# DATABEHANDLERAVTALE

i henhold til artikkel 28 nummer 3, i Europaparlamentets og Rådets forordning 2016/679 (GDPR) med henblikk på databehandlerens behandling av personopplysninger mellom

**<navn på virksomhet>**
**Org.nr. <organisasjonsnummer>**
**<adresse>**
**<postnummer og by>**
**<land>**
heretter «den behandlingsansvarlige»

og

**BDO AS**
**Org.nr. 993 606 650**
**Munkedamsveien 45A**
**0250 OSLO**
**Norge**
heretter «databehandleren»

som hver for seg er en «part» og sammen utgjør «partene».

## 1. DATABEHANDLERAVTALENS HENSIKT

Hensikten med databehandleravtalen (avtalen) er å regulere den behandlingsansvarlige og databehandlerens rettigheter og plikter når databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige.

Avtalen skal sikre at kravene i EUs generelle personvernforordning 2016/679 (GDPR) etterleves, særlig sett hen til at personopplysninger ikke skal behandles urettmessig eller kommer uberettigede i hende. GDPR er gjort til norsk lov gjennom personopplysningsloven 20. juli 2018 nr. 38 § 1.

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

Avtalen inngår som et vedlegg til oppdragsavtalen mellom BDO AS og <Kunde> AS.

Ved motstrid med andre avtaler mellom partene, skal bestemmelsene i denne avtalen ha forrang. Dette gjelder likevel ikke for skriftlige instrukser som er gitt i samsvar med denne avtalen.

Denne avtalen fritar ikke databehandleren fra plikter som databehandleren er pålagt etter GDPR eller annen lovgivning.

## 2. FORMÅL OG BESKRIVELSE AV BEHANDLINGEN

<Kunde> AS (<Kunde>) har DD.MM.ÅÅÅÅ inngått en avtale med BDO AS (BDO) om å levere <sett inn tjeneste>.

I forbindelse med levering av <sett inn tjeneste> vil databehandleren behandle personopplysninger på vegne av den behandlingsansvarlige. Formålet med databehandlerens behandling av personopplysningene er <sett inn formål>.

Databehandler kan behandle personopplysninger om følgende kategorier av registrerte:

- <sett inn hvem personopplysningene omhandler, for eksempel kundens ansatte>

Databehandler kan behandle følgende personopplysninger på vegne av den behandlingsansvarlige:

- <sett inn hvilke personopplysninger som behandles, for eksempel personalia>

## 3. DEN BEHANDLINGSANSVARLIGES RETTIGHETER OG PLIKTER

Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i samsvar med GDPR, annen relevant lovgivning og denne avtalen. Den behandlingsansvarlige plikter blant annet å sikre at det foreligger et rettslig grunnlag for behandlingen som databehandleren skal utføre etter avtalen.

Den behandlingsansvarlige har både en rett og en plikt til å bestemme formålet med behandlingen og hvilke midler som skal benyttes.

Den behandlingsansvarlige skal gi databehandleren dokumenterte instrukser for hvordan personopplysningene skal behandles etter avtalen. Instruksene er en del av denne avtalen. Den behandlingsansvarlige kan til enhver tid endre instruksene under forutsetning av at instruksjonene ikke strider mot krav som følger av GDPR.

## 4. DATABEHANDLERENS PLIKT TIL Å HANDLE ETTER INSTRUKS

Databehandleren kan bare behandle personopplysninger på bakgrunn av denne avtalen og etter dokumenterte instrukser fra den behandlingsansvarlige, med mindre databehandleren er underlagt lovfestede krav til å behandle personopplysningene. Dersom databehandleren er underlagt slike krav, skal databehandleren varsle den behandlingsansvarlige om dette før behandlinger iverksettes, med mindre loven forbyr slik underretning av hensyn til viktige samfunnsinteresser.

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 skriftlig med behandlingsansvarlige.

Databehandleren skal ikke behandle personopplysninger for andre formål eller med andre midler enn det som følger av denne avtalen eller skriftlige instrukser fra den behandlingsansvarlige. Dersom databehandleren behandler personopplysninger til andre formål, eller med andre midler enn det som er avtalt eller instruert, vil databehandleren regnes som behandlingsansvarlig med de plikter og ansvar det medfører, jf. GDPR art. 82,83, og 84.

