

Databehandleravtale

Er inngått mellom:

<Angi navn på virksomhet og organisasjonsnummer>
(heretter kalt Databehandler)

og

<Angi navn på virksomhet og organisasjonsnummer>
(heretter kalt Behandlingsansvarlig)

i fellesskap kalt Partene.

Sted og dato:

Avtaleparter

For Behandlingsansvarlig	For Databehandler
<u><Navn på den som signerer på vegne av Behandlingsansvarlig></u> _____ Underskrift	<u><Navn på den som signerer på vegne av Databehandler></u> _____ Underskrift

1 Formålet med denne Databehandleravtalen

- 1.1 Denne avtalen («Databehandleravtalen») fastsetter partenes rettigheter og plikter når Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige som del av leveransene under Hovedavtalen, jf. Bilag A. Databehandleravtalen har som formål å sikre at partene etterlever EUs personvernforordning («GDPR»), som er gjort til norsk rett gjennom personopplysningsloven.

Databehandleravtalen består av dette dokumentet, samt Bilag A, B og C.

- 1.2 Ved motstrid mellom Hovedavtalen (se Bilag A) og Databehandleravtalen, har Databehandleravtalen forrang når det gjelder forhold spesifikt knyttet til behandling av personopplysninger. Ved motstrid mellom Databehandleravtalen og dens bilag, har bilagene forrang.

- 1.3 Databehandleravtalens **Bilag A** inneholder nærmere beskrivelse av behandlingen som skal foretas, herunder om behandlingsformål, kategorier av personopplysninger og registrerte, regler for sletting og tilbakelevering, partenes kontaktpersoner, samt hvilken eller hvilke underliggende avtaler behandlingen av personopplysninger er knyttet til.

- 1.4 Databehandleravtalens **Bilag B** inneholder en oversikt over godkjente Underdatabehandlere og betingelser for å bruke eller endre dem.

- 1.5 Databehandleravtalens **Bilag C** inneholder spesifikke instruksjoner for behandling av personopplysninger under Hovedavtalen, herunder sikkerhetstiltak og dokumentasjonskrav.

2 Behandlingsansvarliges instruksjoner til Databehandleren

- 2.1 Behandlingsansvarlige har hovedansvaret for at behandlingen av personopplysninger skjer i samsvar med GDPR, jf. GDPR artikkel 5.

- 2.2 Databehandleren skal behandle personopplysningene i samsvar med GDPR og den Behandlingsansvarliges dokumenterte instruksjoner. Hvis annen behandling er nødvendig for å oppfylle forpliktelser som Databehandler er underlagt i henhold til gjeldende rett, skal Databehandleren underrette den Behandlingsansvarlige så langt dette er tillat ved lov, jf. GDPR artikkel 28 (3) (a).

- 2.3 Behandlingsansvarliges instruksjoner fremgår av Hovedavtalen og Databehandleravtalen med bilag. Databehandler skal omgående underrette den Behandlingsansvarlige, dersom vedkommende mener at instruksene er i strid med GDPR, jf. GDPR artikkel 28 (3) (h).

- 2.4 Eventuelle endringer i instruksjoner skal varsles til Databehandler, og skal implementeres av Databehandler innen det tidspunkt Partene avtaler eller (om ingen konkret frist er avtalt) innen rimelig tid.

3 Konfidensialitet og taushetsplikt

- 3.1 Databehandleren skal sikre at ansatte og andre som har tilgang til personopplysninger er autorisert til å behandle slike personopplysninger på Databehandlers vegne. Dersom slik autorisasjon utløper eller trekkes tilbake, skal tilgangen til personopplysningene opphøre uten ugrunnet opphold.
- 3.2 Databehandleren skal kun autorisere personer som trenger tilgang til personopplysningene i forbindelse med arbeid for å kunne oppfylle Hovedavtalen, Databehandleravtalen og eventuelt annen behandling som er nødvendig for å oppfylle forpliktelser som Databehandler er underlagt i henhold til GDPR.
- 3.3 Databehandleren skal sikre at personer som er autorisert til å behandle personopplysninger på vegne av den Behandlingsansvarlige er underlagt taushetsplikt gjennom avtale eller lov. Taushetsplikten skal bestå også etter avtalens og/eller ansettelsesforholdets opphør.
- 3.4 Databehandleren skal kunne dokumentere at de relevante personer er underlagt ovennevnte taushetsplikt på forespørsel fra den Behandlingsansvarlige.

