

## Avtale om felles behandlingsansvar

mellom

OsloMet - Storbyuniversitetet

Org. nr.: 997 058 925

Postboks 4, St. Olavs plass

0130 Oslo

Norge

(heretter kalt «Behandlingsansvarlig 1»)

og

[Navn på institusjon]

[Org. nr.]

[Adresse]

(heretter kalt «Behandlingsansvarlig 2»)

## Avtalens hensikt

Partene har inngått en avtale om gjennomføring av et prosjektsamarbeid («Hovedavtalen») som innebærer behandling av personopplysninger. Denne behandlingen innebærer et felles behandlingsansvar mellom partene, ettersom begge partene i fellesskap fastsetter formålene med og midlene for behandlingen.

Denne avtalen («Avtalen») fastsetter partenes respektive ansvar for å overholde forpliktelsene etter forordning 2016/679/EU («GDPR») og annen gjeldende personvernlovgivning i forbindelse med behandlingen av personopplysningene. Denne Avtalen utgjør ordningen som er påkrevd etter og beskrevet i GDPR artikkel 26, og skal særlig regulere ansvaret partene imellom med hensyn til utøvelse av den registrertes rettigheter og den plikt de har til å framlegge informasjonen nevnt i artikkel 13 og 14.

Ved motstrid skal vilkårene i denne Avtalen gå foran partenes personvernerklæringer eller vilkår i Hovedavtalen inngått mellom partene.

## Formål og beskrivelse av de felles behandlingsaktivitetene

Formålet med den felles behandlingen er å gjennomføre prosjektsamarbeidet som beskrevet i Hovedavtalen. Partene skal ikke behandle personopplysningene for andre formål enn de som er oppgitt i denne Avtalen eller i større utstrekning enn det som er nødvendig for å oppfylle sine plikter etter Hovedavtalen, med mindre annet følger av ufravikelig lov. I så fall skal den andre parten underrettes om denne rettslige forpliktelsen før behandlingen tar til, med mindre den nevnte lovgivningen forbyr slik underretning.

En nærmere beskrivelse av formålet med den felles behandlingen, hvilke typer personopplysninger som behandles om hvilke kategorier av registrerte, samt av partenes respektive roller og ansvarsfordeling i relasjon til den felles behandlingen følger av Vedlegg 1. Disse spesifikasjonene kan ikke endres av noen av partene uten en skriftlig endring av denne Avtalen.

## Overholdelse av GDPR og annen gjeldende personvernlovgivning

Ved å undertegne denne Avtalen bekrefter partene følgende:

* Partene skal overholde alle bestemmelser i GDPR og annen gjeldende personvernlovgivning i forbindelse med behandling av personopplysninger etter denne Avtalen, inkludert, men ikke begrenset til, overholdelse av personvernprinsippene i GDPR artikkel 5.
* Partene skal ha et gyldig rettslig grunnlag i samsvar med GDPR artikkel 6, 9 og 10 for sin behandling av personopplysninger etter denne Avtalen.
* Partene overholder kravet i GDPR artikkel 30 om protokoll over behandlingsaktiviteter, herunder fører en protokoll over den behandlingen som partene er felles behandlingsansvarlig for, og orienterer hverandre om innholdet i sine protokoller.
* Partene skal holde hverandre informert om vesentlige forhold av betydning for den felles behandling og av betydning for denne Avtalen, herunder forhold som påvirker eller kan påvirke partens evne til å behandle personopplysningene i samsvar med denne Avtalen eller oppfylle vilkårene i GDPR eller annen gjeldende personvernlovgivning for øvrig.

## Taushetsplikt

Begge parter skal sørge for at det bare er ansatte eller andre personer hos parten som har tjenstlige behov for tilgang til personopplysningene som behandles i henhold til denne Avtalen som gis slik tilgang. Begge parter skal også 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 Avtalen. 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 en av partene anvender for å utføre samarbeidet etter Hovedavtalen.

## Informasjonssikkerhet

Begge parter er ansvarlige for å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er egnet med hensyn til risikoen, blant annet for å beskytte personopplysninger som omfattes av denne Avtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet, og for å treffe alle tiltak som er nødvendige i henhold til GDPR artikkel 32. Partene skal dokumentere hvilke tekniske og organisatoriske tiltak de har etablert.

Begge parter skal som et minimum gjennomføre risikovurderinger og gjennomføre tiltak for å begrense identifiserte risikoer, etablere beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser, gi ansatte informasjon og opplæring i informasjonssikkerhet og gjennomføre jevnlige sikkerhetsrevisjoner av eget arbeid med sikring av personopplysninger, systemer og lignende som er relevant for behandlingen av personopplysninger knyttet til samarbeidet som utføres under Hovedavtalen. Partene skal dokumentere sitt arbeid med informasjonssikkerhet. Begge parter er også ansvarlig for overholdelse av bestemmelsen om innebygd personvern og personvern som standardinnstilling i GDPR artikkel 25.

