# Databehandleravtale

I henhold til GDPR art. 28

mellom

**<sett inn navn på virksomhet>**

behandlingsansvarlig

og

**<sett inn navn på virksomhet>**

databehandler

**1. Databehandleravtalens hensikt**

Hensikten med databehandleravtalen (avtalen) er å regulere rettigheter og plikter forbundet med behandling av personopplysninger. Avtalen skal sikre at kravene i GDPR etterleves, særlig sett hen til at personopplysninger ikke skal behandles urettmessig eller kommer uberettigede i hende.

Avtalen fastsetter rammer og vilkår for den behandling av personopplysninger som databehandler utfører på vegne av behandlingsansvarlig, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

**2. Formål med behandling av personopplysninger**

<Oppdragsgiver> AS (Oppdragsgiver) har den DD.MM.ÅÅÅÅ inngått en avtale med <Oppdragstaker> AS (Oppdragstaker) som omfatter \*Her må det fylles inn hva avtalen omfatter, dvs. En beskrivelse av oppdraget\*.

Utføringen av dette arbeidet innebærer at databehandler vil behandle personopplysninger på vegne av behandlingsansvarlig. Formålet med den behandling av opplysninger som avtalen omfatter er \*fyll inn formålet med behandlingen av personopplysninger\*.

Rammene for databehandlers behandling av personopplysninger på vegne av behandlingsansvarlig følger av den inngåtte oppdragsavtalen mellom partene, samt denne avtalen. Databehandler kan ikke behandle opplysningene på annet vis eller til noe annet formål enn det som følger av oppdragsavtalen og databehandleravtalen.

Oppdraget innebærer at databehandler kan behandle personopplysninger om følgende kategorier registrerte:

NB: Stryk det som ikke passer. Listen er ikke uttømmende, og må suppleres ved behov.

For eksempel:

* Jobbsøkere
* Ansatte
* Pårørende
* Frivillige
* Leverandører
* Kunder
* Potensielle kjøpere

Nedenfor er det opplistet eksempler på hvilke personopplysninger som kan behandles av databehandler under denne databehandleravtalen:

NB: Stryk det som ikke passer. Listen er ikke uttømmende, og må suppleres ved behov.

For eksempel:

* Personalia
* Kontaktopplysninger
* Personnummer
* Lønnsopplysninger
* Boligopplysninger (adresse, Gnr/Bnr, osv.)
* Kontonummer
* Evalueringer
* Kjøpshistorikk
* Opplysninger om mulige straffbare forhold
* Opplysninger om helseforhold
* Opplysninger om fagforeningsforhold
* Gjennomgang av elektronisk lagret informasjon, herunder epostkasser, filområder på virksomhetens server mv.
* E-postkorrespondanse

**3.Behandlingsansvarliges instruksjonsmyndighet**

Under utføring av oppdraget for behandlingsansvarlig står databehandler under instruksjon fra behandlingsansvarlig. Databehandler skal til enhver tid behandle de personopplysninger som omfattes av denne avtalen (heretter personopplysninger) i samsvar med de instrukser, rutiner og pålegg som er gitt av behandlingsansvarlig. Behandlingsansvarlig kan til enhver tid endre kravene til hvordan personopplysningene skal behandles etter avtalen. Dette under forutsetning av at instruksjonene ikke strider med krav som følger av GDPR.

Den behandlingsansvarlige plikter på sin side til å bidra til at databehandler kan behandle opplysningene i samsvar med kravene i GDPR.

**4. Databehandlers plikter**

Databehandler skal utelukkende behandle personopplysninger i den utstrekning det er nødvendig for å etterleve oppdragsavtalen og denne avtalen. Databehandler kan ikke behandle personopplysningene til andre formål.

Databehandler skal til enhver tid kunne dokumentere hvor personopplysninger som behandles i medhold av denne avtalen er lagret. Personopplysninger kan ikke overføres til land utenfor EØS-området eller til internasjonale organisasjoner uten at det er avtalt med behandlingsansvarlige.

Databehandler kan ikke utlevere personopplysninger til eksterne parter uten at dette fremgår klart av databehandleravtalen, eller annen skriftlig avtale.