Databehandleren plikter å varsle den behandlingsansvarlige dersom den behandlingsansvarliges instruksjoner er i strid med krav som følger av GDPR eller annen lovgivning. Dersom det oppstår uenighet om instruksjonene er i strid med GDPR eller annen relevant lovgivning, skal den behandlingsansvarliges forståelse legges til grunn.

## 5. INFORMASJONSSIKKERHET VED BEHANDLINGEN

Databehandleren plikter å gjennomføre alle sikkerhetstiltak som er nødvendige i henhold til GDPR artikkel 32 og for å oppfylle den behandlingsansvarliges krav til informasjonssikkerhet.

Databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandlingen av personopplysninger på vegne av den behandlingsansvarlige. Databehandleren skal gjennomføre risikovurderinger for å fastsette hva som er tilfredsstillende informasjonssikkerhet.

Databehandleren skal sørge for at personopplysningene etter denne avtalen bare er tilgjengelig for autoriserte personer ved hjelp av tilgangskontroll og tilgangsstyring. Databehandleren skal kun autorisere personer som har et behov for tilgang til opplysningene for å utføre sine arbeidsoppgaver. Databehandleren skal ha rutiner for å frata tilganger dersom behovet ikke lenger er til stede.

Databehandleren skal sørge for at autoriserte personer med tilgang til opplysningene er forpliktet til å behandle opplysningene konfidensielt eller er underlagt lovfestet taushetsplikt. Den behandlingsansvarlige kan kreve at databehandleren dokumenterer at autoriserte personer er underlagt slik plikt. Plikten til å sikre opplysningenes konfidensialitet gjelder også etter avtalens opphør.

Bruk av informasjonssystemer skal loggføres, og det skal legges til rette for varsling om og håndtering av uønskede hendelser som gjelder personvern og sikkerhet.

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

Databehandleren plikter å bistå den behandlingsansvarlige med å sikre overholdelse av forpliktelsene i henhold til GDPR artikkel 32-36 som er relevante for avtaleforholdet.

Dersom det oppstår sikkerhetsbrudd eller hendelser som innebærer at opplysninger er behandlet i strid med avtalen, skal databehandleren varsle den behandlingsansvarlige ved <sett inn navn, stilling og kontaktinfo> uten ugrunnet opphold etter å ha fått kjennskap til bruddet. Dersom bruddet medfører at den behandlingsansvarlige må varsle tilsynsmyndigheten eller de registrerte, skal databehandleren gi den behandlingsansvarlige informasjonen som kreves for å kunne oppfylle sine forpliktelser etter GDPR artikkel 33 nr. 3 sammen med varselet.

## 6. BRUK AV UNDERLEVERANDØRER

Med underleverandør menes en person (fysisk eller juridisk) som er databehandler til BDO AS.

Den behandlingsansvarlige gir databehandleren en generell skriftlig tillatelse til bruk av underleverandører. Dersom databehandleren benytter seg av underleverandører, skal databehandleren underrette den behandlingsansvarlige om navn og kontaktinformasjon på underleverandøren innen rimelig tid før underleverandøren engasjeres. Den behandlingsansvarlige har rett til å motsette seg databehandlerens bruk av underleverandør.

Det skal inngås skriftlig avtale mellom databehandleren og underleverandøren som pålegger underleverandøren de samme forpliktelsene som databehandleren er underlagt etter denne avtalen med hensyn til vern av personopplysninger.

Databehandleren er ansvarlig overfor den behandlingsansvarlige for ethvert lov- og/eller forskriftsbrudd eller brudd på forpliktelsene etter denne avtalen som underleverandøren til databehandleren gjør seg skyld i, som om handlingen var utført av ham selv.

Ved inngåelse av avtalen, har databehandleren oppgitt at følgende underleverandører vil bli benyttet:

| Navn | Beskrivelse av behandlingen | Lokasjon datasenter |
|---|---|---|
| <Sett inn underleverandør som benyttes> | <Beskriv behandlingen som underleverandøren gjør> | <Sett inn hvor personopplysningene lagres> |
| | | |
| | | |
| | | |

Ved inngåelse av avtalen har den behandlingsansvarlige godkjent bruken av ovennevnte underdatabehandlere for den behandlingsaktiviteten som er beskrevet.