## De registrertes rettigheter

Begge parter er ansvarlig for å sikre de registrertes rettigheter i samsvar med GDPR kapittel 3 og annen gjeldende personvernlovgivning. Dersom en part mottar en anmodning eller henvendelse fra en registrert om forhold som er omfattet av den annen parts ansvar, skal henvendelsen oversendes til den annen part for besvarelse snarest mulig. Partene er ansvarlige for å bistå hverandre i det omfang det er relevant og nødvendig for at begge parter kan etterleve forpliktelsene overfor de registrerte.

Begge parter skal sørge for at de registrerte får informasjon om behandlingen av personopplysninger i samsvar med GDPR artikkel 13 og 14.

I forbindelse med oppfyllelse av informasjonsplikten skal partene også gjøre det vesentligste innholdet i denne Avtalen tilgjengelig for de registrerte. Dette omfatter som et minimum følgende:

* Informasjon om at det foreligger et felles behandlingsansvar
* Identiteten til de felles behandlingsansvarlige
* Informasjon om rollene til hver av de felles behandlingsansvarlige i forbindelse med den felles databehandlingen slik dette er beskrevet i Vedlegg 1
* Informasjon om at hver av de behandlingsansvarlige har plikt til å oppfylle de registrertes rettigheter etter GDPR kapittel 3
* Kontaktpunkt for de registrerte i henhold til punkt 7 og Vedlegg 1

## Kontaktpunkt for de registrerte

Partene kan oppnevne et kontaktpunkt for de registrerte i Vedlegg 1. Dersom slik kontaktpunkt er oppnevnt, kan de registrerte henvende seg til dette kontaktpunktet for spørsmål angående utøvelse sine rettigheter. Kontaktpunktet vil deretter oversende henvendelsen til den parten som har ansvar for det relevante forholdet. Begge parterhar allikevel et selvstendig ansvar for å sørge for at de registrertes rettigheter ivaretas.

## Varsling ved sikkerhetsbrudd

Dersom personopplysninger som er gjenstand for felles behandlingsansvar under denne Avtalen utsettes for et sikkerhetsbrudd, er begge parter er ansvarlig for overholdelse av GDPR artikkel 33 og 34 om melding av brudd på personopplysningssikkerhet til tilsynsmyndigheten og/eller de registrerte. Partene skal bli enige om hvilken av partene som skal oppfylle varslingsforpliktelsene i det enkelte tilfellet.

Begge parter skal uten ugrunnet opphold varsle den andre parten dersom personopplysninger som behandles under denne Avtalen utsettes for sikkerhetsbrudd. Varselet skal som et 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.

## Konsekvensutredninger

Begge parter er ansvarlige for å foreta en vurdering av personvernkonsekvenser dersom dette er nødvendig etter GDPR artikkel 35. Begge parter er tilsvarende forpliktet til å overholde kravet i GDPR artikkel 36 om forhåndsdrøftinger med tilsynsmyndigheten når dette er aktuelt. Partene skal ved behov bistå hverandre med gjennomføringen av en vurdering av personvernkonsekvenser og forhåndsdrøftelse med tilsynsmyndigheten. Begge parter plikter å underrette hverandre om innholdet i og konklusjonen av en eventuell forhåndsdrøfting.

## Informasjon og revisjon

Partene skal på forespørsel gi den andre parten tilgang til all informasjon og dokumentasjon som er nødvendig for å påvise at forpliktelsene fastsatt i denne Avtalen er oppfylt. Dette 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), databehandleravtaler, grunnlag for overføring til tredjeland og annen dokumentasjon som er nødvendig for at partene skal kunne ivareta sine forpliktelser i henhold til denne Avtalen, GDPR og annen gjeldende personvernlovgivning.

## Databehandlere og leverandører

Partene kan ikke benytte seg av databehandlere eller leverandører i tilknytning til den felles behandlingen av personopplysninger med mindre dette er skriftlig godkjent av den andre parten. Partene godkjenner bruk av databehandlerne som er angitt i Vedlegg 1. Partene kan ikke engasjere andre databehandlere enn de som er nevnt i Vedlegg 1 uten at dette på forhånd er skriftlig godkjent av den andre parten.

Hver av partene er selvstendig ansvarlig for databehandlere som de selv engasjerer og inngår avtale med, selv om databehandleren brukes i forbindelse med behandling som partene er felles behandlingsansvarlig for etter denne Avtalen. Hvilken part som er ansvarlig for de godkjente databehandlerne fremgår av Vedlegg 1.

Det betyr at hver av partene er ansvarlig for å etterleve kravene i GDPR artikkel 28 i forbindelse med sin bruk av databehandlere. Partene skal bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i GDPR og annen gjeldende personvernlovgivning. Partene skal også å sikre at det foreligger en gyldig databehandleravtale med databehandleren og at denne databehandleravtalen viderefører alle forpliktelser som er nødvendig for at partene skal kunne oppfylle sine forpliktelser overfor hverandre etter denne Avtalen. Partene skal sikre at sine databehandlere overholder forpliktelsene som databehandleren er underlagt i henhold til databehandleravtalen og i henhold til GDPR og annen gjeldende personvernlovgivning.

Det betyr også at i den grad en parts databehandler påfører den andre parten et økonomisk tap, herunder administrative overtredelsesgebyr eller erstatningsansvar, og dette skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos databehandleren, så er denne parten erstatningsansvarlig overfor den andre parten.

