****

## Databehandleravtale

mellom

[Navn på institusjonen]

[Org. nr.]

[Adresse]

 (heretter kalt «Behandlingsansvarlig»)

og

[Navn på tjenesteleverandøren]

[Org. nr.]

[Adresse]

 (heretter kalt «Databehandler»)

## 1. Avtalens hensikt

Partene har inngått en avtale om levering av tjenester («Hovedavtalen») som innebærer behandling av personopplysninger.

Denne databehandleravtalen («Databehandleravtalen») regulerer partenes rettigheter og plikter når Databehandleren behandler personopplysninger på vegne av Behandlingsansvarlig. Formålet med Databehandleravtalen er å sikre at personopplysningene behandles i samsvar med forordning 2016/679/EU («GDPR») og annen gjeldende personvernlovgivning.

Ved motstrid skal vilkårene i denne Databehandleravtalen gå foran Databehandlerens personvernerklæring eller vilkår i Hovedavtalen inngått mellom Behandlingsansvarlig og Databehandleren.

## 2. Formålsbegrensning

Formålet med Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig er å levere og administrere tjenester som beskrevet i Hovedavtalen. En nærmere beskrivelse av formålet med behandlingen følger av Vedlegg 1. Databehandleren kan ikke behandle personopplysningene for andre formål uten at dette på forhånd er skriftlig godkjent av Behandlingsansvarlig.

## 3. Opplysningstyper og kategorier av registrerte

En oversikt over hvilke typer personopplysninger og hvilke kategorier av registrerte som Databehandleren behandler på vegne av Behandlingsansvarlig under denne Databehandleravtalen følger av Vedlegg 1.

## 4. Instrukser

Databehandleren skal bare behandle personopplysninger i henhold til dokumenterte instrukser fra Behandlingsansvarlig. Detaljerte instrukser til databehandler beskrives i vedlegg 1.

Dette gjelder også med hensyn til overføring av personopplysninger til en tredjestat eller en internasjonal organisasjon, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som Databehandleren er underlagt. I så fall skal Databehandleren underrette den Behandlingsansvarlige om nevnte rettslige krav før behandlingen, men mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning.

Databehandleren skal overholde alle bestemmelser i denne Databehandleravtalen, i GDPR og annen gjeldende personvernlovgivning.

Databehandleren forplikter seg til å varsle Behandlingsansvarlig omgående dersom Databehandleren mener at mottatte instrukser er i strid med GDPR eller annen gjeldende personvernlovgivning.

## 5. Taushetsplikt

Kun ansatte eller andre personer hos Databehandleren som har tjenstlige behov for tilgang til personopplysninger som behandles på vegne av Behandlingsansvarlig, kan gis slik tilgang.

Databehandleren skal sikre at slike ansatte eller andre personer som er autorisert til å behandle personopplysningene er underlagt taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til denne Databehandleravtalen. Denne bestemmelsen gjelder også etter avtalens opphør. Taushetsplikten omfatter ansatte hos tredjeparter som utfører vedlikehold (eller liknende oppgaver) av systemer, utstyr, nettverk eller bygninger som Databehandleren anvender for å levere eller administrere tjenesten etter Hovedavtalen.

## 6. Informasjonssikkerhet

Databehandleren skal gjennomføre egnede tekniske, fysiske og organisatoriske sikringstiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, blant annet for å beskytte personopplysninger som omfattes av denne Databehandleravtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet. Databehandleren skal treffe alle tiltak som er nødvendige i henhold til GDPR artikkel 32, samt bistå Behandlingsansvarlig med å sikre overholdelse av sine forpliktelser etter denne bestemmelsen. Sikkerhetstiltak listes opp i Vedlegg. 1.