4 BISTAND TIL BEHANDLINGSANSVARLIG

- 4.1 Databehandleren skal på forespørsel bistå Behandlingsansvarlig med oppfyllelse av de registrertes rettigheter etter GDPR kapittel III gjennom egnede tekniske eller organisatoriske tiltak. Plikten til å bistå gjelder likevel bare i den utstrekning dette er mulig og hensiktsmessig sett hen til karakteren og omfanget av behandlingen av personopplysninger under Hovedavtalen.
- 4.2 Databehandler skal uten ugrunnet opphold videresende alle henvendelser som Databehandler eventuelt mottar fra den registrerte vedrørende den registrertes rettigheter i henhold til GDPR til Behandlingsansvarlig. Slike henvendelser kan kun besvares av Databehandler når dette er skriftlig godkjent av Behandlingsansvarlig.
- 4.3 Databehandleren skal bistå den Behandlingsansvarlige med å overholde kravene til personopplysningssikkerhet i GDPR artikkel 32-36, herunder yte bistand ved personvernkonsekvensvurdering og forhåndsdrøftinger med Datatilsynet, sett hen til karakteren og omfanget av behandlingen av personopplysninger under Hovedavtalen.

5 Sikkerhet ved behandlingen

- 5.1 Databehandler skal iverksette egnede tekniske og organisatoriske tiltak for å oppnå et tilfredsstillende sikkerhetsnivå sett hen til behandlingens karakter og omfang, den tekniske

utviklingen, implementeringskostnader og aktuelle risikoer for fysiske personers rettigheter og friheter. Databehandleren skal som minimum iverksette de tiltak som eventuelt er spesifisert i Databehandleravtalens Bilag C.

- 5.2 Databehandleren skal foreta risikovurderinger for å sikre at et egnet sikkerhetsnivå opprettholdes til enhver tid. Databehandler skal dokumentere risikovurderingen og sikkerhetstiltakene, og gjøre dem tilgjengelig for Behandlingsansvarlige på forespørsel, samt gi adgang til slik revisjon som er avtalt mellom partene.

6 Melding om brudd på personopplysningssikkerheten

- 6.1 Databehandler skal uten ugrunnet opphold skriftlig underrette den Behandlingsansvarlige om eventuelle brudd på personopplysningssikkerheten, samt for øvrig gi slik bistand og informasjon som er nødvendig for at den Behandlingsansvarlige skal kunne melde bruddet til tilsynsmyndigheter i tråd med Gjeldende personvernregelverk.
- 6.2 Underretning etter punkt 6.1 skal meddeles kontaktpunktet for Behandlingsansvarlig i henhold til Bilag C. Informasjonen kan i den grad det er nødvendig gis trinnvis uten ytterligere ugrunnet opphold.
- 6.3 Behandlingsansvarlig er ansvarlig for å underrette Datatilsynet og de berørte registrerte om brudd på personopplysningssikkerheten. Databehandler skal ikke informere tredjeparter om brudd på personopplysningssikkerheten med mindre noe annet er påkrevd etter gjeldende rett eller det følger av uttrykkelig skriftlig instruks fra Behandlingsansvarlig.

7 Bruk av Underdatabehandler

- 7.1 Underdatabehandler er en annen virksomhet som benyttes av Databehandler som underleverandør til behandling av personopplysninger under Hovedavtalen.
- 7.2 Databehandler kan kun benytte Underdatabehandler etter forutgående generell eller spesifikk skriftlig tillatelse fra Behandlingsansvarlig i samsvar med Databehandleravtalens Bilag B. Oversikt over godkjente Underdatabehandlere fremgår av Databehandleravtalens Bilag B.
- 7.3 Dersom en Databehandler engasjerer en Underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den Behandlingsansvarlige, plikter Databehandler å inngå skriftlig avtale med Underdatabehandleren som pålegger denne tilsvarende forpliktelser med hensyn til vern av personopplysninger som Databehandleren selv er underlagt etter denne Databehandleravtalen.
- 7.4 Databehandler skal kun engasjere Underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene etter Gjeldende

personvernregler. Databehandler skal gjennomføre kontroller av Underdatabehandlere for å verifisere at tilfredsstillende tiltak er iverksatt. Databehandler skal kunne fremlegge dokumentasjon fra slike kontroller for Behandlingsansvarlig på forespørsel.