## Overføring til land utenfor EU/EØS

Partene kan ikke overføre eller tillate overføring av personopplysninger til stater utenfor EU/EØS eller til internasjonale organisasjoner eller bruke databehandlere i slike tredjeland uten skriftlig forhåndsgodkjenning fra den andre parten. Dette omfatter også fjerntilgang fra utlandet. Ved enhver overføring av personopplysninger til tredjeland eller bruk av databehandlere i tredjeland skal begge parter 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 partene behandler i henhold til denne Avtalen vil bli overført til og det rettslige grunnlaget for overføringene følger av Vedlegg 1.

## Klager

Partene er selvstendig ansvarlige for behandlingen av eventuelle klager fra registrerte om brudd på bestemmelser i GDPR og annen gjeldende personvernlovgivning, i forbindelse med den behandling av personopplysninger som den aktuelle parten er ansvarlig for i henhold til denne avtale.

Den parten som mottar en klage skal underrette den andre parten snarest mulig, dersom klagen gjelder den felles behandlingen av personopplysninger under denne Avtalen. Det skal også opplyses om parten som mottok klagen skal behandle klagen selv og i hvilken utstrekning. Hvis én av partene mottar en klage som helt eller delvis bør behandles av den andre parten, oversendes klagen til denne behandlingsansvarlige snarest mulig. Den registrerte skal, i forbindelse med partens oversendelse av en klage eller en del av en klage til den andre parten, opplyses om det vesentlige innholdet i denne avtalen.

## Mislighold og ansvar

Dersom partene ikke overholder sine plikter etter denne Avtalen eller etter GDPR og annen gjeldende personvernlovgivning, anses det som mislighold av denne Avtalen og Hovedavtalen. Ved slikt mislighold kan hver av partene si opp Hovedavtalen med øyeblikkelig virkning.

Partene kan kreve erstatning for økonomiske tap, herunder administrative overtredelsesgebyr og erstatningskrav, som skyldes den andre partens brudd på sine plikter etter denne Avtalen eller etter GDPR og annen gjeldende personvernlovgivning. I den grad det økonomiske tapet skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos en av partenes databehandlere, er parten som er ansvarlig for den aktuelle databehandleren på samme måte erstatningsansvarlig overfor den andre parten.

## Avtalens varighet

Denne Avtalen gjelder så lenge Hovedavtalen løper, eller så lenge partene behandler personopplysninger som felles behandlingsansvarlige.

## Kontaktpersoner

Kontaktpersoner hos partene for spørsmål knyttet til denne Avtalen er oppført i Vedlegg 1.

## Lovvalg, tvister og verneting

Partenes rettigheter og plikter etter denne Avtalen bestemmes i sin helhet av norsk rett. Eventuelle tvister som springer ut av denne Avtalen skal først søkes løst gjennom forhandlinger. Dersom partene ikke oppnår enighet gjennom forhandlinger, skal tvisten løses med bindende virkning av Oslo tingrett. Dersom begge partene er statlige universiteter eller høyskoler, 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 1 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_På vegne av Behandlingsansvarlig 2 |
| Navn: | Navn: |
| Stilling: | Stilling: |

## Vedlegg 1

## Formål med behandlingen

[Beskrivelse av formålet med behandlingen. Dette vil som hovedregel være å utføre samarbeidet i henhold til Hovedavtalen. Gi en oppsummering av samarbeidet som skal utføres under Hovedavtalen.]

## 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.]

## Behandlingsaktiviteter og partenes roller

Behandlingsansvarlig 1 vil ha følgende rolle og utføre de følgende behandlingsaktivitetene under Avtalen: [Beskriv OsloMets rolle i forbindelse med behandlingsaktivitetene, for eksempel at OsloMet skal stå for innsamlingen av dataene til prosjektet.]

Behandlingsansvarlig 2 vil ha følgende rolle og utføre de følgende behandlingsaktivitetene under Avtalen: [Beskriv den andre behandlingsansvarliges rolle i forbindelse med de felles behandlingsaktivitetene, for eksempel at de skal stå for analysene av de innsamlede dataene.]

## Underleverandører i EU/EØS

|  |  |  |
| --- | --- | --- |
| **Navn** | **Type behandling** | **Ansvarlig part** |
| [Analyse1] | [Analyse av data] | [Behandlingsansvarlig 2] |
|  |  |  |
|  |  |  |

## Underleverandører utenfor EU/EØS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Navn** | **Type** | **Land** | **Overføringsgrunnlag** | **Ansvarlig part** |
| [Microsoft Azure] | [Skyleverandør] | [USA] | [Data Privacy Framework] | [Behandlingsansvarlig 1] |
|  |  |  |  |  |
|  |  |  |  |  |

## Kontaktpunkt for de registrerte

Partene har utpekt følgende kontaktpunkt for de registrerte: [Navn/e-post/telefon]

## Kontaktpersoner

Kontaktperson for Behandlingsansvarlig 1: [Navn, e-post, telefon]

Kontaktperson for Behandlingsansvarlig 2: [Navn, e-post, telefon]