Databehandleravtale

mellom

[navn på virksomhet]
Org.nr. [organisasjonsnummer]
[adresse]
[postnummer og by]
[land]

heretter omtalt som «Behandlingsansvarlige»

og

BDO AS
Org.nr. 993 606 650
Munkedamsveien 45A
0250 OSLO
Norge

heretter omtalt som «Databehandleren»

som hver for seg er en «Part» og sammen utgjør «Partene».

1. Om databehandleren

Partene har inngått avtale om [sett inn en kort beskrivelse av oppdraget] («Oppdragsavtalen»).

Formålet med denne avtalen («Databehandleravtalen») er å fastsette Partenes rettigheter og plikter når Databehandleren behandler personopplysninger på vegne av Behandlingsansvarlige i forbindelse med å levere tjenestene som beskrevet i Oppdragsavtalen.

Databehandleravtalen skal sikre at kravene i EUs personvernforordning 2016/679 (GDPR) og personopplysningsloven med tilhørende forskrifter etterleves. GDPR og personopplysningsloven med forskrifter omtales heretter i fellesskap som «Personvernregelverket».

Databehandleravtalen inngår som et vedlegg til Oppdragsavtalen mellom Behandlingsansvarlige og Databehandleren. Ved motstrid mellom Databehandleravtalen og andre avtaler inngått mellom Partene, skal bestemmelsene i Databehandleravtalen ha forrang dersom motstriden gjelder behandling av personopplysninger. Dette gjelder likevel ikke for skriftlige instrukser som er gitt i henhold til Databehandleravtalen.

Databehandleravtalen fritar ikke Databehandleren fra plikter som Databehandleren er pålagt etter Personvernregelverket eller annen lovgivning.

2. Beskrivelse av behandlingen

Formålet med Databehandlerens behandling av personopplysninger er [sett inn formål].

Databehandleren kan behandle personopplysninger om følgende kategorier av registrerte:

- [sett inn hvem personopplysningene omhandler, for eksempel kundens ansatte, kontaktpersoner hos kundens kunder eller leverandører mv.]

Databehandleren kan behandle følgende typer av personopplysninger om de registrerte:

☐ **Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9:**

[Spesifiser type, for eksempel helseopplysninger eller fagforeningsmedlemskap]

☐ **Andre beskyttelsesverdige personopplysninger:**

[Spesifiser type, for eksempel personnummer, opplysninger om inntekt og gjeld og vurderinger av prestasjoner]

☐ **Andre personopplysninger:**

[Spesifiser type, for eksempel navn, telefonnummer, e-postadresse, utdanning og opplysninger om ansattforhold, herunder stilling, tittel eller arbeidstid]

3. Behandlingsansvarliges rettigheter og plikter

Behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i samsvar med GDPR, annen relevant lovgivning og Databehandleravtalen. Behandlingsansvarlige

plikter blant annet å sikre at det foreligger et gyldig rettslig grunnlag for behandlingen som Databehandleren skal utføre etter Databehandleravtalen.

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

Behandlingsansvarlige skal gi Databehandleren instrukser for hvordan personopplysningene skal behandles etter Databehandleravtalen. Instruksene er en del av Databehandleravtalen, men Behandlingsansvarlige kan til enhver tid endre instruksene under forutsetning av at instruksjonene ikke strider mot krav som følger av GDPR. Slike instrukser skal gis skriftlig.

4. Databehandlerens plikt til å handle etter instruks

Databehandleren kan bare behandle personopplysninger i henhold til Databehandleravtalen, Oppdragsavtalen og etter dokumenterte instrukser fra Behandlingsansvarlige, med mindre Databehandleren er underlagt lovfestede krav til å behandle personopplysningene. Dersom Databehandleren er underlagt slike krav, skal Databehandleren varsle Behandlingsansvarlige om dette før behandlingen iverksettes, med mindre loven forbyr slik underretning.

Databehandleren plikter å varsle Behandlingsansvarlige dersom Behandlingsansvarliges instruksjoner er i strid med krav som følger av GDPR eller annen lovgivning.

5. Taushetsplikt

Databehandleren skal sørge for at personopplysningene etter Databehandleravtalen bare er tilgjengelig for autoriserte personer. Databehandleren skal kun autorisere personer som har behov for tilgang til personopplysningene for å utføre tjenestene som beskrevet i Oppdragsavtalen. Databehandleren skal frata tilganger dersom behovet for tilgang ikke lenger er til stede.

Databehandleren skal sørge for at autoriserte personer med tilgang til personopplysningene er forpliktet til å behandle opplysningene konfidensielt. Behandlingsansvarlige kan kreve at Databehandleren dokumenterer at autoriserte personer er underlagt slik taushetsplikt. Plikten til å sikre personopplysningenes konfidensialitet gjelder også etter Databehandleravtalens opphør.