7.5 Dersom Behandlingsansvarlig motsetter seg endringer i bruken av Underdatabehandlere etter Databehandleravtalens Bilag B, skal Partene i god tro forhandle med sikte på å enes om en rimelig løsning på hvordan videre levering av tjenestene under Hovedavtalen skal gjennomføres, herunder om fordeling av eventuelle kostnader mellom Partene. Endringen i bruk av Underdatabehandlere kan ikke gjennomføres før Partene har kommet til enighet.

7.6 Dersom Underdatabehandleren ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, skal Databehandleren overfor den Behandlingsansvarlige ha fullt ansvar på samme måte som om Databehandler selv sto for behandlingen.

8 Overføring av personopplysninger til land utenfor EØS-området

8.1 Personopplysninger kan bare overføres til et land utenfor EØS-området («Tredjestat») eller til internasjonal organisasjon hvis Behandlingsansvarlig skriftlig har godkjent slik overføring.

8.2 Databehandler kan likevel overføre personopplysninger dersom det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandler underrette Behandlingsansvarlig så langt dette er tillat ved lov.

8.3 Overføring til Tredjestater eller internasjonale organisasjoner kan kun finne sted dersom det foreligger nødvendige garantier for et tilstrekkelig beskyttelsesnivå for personvern i henhold til GDPR. Med mindre annet er avtalt mellom Partene kan slik overførsel kun finne sted med grunnlag i:

- a) en av EU-kommisjonens beslutninger om tilstrekkelig beskyttelsesnivå i henhold til GDPR artikkel 45; eller
- b) en Databehandleravtale som inkorporerer standard personvernbestemmelser som angitt i GDPR artikkel 46 (2) (c) eller (d) (EU Model clauses); eller
- c) bindende virksomhetsregler (Binding Corporate Rules) i henhold til GDPR artikkel 47.

9 Generelt om revisjon

9.1 Databehandler skal på forespørsel gjøre tilgjengelig for den Behandlingsansvarlige, all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i GDPR artikkel 28 og denne Databehandleravtalen er oppfylt.

- 9.2 Databehandler skal muliggjøre og bidra ved inspeksjoner og revisjoner som gjennomføres av eller på oppdrag fra Behandlingsansvarlig. Den Behandlingsansvarliges tilsyn med eventuelle Underdatabehandler skal skje gjennom Databehandleren med mindre annet er særskilt avtalt.
- 9.3 Dersom en revisjon avdekker avvik fra forpliktelsene i GDPR eller Databehandleravtalen, skal Databehandler så snart som mulig utbedre avviket. Behandlingsansvarlig kan kreve at Databehandleren midlertidig stopper hele eller deler av behandlingsaktivitetene frem til utbedringen er godkjent av Behandlingsansvarlig.
- 9.4 Hver av Partene dekker sine egne kostnader forbundet med en revisjon.

10 Sletting og tilbakelevering av opplysninger

- 10.1 Ved opphør av denne Databehandleravtalen plikter Databehandler å tilbakelevere og slette alle personopplysninger som behandles på vegne av Behandlingsansvarlig, i henhold til den Behandlingsansvarliges instruks. Dette gjelder også eventuelle sikkerhetskopier. Behandlingsansvarlig bestemmer hvordan en eventuell tilbakelevering av personopplysninger skal skje.
- 10.2 Databehandler skal bekrefte skriftlig overfor Behandlingsansvarlig at sletting eller utilgjengeliggjøring er foretatt og skal på forespørsel dokumentere hvordan det er gjennomført.