Som et minimum skal Databehandleren foreta risikovurderinger og etablere tiltak for å mitigere risiko, etablere beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser og gi ansatte informasjon og opplæring i informasjonssikkerhet. Databehandleren skal også gjennomføre jevnlige sikkerhetsrevisjoner av eget arbeid med sikring av personopplysninger, systemer og lignende som er relevant for behandlingen av personopplysninger knyttet til tjenesten som leveres under Hovedavtalen.

## 7. De registrertes rettigheter

Databehandleren skal i den grad det er mulig med hensyn til behandlingens art og ved hjelp av egnede tekniske og organisatoriske tiltak bistå Behandlingsansvarlig med å svare på henvendelser fra de registrerte om utøvelse av deres rettigheter.

De registrertes rettigheter inkluderer retten til informasjon om hvordan hans eller hennes personopplysninger behandles, retten til å kreve innsyn i egne personopplysninger, retten til å kreve retting eller sletting av egne personopplysninger, retten til å protestere mot behandlingen og retten til å kreve at behandlingen av egne personopplysninger begrenses.

I den grad det er relevant, skal Databehandleren bistå Behandlingsansvarlig med å ivareta de registrertes rett til dataportabilitet og retten til å motsette seg automatiske avgjørelser, inkludert profilering.

## 8. Varsling ved sikkerhetsbrudd

Databehandleren skal bistå Behandlingsansvarlig med å overholde sine varslingsforpliktelser i henhold til GDPR artikkel 33 og 34.

Dersom personopplysninger som behandles på vegne av Behandlingsansvarlig utsettes for sikkerhetsbrudd som innebærer risiko for de registrertes rettigheter og friheter, skal Databehandleren uten ubegrunnet opphold og senest innen 36 timer varsle Behandlingsansvarlig ved å sende e-epost til sikkerhet@oslomet.no.

Varselet til Behandlingsansvarlig skal som minimum inneholde informasjon som beskriver sikkerhetsbruddet, hvilke registrerte som er berørt av sikkerhetsbruddet, hvilke personopplysninger som er berørt av sikkerhetsbruddet, hvilke strakstiltak som er iverksatt for å håndtere sikkerhetsbruddet og hvilke forebyggende tiltak som eventuelt er etablert for å unngå liknende hendelser i fremtiden.

Behandlingsansvarlig er ansvarlig for at varsler om sikkerhetsbrudd fra Databehandleren blir videreformidlet til Datatilsynet og for at de registrerte underrettes om sikkerhetsbruddet dersom Behandlingsansvarlig finner at det vil medføre en høy risiko for de registrertes rettigheter og friheter.

## 9. Konsekvensutredninger

Databehandleren skal bistå Behandlingsansvarlig med å sikre overholdelse av sine forpliktelser i henhold til GDPR artikkel 35 og 36. Dersom det etter Behandlingsansvarliges oppfatning er nødvendig å foreta en vurdering av personvernkonsekvenser etter GDPR artikkel 35, skal Databehandleren bistå Behandlingsansvarlig med denne vurderingen og om nødvendig iverksetting av personvernfremmende tiltak dersom konsekvensutredningen viser at dette er nødvendig. Dersom det etter vurderingen av personvernkonsekvenser er nødvendig å gjennomføre en forhåndsdrøfting med Datatilsynet etter GDPR artikkel 36, skal Databehandleren bistå Behandlingsansvarlig med disse drøftelsene.

## 10. Informasjon og revisjon

Databehandleren skal på forespørsel gi den Behandlingsansvarlige tilgang til all informasjon og dokumentasjon som er nødvendig for å påvise at forpliktelsene fastsatt i denne Databehandleravtalen er oppfylt.

Denne informasjonen og dokumentasjonen omfatter, men er ikke begrenset til, dokumentasjon på sikkerhetstiltak som nevnt i punkt 6 (risikovurderinger og etablerte sikringstiltak, beredskapsplanene for håndtering av alvorlige sikkerhetshendelser, rutiner for informasjon og opplæring av ansatte, rapporter fra egne sikkerhetsrevisjoner, etc), tilgangsdokumentasjon (retningslinjer og rutiner for tilgangsstyring), underdatabehandleravtaler, grunnlag for overføring til tredjeland og annen dokumentasjon som er nødvendig for at Behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til GDPR og annen gjeldende personvernlovgivning.