6. Informasjonssikkerhet

Databehandleren plikter å treffe og gjennomføre alle tekniske, organisatoriske og sikkerhetsmessige tiltak som er nødvendige i henhold til GDPR artikkel 32 og Databehandleravtalen.

Databehandleren skal, som minimum:

- Sørge for nødvendige tekniske og organisatoriske tiltak med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandlingen av personopplysninger på vegne av Behandlingsansvarlige for å sikre tilfredsstillende informasjonssikkerhet. Databehandleren skal gjennomføre regelmessige risikovurderinger for å fastsette hva som er tilfredsstillende informasjonssikkerhet.
- Gjennomføre internkontroll.
- Ha rutiner for autorisasjon og styring av tilganger som sikrer at det kun er personer med tjenstlig behov for tilgang til personopplysningene som har slik tilgang, og sørge for at disse etterleves.
- Ha rutiner for avvikshåndtering, og sørge for at disse etterleves.

- Sørge for at personopplysninger som omfattes av GDPR artikkel 9 om «særlige kategorier personopplysninger», og andre beskyttelsesverdige personopplysninger, som for eksempel personnummer og lønnsinformasjon, underlegges særlig beskyttelse og ikke sendes via ukryptert e-post.

7. Brudd på personopplysningssikkerheten

Ved brudd på personopplysningssikkerheten i henhold til GDPR artikkel 4 nr. 12, skal Databehandleren varsle Behandlingsansvarlige uten ugrunnet opphold etter å ha fått kjennskap til bruddet.

Dersom bruddet medfører at Behandlingsansvarlige må varsle tilsynsmyndigheten eller de registrerte, skal Databehandleren, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for Databehandleren, bistå Behandlingsansvarlige med å oppfylle forpliktelsene etter GDPR artikkel 33 nr. 3 og artikkel 34 nr. 3. I den grad det ikke er mulig å gi all informasjon samtidig som varselet, kan den gis trinnvis uten ytterligere ugrunnet opphold.

8. Underdatabehandlere

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

Behandlingsansvarlige gir Databehandleren en generell skriftlig tillatelse til bruk av underdatabehandlere. Ved inngåelse av Databehandleravtalen, har Databehandleren oppgitt at underdatabehandlere som er listet opp i vedlegg 1 vil bli benyttet for utføre de avtalte tjenestene. En fullstendig og oppdatert liste over BDOs underdatabehandlere finnes på BDOs nettsider.

Dersom Databehandleren gjør endringer i bruk av underdatabehandlere som ikke Behandlingsansvarlige er kjent med, skal Databehandleren underrette Behandlingsansvarlige om dette innen rimelig tid før underdatabehandleren engasjeres. Slik underretning skal skje ved at BDO oppdaterer listen over underdatabehandlere BDOs nettsider. Behandlingsansvarlige har rett til å motsette seg Databehandlerens bruk av underdatabehandlere så lenge dette er saklig begrunnet. Dersom Behandlingsansvarlige motsetter seg endringen, skal Databehandleren varsles så snart som mulig.

Dersom Databehandleren engasjerer en underdatabehandler for å utføre behandling av personopplysninger, skal det inngås en skriftlig avtale mellom som pålegger underdatabehandlerne de samme forpliktelsene som Databehandleren er underlagt etter denne Databehandleravtalen.

Databehandleren er fullt ut ansvarlig overfor Behandlingsansvarlige for ethvert brudd på forpliktelsene etter Databehandleravtalen som en underdatabehandler til Databehandleren gjør seg skyld i.

9. Overføring av personopplysninger

Databehandleren kan ikke uten skriftlig avtale med Behandlingsansvarlige overføre personopplysninger som behandles etter Databehandleravtalen til land utenfor EU/EØS-området («Tredjeland») eller til internasjonale organisasjoner, med mindre EU-kommisjonen har besluttet at landet eller den internasjonale organisasjonen har et tilstrekkelig beskyttelsesnivå eller Databehandleren er underlagt rettslige forpliktelser som krever slik overføring. Ved en eventuell overføring skal det foreligge nødvendige garantier i henhold til Personvernregelverket.

10. Databehandlerens bistand til behandlingsansvarlige

Dersom Databehandleren mottar henvendelser fra de registrerte i forbindelse med behandlingen av personopplysninger for den Behandlingsansvarlige, skal Databehandleren videreformidle henvendelsen til Behandlingsansvarlige uten ugrunnet opphold.

Databehandleren plikter, i den grad det er mulig og med hensyn til behandlingens art, å bistå Behandlingsansvarlige med å svare på henvendelser fra de registrerte om utøvelse av deres rettigheter.

Databehandleren skal også bistå Behandlingsansvarlige med å sikre overholdelse av forpliktelsene i GDPR artikkel 35 og 36, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren.

11. Revisjon

Databehandleren plikter å gjøre tilgjengelig for Behandlingsansvarlige all informasjon som er nødvendig for å påvise at Databehandleren etterlever sine forpliktelser etter Databehandleravtalen.