11 Varighet og opphør

- 11.1 Databehandleravtalen gjelder fra den er signert av begge Parter. Databehandleravtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig. Den gjelder også for eventuelle personopplysninger som måtte finnes hos Databehandler eller noen av dennes Underdatabehandler etter Hovedavtalens opphør.
- 11.2 Reglene om oppsigelse i Hovedavtalen gjelder tilsvarende for Databehandleravtalen, så langt det passer. Databehandleravtalen kan ikke sies opp så lenge Hovedavtalen består med mindre den avløses av en ny databehandleravtale.
- 11.3 Ved brudd på Databehandleravtalen og/eller GDPR, kan Behandlingsansvarlig pålegge Databehandler å stoppe hele eller deler av behandlingen av opplysningene med øyeblikkelig virkning.

12 Erstatning og overtredelsesgebyrer

- 12.1 Partenes erstatningsansvar for skade som rammer den registrerte eller andre fysiske personer og som skyldes overtredelse av GDPR, personopplysningsloven med forskrifter eller annet regelverk som gjennomfører GDPR, følger bestemmelsene i GDPR artikkel 82.
- 12.2 Partene er hver for seg ansvarlige for overtredelsesgebyr ilagt i henhold til GDPR artikkel 83.

13 Lovvalg og vernetting

Databehandleravtalen er underlagt norsk rett. Tvister løses i samsvar med Hovedavtalens bestemmelser, herunder eventuelle bestemmelser om vernetting.

BILAG TIL DATABEHANDLERAVTALEN

DOKUMENTET BESTÅR AV FØLGENDE BILAG:

BILAG A – OPPLYSNINGER OM BEHANDLINGEN

BILAG B – BETINGELSER FOR DATABEHANDLERENS BRUK AV UNDERDATABEHANDLERE

BILAG C – INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER

BILAG A: OPPLYSNINGER OM BEHANDLINGEN

- 13.1 Hovedavtalen og formålet med behandlingen av personopplysninger
- Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige er knyttet til å levere tjenester som beskrevet i Hovedavtalen.

Med Hovedavtalen menes følgende avtale(r) inngått mellom partene:

<Sett inn navn og dato for inngåelse av den eller de underliggende tjenesteavtalen(e) som Databehandleravtalen er knyttet til.>

Behandlingen har følgende formål:

Beskriv behandlingsformål, for eksempel:

- **Levering av lagringstjenester som nærmere beskrevet i annen [Avtale].**

- 13.2 Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige
- Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige omhandler (karakteren av behandlingen):

Beskriv hva behandlingen omfatter, for eksempel:

- **Registrering, organisering og oppbevaring av personopplysninger i system X**

Typer av personopplysninger

Behandlingen omfatter følgende typer av personopplysninger om de registrerte (flere valg mulig):

☐	Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 (1): <Angi type, f.eks. helseopplysninger, rasemessig eller etnisk opprinnelse eller fagforeningstilhørighet>
☐	Andre opplysninger med særlig behov for beskyttelse: <Angi type, f.eks. fødselsnummer, opplysninger om økonomi, prestasjonsvurderinger i ansettelsesforhold osv.>
☐	Andre personopplysninger: <Angi type, f.eks. navn og kontaklinformasjon, utdanning, kommunikasjonspreferanser osv.>

- 13.3 Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

<Beskriv hvem behandlingen av personopplysninger omfatter, for eksempel: Ansatte i Kolumbus, skolelever.>

Dersom det behandles opplysninger om en særlig sårbar eller utsatt gruppe som f.eks. barn eller handikappede bør det oppføres særskilt.>

13.4 Varighet av behandlingen

Databehandlers behandling av personopplysninger under Hovedavtalen kan påbegynne når Databehandleravtalen har trådt i kraft. Behandlingen har følgende varighet (velg ett alternativ):

☐	Behandlingen er ikke tidsbegrenset, og varer frem til opphør av Hovedavtalen.
☐	Behandlingen er tidsbegrenset, og gjelder frem til <i><angi dato eller kriterium for avslutning, eksempelvis avslutningen av et prosjekt. Merk at behandlingen normalt ikke kan avslutte før Hovedavtalen utløper>.</i>

14 BETINGELSER FOR DATABEHANDLERENS BRUK OG ENDRING AV EVENTUELLE UNDERDATABEHANDLERE

14.1 Behandlingsansvarliges godkjennelse av bruk av Underdatabehandlere

Ved inngåelse av Databehandleravtalen godkjenner Behandlingsansvarlig bruk av de Underdatabehandlere som er oppført i punkt 14.2. Merk at også mor-, søster- og datterselskaper til Databehandleren regnes som Underdatabehandlere hvis de bidrar til leveransen og behandler personopplysninger.