Databehandlerplikter å påse at samtlige personer i virksomheten som har tilgang til personopplysninger, er kjent med denne avtalen og underlagt avtalens bestemmelser.

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til å få tilgang til personopplysningene.

Databehandler, herunder alle databehandlers ansatte, har taushetsplikt om informasjon om behandlingsansvarliges sikkerhetstiltak og systemer for øvrig. Taushetsplikten omfatter også alle personopplysninger som vedkommende får tilgang til iht. denne avtalen. Dette gjelder også etter avtalens opphør.

Databehandler plikter å bistå behandlingsansvarlig i å etterkomme anmodninger fra de registrerte om innsyn, retting og sletting av deres personopplysninger, samt anmodninger om reservasjon og dataportabilitet. Dersom databehandler mottar anmodninger om innsyn, retting/sletting, reservasjon eller dataportabilitet skal behandlingsansvarlig ved <sett inn navn, stilling og kontaktinfo> kontaktes uten unødig opphold.

Databehandler plikter å orientere den behandlingsansvarlige dersom den behandlingsansvarliges instruksjoner er i strid med krav i GDPR. Dersom det oppstår uenighet om hvorvidt instruksjonene er i strid med GDPR skal den behandlingsansvarliges forståelse legges til grunn.

Dersom det oppstår sikkerhetsbrudd eller hendelser som innebærer at opplysninger er behandlet i strid med avtalen skal databehandler omgående varsle den behandlingsansvarlige og gjennomføre tiltak for å lukke avviket. Slik varsling skal senest finne sted 24 timer etter at databehandler fikk kunnskap om hendelsen.

Stryk det som ikke passer her vedrørende sletting: Databehandler skal løpende slette personopplysninger i tråd med behandlingsansvarliges instrukser, jf. vedlegg X til denne avtalen/Innen tre måneder etter at behandlingsansvarlig har bekreftet at oppdraget er utført, skal databehandler slette all informasjon som er mottatt i forbindelse med oppdraget, med mindre behandlingsansvarlig skriftlig ber om å få dette tilbakelevert. Databehandler skal etter dette bekrefte at all informasjon er slettet og at de ikke besitter noen informasjon som er sikret i forbindelse med oppdraget.

Dersom databehandler behandler personopplysninger til andre formål, eller med andre virkemidler enn avtalt, blir databehandler å regne som behandlingsansvarlig med de plikter og ansvar det medfører, jf. GDPR art. 82,83, og 84.

**5. Bruk av underleverandør**

Stryk det som ikke passer her:

\*Databehandler kan ikke benytte underleverandører i sin behandling av personopplysninger for behandlingsansvarlig, uten at dette på forhånd er skriftlig avtalt med behandlingsansvarlig

\*Behandlingsansvarlig gir databehandler en generell skriftlig tillatelse til bruk av underleverandører. Dersom databehandler benytter seg av underleverandører skal databehandleren underrette den behandlingsansvarlige om navn og kontaktinformasjon på underleverandør. Behandlingsansvarlig har rett til å motsette seg databehandlers bruk av underleverandør uten nærmere begrunnelse.

Med underleverandør menes en person (fysisk eller juridisk) som er databehandler til <denne avtalens databehandler>.

Det skal inngås skriftlig avtale mellom databehandler og underleverandør som pålegger underleverandør de samme forpliktelser som databehandler med hensyn til vern av personopplysninger. Samtlige som på vegne av databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser. Tilsvarende forpliktelser skal pålegges vedkommende.

Databehandler er ansvarlig overfor behandlingsansvarlig for ethvert lov- og/eller forskriftsbrudd eller brudd på forpliktelsene etter denne avtalen som underleverandør til databehandler gjør seg skyld i, som om handlingen var utført av ham selv.

**6. Sikkerhet**

Databehandler skal oppfylle de krav til sikkerhetstiltak som er nødvendige i henhold til GDPR art. 32 og for å oppfylle behandlingsansvarliges sikkerhetskrav. Databehandler skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandlingen av personopplysninger på vegne av behandlingsansvarlig.