Databehandleren skal gjennomføre sikkerhetsrevisjoner av informasjonssystemer som benyttes til å behandle personopplysninger på vegne av Behandlingsansvarlige. Databehandleren kan benytte en uavhengig tredjepart til å gjennomføre sikkerhetsrevisjoner med Databehandleren. Databehandleren skal på forespørsel tilgjengeliggjøre for Behandlingsansvarlige oppsummeringen av revisjonen. På forespørsel, kan også detaljert rapport deles med Behandlingsansvarlige i et møte.

Databehandleren skal legge til rette for at Behandlingsansvarlige, tilsynsmyndigheter eller en tredjepart som Behandlingsansvarlige utpeker, kan gjennomføre egne revisjoner i henhold til Personvernregelverket, herunder inspeksjoner. Dersom en uavhengig tredjepart har gjennomført en sikkerhetsrevisjon med Databehandleren i løpet av de siste 12 månedene, og Databehandleren bekrefter at det ikke foreligger endringer etter dette, skal Behandlingsansvarlige imidlertid akseptere disse rapportene fremfor å etterspørre en ny revisjon.

Dersom tredjepartsrevisjonen ikke dekker Behandlingsansvarliges behov, kan det avtales egen revisjon med Databehandleren. Behandlingsansvarlige skal ha rett til å gjennomføre slik revisjon maks én gang per år og er selv ansvarlig for å dekke kostnadene ved revisjonen, herunder Databehandlers kostnader og tidsforbruk. Dersom slik revisjon skal inneholde en inspeksjon, skal Databehandleren varsles skriftlig og senest 30 dager før inspeksjonen skal gjennomføres. Inspeksjoner skal skje innenfor Databehandlerens alminnelige kontortider, og skal i minst mulig grad påvirke Databehandlerens daglige virksomhet. Dersom Behandlingsansvarlige utpeker en tredjepart til å gjennomføre revisjonen, skal tredjeparten være bundet av taushetsplikt i henhold til BDOs krav.

Behandlingsansvarliges rett til informasjon i forbindelse med revisjon skal være begrenset til det som er relatert til oppdraget som Databehandleren utfører på vegne av Behandlingsansvarlige. Behandlingsansvarlig skal ikke ha rett til tilgang til informasjon som gjelder Databehandlerens andre kunder og annen informasjon som er underlagt taushetsplikt.

12. Varighet og opphør

Databehandleravtalen trer i kraft når begge Parter har signert Databehandleravtalen og gjelder så lenge Oppdragsavtalen gjelder.

Ved brudd på Databehandleravtalen eller Personvernregelverket, kan Behandlingsansvarlige pålegge Databehandleren å stoppe behandlingen av opplysningene med øyeblikkelig virkning.

Ved opphør av Databehandleravtalen, skal Databehandleren på forespørsel returnere og/eller tilbakelevere alle personopplysninger som har blitt behandlet etter Databehandleravtalen, med mindre det er nødvendig å oppbevare personopplysningene lenger for å kunne dokumentere Databehandlerens oppdragsutførelse eller Databehandleren er underlagt rettslige forpliktelser om å oppbevare personopplysningene. Dette gjelder også for eventuelle sikkerhetskopier, men hvor det er tilstrekkelig med å overskrive etter Databehandlers etablerte rutiner for sikkerhetskopiering. Databehandleren skal på forespørsel gi Behandlingsansavarlige skriftlig bekreftelse på at personopplysningene er slettet.

13. Meddelelser

Meddelelser etter Databehandleravtalen skal sendes skriftlig til:

Behandlingsansvarlig	Databehandler
Navn: [Sett inn]	**Navn:** **[Sett inn]**
E-post: [Sett inn]	**E-post:** **[Sett inn]**
Telefon: **[Sett inn]**	**Telefon:** **[Sett inn]**

14. Lovvalg og verneting

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

Vedlegg 1: Underdatabehandlere

Navn	Type tjenester	Lokasjon for datasenter
Intility AS	Leverandør av IT-infrastruktur, herunder drift av applikasjoner, lagring og sikkerhetskopiering av data.	Norge
Brussel Worldwide Services BV/ BDO Global	Drift og utvikling av BDOs Kundeportal.	Nederland / Irland
Microsoft Ireland Operations Ltd.	Leverandør av Microsoft 365 og Azure.	Nederland / Irland
Tessian	Leverandør av programvare for å ivareta informasjonssikkerhet ved bruk av e-post.	Irland
Inmeta Consulting AS	Personell som bistår med utvikling og forbedring av IT-systemer.	I/A (kun personell som jobber i BDOs systemer)
[Sett inn eventuelle andre underdatabehandlere som benyttes]	[Beskriv tjenesten som leveres]	[Sett inn hvor personopplysningene lagres]