## 7. BISTAND TIL Å ETTERKOMME ANMODNINGER FRA REGISTRERTE

Databehandleren plikter, i den grad det er mulig og med hensyn til behandlingens art, å bistå den behandlingsansvarlige i å etterkomme anmodninger fra de registrerte om utøvelse av deres rettigheter. Dersom databehandleren mottar anmodninger fra de registrerte om deres

rettigheter, skal den behandlingsansvarlige ved <sett inn navn, stilling og kontaktinfo> kontaktes uten ugrunnet opphold.

## 8. SLETTING AV PERSONOPPLYSNINGER

Personopplysningene skal ikke lagres lengre enn nødvendig for å oppfylle formålet.

Databehandleren skal slette personopplysninger etter <beskriv sletterutiner>.

Databehandleren skal jevnlig kontrollere at den behandlingsansvarliges instruksjoner om sletting etterleves og at ikke kopier av opplysninger blir lagret i databehandlerens systemer.

## 9. TILGJENGELIGGJØRING AV INFORMASJON OG SIKKERHETSREVISJONER

Databehandleren plikter å gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at databehandleren etterlever sine forpliktelser etter denne avtalen.

Databehandleren skal sørge for å gjennomføre sikkerhetsrevisjoner av informasjonssystemer som benyttes til å behandle personopplysninger på vegne av den behandlingsansvarlige. Databehandleren skal på anmodning oversende denne til den behandlingsansvarlige.

Databehandleren plikter å legge til rette for at den behandlingsansvarlige kan gjennomføre sikkerhetsrevisjoner. Revisjonen kan omfatte stedlig inspeksjon, stikkprøvekontroller eller gjennomføres ved at databehandleren oversender sine risikovurderinger, oppdaterte rutiner for informasjonssikkerhet og internkontroll, samt resultatet av den sikkerhetsrevisjonen som databehandleren har gjort av informasjonssystemet. For eventuelle kostnader forbundet med slik revisjon skal Partene dekke sine egne kostnader.

Dersom den behandlingsansvarlige ønsker å få gjennomført stedlig inspeksjon eller stikkprøvekontroll skal databehandler varsles skriftlig og senest 30 dager forut for inspeksjonen eller kontrollen.

Dersom en kvalifisert tredjepart har gjennomført en sikkerhetsrevisjon med databehandleren i ISAE3402, ISO eller lignende rapport i løpet av de siste 12 månedene, og databehandler bekrefter at det ikke foreligger endringer etter dette, skal den behandlingsansvarlige akseptere disse rapportene i stedet for å forespørre ny revisjon.

Dersom tredjepartsrevisjonen ikke dekker den behandlingsansvarliges behov kan det avtales egen revisjon med databehandleren. Den behandlingsansvarlige er selv ansvarlig for kostnadene av slikt tilsyn. Dersom den behandlingsansvarlige trenger mer assistanse enn den

som tilbys av databehandleren for å oppfylle gjeldene personvernlovgivning, kan databehandleren kreve betaling for denne tilleggstjenesten.

## 10. IKRAFTTREDELSE OG OPPHØR

Avtalen trer i kraft når begge parter har signert avtalen.

Avtalen er ikke tidsbegrenset og gjelder så lenge databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige.

Ved brudd på avtalen eller krav som kan utledes av GDPR, kan den behandlingsansvarlige pålegge databehandleren å stoppe behandlingen av opplysningene med øyeblikkelig virkning.

Ved opphør av avtalen plikter databehandleren å slette alle personopplysninger som har blitt behandlet etter denne avtalen innen tre måneder, med mindre databehandleren er underlagt rettslige forpliktelser til å oppbevare personopplysningene. Databehandleren skal gi den behandlingsansavarlige skriftlig bekreftelse på at personopplysningene er slettet innen rimelig tid etter avtalens opphør, og ved forespørsel kunne dokumentere hvordan sletting er utført.

## 11. 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>

## 12. LOVVALG OG VERNETING

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