Her må konkrete sikkerhetstiltak som databehandler skal ha på plass beskrives. Alternativt kan det henvises til <virksomhet>s sikkerhetspolicy eller andre dokumenter som eventuelt vedlegges denne avtalen.

Databehandler skal oversende de rutiner eller andre tiltak som er på plass for å oppfylle disse kravene.

Databehandler skal blant annet sørge for at personopplysningene ikke gjøres tilgjengelige for uvedkommende gjennom fysiske og tekniske tiltak. Databehandler skal også sørge for tilgangsstyring internt. Tilgang skal være basert på den enkelte ansattes behov, sett hen til vedkommende arbeidsoppgaver. Personopplysningene skal beskyttes mot uautorisert endring og sletting. Bruk av informasjonssystemer skal loggføres. Logger skal lagres i tre måneder. Sikkerhetstiltakene må tilfredsstille allment aksepterte bransjestandarder såfremt slike er egnede.

Personopplysninger som omfattes av GDPR art. 9s angivelse av «særlige kategorier personopplysninger» må underlegges særlig beskyttelse og kan ikke formidles via ukryptert e-post. Det samme gjelder personnummer og opplysninger knyttet til straffbare forhold.

Personopplysningene skal ikke lagres lengre enn nødvendig for å oppfylle formålet. Databehandler skal jevnlig kontrollere at den behandlingsansvarliges instruksjoner om sletting etterleves og at ikke kopier av opplysninger blir lagret i databehandlers systemer.

Databehandler skal \*stryk det som ikke passer årlig/hvert andre år foreta risikovurdering som skal oversendes behandlingsansvarlig.

**7. Sikkerhetsrevisjoner**

Databehandler skal \*stryk det som ikke passer årlig/hvert andre år gjennomføre sikkerhetsrevisjoner av informasjonssystemer som benyttes til å behandle personopplysninger på vegne av behandlingsansvarlig. Resultatet av denne sikkerhetsrevisjonen skal oversendes behandlingsansvarlig.

Databehandler plikter å legge til rette for at behandlingsansvarlige kan gjennomføre sikkerhetsrevisjoner og -inspeksjoner, både av databehandlers sikkerhetsdokumentasjon og den konkrete etterlevelsen av dokumentasjonen.

Revisjonen kan omfatte stedlig inspeksjon eller gjennomføres ved at databehandler oversender sine risikovurderinger, oppdaterte rutiner for informasjonssikkerhet og internkontroll, samt resultatet av den sikkerhetsrevisjonen som databehandler har gjort av informasjonssystemet.

Dersom behandlingsansvarlig ønsker å få gjennomført stedlig inspeksjon eller stikkprøvekontroll skal databehandler varsles skriftlig og innen rimelig tid forut for stedlig inspeksjon.

Behandlingsansvarlig har også adgang til å gjennomføre stikkprøvekontroller av databehandlers informasjonssikkerhet og internkontroll, men kun begrenset til å gjelde behandling av de opplysninger som behandles på vegne av behandlingsansvarlig.

**8. Varighet, pålegg om stans, oppsigelse mv**

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig.

Ved brudd på denne avtale eller krav som kan utledes av GDPR kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

**9. Ved opphør**

Ved opphør av denne avtalen plikter databehandler å tilbakelevere og/eller slette alle personopplysninger som omfattes av denne avtalen.

Databehandler skal slette, eller på en forsvarlig måte destruere alle øvrige dokumenter og lagringsmedier, som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier. Eventuelle kostnader forbundet med dette skal bære av databehandler.

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

**10. Meddelelser**

Meddelelser etter denne avtalen skal sendes skriftlig til:

BEHANDLINGSANSVARLIG: Sett inn navn på kontaktperson og riktig e-postadresse

DATABEHANDLER: Sett inn navn på kontaktperson og riktig e-postadresse

**11. Lovvalg og verneting**

Avtalen er underlagt norsk rett og partene vedtar <sett inn riktig tingrett> tingrett som verneting. Dette gjelder også etter opphør av avtalen.

\*\*\*

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

Sted og dato

Behandlingsansvarlig Databehandler

……………………….. ………………………