Ansatte hos Behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som Databehandleren gjør tilgjengelig for Behandlingsansvarlig.

Databehandleren skal bidra til å muliggjøre revisjoner og inspeksjoner som gjennomføres av Behandlingsansvarlig eller en tredjepart på fullmakt fra Behandlingsansvarlig. Ved bruk av tredjepart skal det utarbeides en rapport som vil bli overlevert Behandlingsansvarlig, og som Behandlingsansvarlig kan vise til Datatilsynet eller andre som har behov for å kjenne innholdet.

## 11. Underleverandører

Dersom Databehandleren benytter underleverandører, plikter Databehandleren å sørge for at underleverandøren gir tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i GDPR og annen gjeldende personvernlovgivning. Databehandleren plikter også å inngå egne avtaler som pålegger underleverandørene de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i denne Databehandleravtalen. Databehandleren skal sikre at underleverandøren overholder forpliktelsene som Databehandleren er underlagt i henhold til denne Databehandleravtalen og i henhold til GDPR og annen gjeldende personvernlovgivning.

Enhver underleverandør skal godkjennes skriftlig av Behandlingsansvarlig før underleverandøren kan behandle personopplysninger. Behandlingsansvarlig godkjenner at Databehandleren engasjerer underleverandørene som er angitt i Vedlegg 1. Databehandleren kan ikke engasjere andre underleverandører enn de som er nevnt i Vedlegg 1 uten at dette på forhånd er skriftlig godkjent av Behandlingsansvarlig.

## 12. Overføring til land utenfor EU/EØS

Overføring av personopplysninger til tredjeland eller bruk av underleverandører i tredjeland kan bare skje på instruks fra Behandlingsansvarlig. Dette omfatter også fjerntilgang fra utlandet. Ved enhver slik overføring til tredjeland eller bruk av underleverandører i tredjeland skal Databehandleren sikre at bestemmelsene i GDPR og annen gjeldende personvernlovgivning overholdes, inkludert at overføringen skjer i overensstemmelse med et av de godkjente overføringsgrunnlagene i GDPR kapittel V.

En oversikt over hvilke tredjeland personopplysningene som Databehandler behandler i henhold til denne Databehandleravtalen vil bli overført til og grunnlaget for overføringene følger av Vedlegg 1.

## 13. Tilbakelevering og sletting

Ved opphør av denne Databehandleravtalen plikter Databehandleren å slette og tilbakelevere alle personopplysninger som behandles på vegne av Behandlingsansvarlig i forbindelse med levering av tjenester under Hovedavtalen. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

Databehandleren skal stanse behandlingen av og slette personopplysningene fra alle lagringsmedier uten ugrunnet opphold etter Databehandleravtalens opphør, inkludert sikkerhetskopier. Databehandleren skal på forespørsel fra Behandlingsansvarlig gi en skriftlig erklæring på at sletting av personopplysninger er foretatt i henhold til denne Databehandleravtalen. Databehandler dekker alle kostnader i forbindelse med tilbakelevering og sletting av de personopplysninger som omfattes av denne Databehandleravtalen.

## 14. Mislighold og ansvar

Dersom Databehandleren ikke overholder sine plikter etter denne Databehandleravtalen eller etter GDPR og annen gjeldende personvernlovgivning, anses det som mislighold av denne Databehandleravtalen og Hovedavtalen. Ved slikt mislighold kan Behandlingsansvarlig si opp Hovedavtalen med øyeblikkelig virkning. Databehandleren vil fortsatt være pliktig til å tilbakelevere og slette personopplysninger som behandles på vegne av Behandlingsansvarlig i henhold til bestemmelsene i punkt 13 ovenfor.

