barnevernstjenesten saksnr. xxxxx».

# Lovvalg og verneting

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

\*\*\*

Denne avtale er i 2 – to eksemplarer, hvorav partene har hvert sitt.

For Databehandler For Behandlingsansvarlig:

Sted: Sted:

Dato: Dato:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

XXXXXX XXXXXX

**Bilag 1 Oversikt over Databehandlers underleverandører og tredjeparter/samarbeidspartnere**