For endringer i bruk av Underdatabehandlere er det i tillegg avtalt følgende:

☐	Databehandleren kan benytte Underdatabehandler som i samme konsern (mor-søster- eller datterselskap) som er etablert i et land innenfor EØS-området. Databehandleren skal på forhånd informere Behandlingsansvarlige om bruken av slik Underdatabehandler. (Dette alternativet kan kombineres med et av de andre alternativene.)
☐	Databehandler kan gjennomføre endringer i bruken av Underdatabehandlere forutsatt at den Behandlingsansvarlige underrettes og gis mulighet til å motsette seg endringene. En slik underretning skal være mottatt av Behandlingsansvarlig senest 1 måned før endringen trer i kraft, med mindre annet er avtalt skriftlig mellom partene. Merk at endringer som medfører overføring av personopplysninger til land utenfor EØS-området (Tredjestater) uansett krever skriftlig godkjenning etter Databehandleravtalens punkt 10. Hvis Behandlingsansvarlig motsetter seg endringen skal Databehandler underrettes så snart som mulig. Den behandlingsansvarlige kan ikke motsette seg endringen uten saklig grunn.
☐	Databehandler kan kun gjennomføre endringer i bruken av Underdatabehandlere etter spesifikk og forutgående skriftlig godkjennelse fra Behandlingsansvarlig. Underdatabehandleren kan ikke behandle personopplysninger under Hovedavtalen før slik godkjennelse er gitt. Godkjennelse kan ikke nektes uten saklig grunn.

14.2 Godkjente Underdatabehandlere

Den Behandlingsansvarlige har godkjent bruk av følgende Underdatabehandlere:

Navn	Org.nr.	Adresse	Beskrivelse av behandling
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]
[Navn]	[Org.nr.]	[Adresse]	[Overordnet beskrivelse av behandlingen hos Underdatabehandleren]

15 INSTRUKS VEDRØRENDE BEHANDLING AV PERSONOPPLYSNINGER

15.1 Behandlingens omfang og formål

Personopplysningene skal utelukkende behandles i det omfang og for de formål som er beskrevet i

- Hovedavtalen
- Databehandleravtalen med bilag

Databehandler har ikke råderett over personopplysningene utover det som er nødvendig for å oppfylle sine plikter etter Databehandleravtalen, og kan ikke behandle disse til egne formål.

15.2 Sikkerhet ved behandlingen

[Angi relevante tiltak ved behov]

15.3 Dokumentasjon

Databehandler skal dokumentere de rutiner og tiltak som er iverksatt for å oppfylle kravene som fremkommer av GDPR og Databehandleravtalen, herunder kravene til informasjonssikkerhet. Slik dokumentasjon skal oppbevares og ajourholdes så lenge Databehandleravtalen består, og gjøres tilgjengelig for Behandlingsansvarlig eller tilsynsmyndigheter på forespørsel.

15.4 Kontaktinformasjon

Ved henvendelser i henhold til denne avtalen, eksempelvis ved varsling om brudd på personopplysningssikkerheten eller endring i bruk av underdatabehandlere, skal følgende kanaler benyttes:

Hos Behandlingsansvarlig

Sikkerhetsbrudd:

Telefon: [Fyll ut]

E-post [Fyll ut]

Andre henvendelser:

Navn: [Fyll ut]

Stilling: [Fyll ut]

Telefon: [Fyll ut]

E-post: [Fyll ut]

Hos Databehandleren

Sikkerhetsbrudd:

Telefon: [Fyll ut]

E-post [Fyll ut]

Andre henvendelser:

Navn: [Fyll ut]

Stilling: [Fyll ut]

Telefon: [Fyll ut]

E-post: [Fyll ut]