Behandlingsansvarlig kan kreve erstatning for økonomiske tap, herunder administrative overtredelsesgebyr og erstatningskrav som rettes mot Behandlingsansvarlig, som skyldes Databehandlerens brudd på sine plikter etter denne Databehandleravtalen eller etter GDPR og annen gjeldende personvernlovgivning. I den grad det økonomiske tapet skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos Databehandlerens underleverandører, er Databehandleren på samme måte erstatningsansvarlig overfor Behandlingsansvarlig.

## 15. Avtalens varighet

Denne Databehandleravtalen gjelder så lenge Hovedavtalen løper, eller inntil Databehandlerens plikt til å levere tjenester under Hovedavtalen opphører av annen grunn.

## 16. Kontaktpersoner

Kontaktpersoner hos Databehandleren og Behandlingsansvarlig for spørsmål knyttet til denne Databehandleravtalen er oppført i Vedlegg 1.

## 17. Lovvalg, tvister og verneting

Partenes rettigheter og plikter etter denne Databehandleravtalen bestemmes i sin helhet av norsk rett. Eventuelle tvister som springer ut av denne Databehandleravtalen skal først søkes løst gjennom forhandlinger. Dersom partene ikke oppnår enighet gjennom forhandlinger, skal tvisten løses med bindende virkning av Oslo tingrett. Dersom Databehandleren er et annet statlig universitet eller høyskole, skal tvisten løses med bindende virkning av Kunnskapsdepartementet og hver av partene kan forlange at tvisten oversendes departementet.

\*\*\*

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

|  |  |
| --- | --- |
| Sted og dato:  | Sted og dato: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_På vegne av Behandlingsansvarlig | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_På vegne av Databehandler |
| Navn: | Navn: |
| Stilling: | Stilling: |

## Vedlegg 1

## Formål med behandlingen

[Angi formålet med behandlingen. Dette vil være å levere tjenesten i henhold til Hovedavtalen. Gi en oppsummering av hvilke tjenester Hovedavtalen går ut på.]

## Behandlingsaktiviteter

[Angi typer behandlingsaktiviteter, for eksempel innsamling, analyse, testing, arkivering etc.]

## Kategorier av datasubjekter

[Angi kategorier av datasubjekter som det behandles personopplysninger om, for eksempel ansatte, studenter, leverandører, etc.]

## Typer av personopplysninger

[Angi de typer personopplysninger som blir behandlet om datasubjektene, for eksempel navn, adresser, telefonnumre, e-postadresser, etc. Dersom det er relevant, oppgi også hvilke særlige kategorier av personopplysninger som blir behandlet.]

1. **Instrukser**

[Formuler en instruks for datahåndtering der det opplyses hvordan data skal samles inn, sendes, deles, analyseres, lagres, hvilke digitale verktøy som skal brukes m.m.]

1. **Informasjonssikkerhet**

[Gi en spesifikasjon av iverksatte sikkerhetstiltak der det opplyses egnede tekniske, fysiske og organisatoriske sikringstiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, for å hindre uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.]

## Underleverandører i EU/EØS

|  |  |
| --- | --- |
| **Navn** | **Behandlingsaktivitet** |
| [Schibsted] | [Markedsføring] |
|  |  |
|  |  |

## Underleverandører utenfor EU EØS

|  |  |  |  |
| --- | --- | --- | --- |
| **Navn** | **Behandlingsaktivitet** | **Land** | **Overføringsgrunnlag** |
| [Microsoft Azure] | [Skyleverandør] | [USA] | [Data Privacy Framework] |
|  |  |  |  |
|  |  |  |  |

## Kontaktpersoner

Kontaktperson for Behandlingsansvarlig: [Navn, e-post, telefon]

Kontaktperson for Databehandler: [Navn, e-post, telefon]