****

**Mal for avtale om felles behandlingsansvar**

I henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016, artikkel 26, inngås følgende avtale

mellom

MF vitenskapelig høyskole

Org. nr.: 917 387 079

 Postboks 5144, Majorstuen

0363 Oslo

Norge

og

Navn på institusjon

……………………………………………

Org. nr.:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Postadresse:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Postnummer:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Land:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Måned/Årstall

*Gult=veiledning/kommentarer som skal slettes. Grønt= markerer der det skal settes inn noe. Rødt=markerer den som er prosjektleder/hovedansvarlig. Der skal det også, i de tilfeller ekstern er prosjektleder/hovedansvarlig, fylles inn noe. Farge, samt alternativ som ikke benyttes, slettes.*

1. **Felles behandlingsansvar**
	1. Denne (Avtalen) fastsetter ansvarsfordelingen mellom MF vitenskapelig høyskole (MF) og [*navn på ekstern part*] i forbindelse med prosjektet som er gjengitt på avtalens førsteside [*navn på behandling/prosjekt*] (Hovedavtalen).

Felles databehandleransvar gjelder:

* Veiledning: Gi en kort [gjerne punktvis] oversikt over hvilke typer av personopplysninger som skal behandles (eksempel dokumenter, datafiler, intervjudata, avidentifiserte data, sensitive data o.l).
* Veiledning: Gi en kort oversikt over hvem opplysningene gjelder, for eksempel studenter og ansatte ved institusjonen eller pasienter ved en helseinstitusjon, hva som er behandlingsgrunnlaget og hvilke godkjennelser som er gitt.
	1. I flg. personvernforordningen artikkel 26 foreligger det et felles behandlingsansvar dersom to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med og midlene for behandlingen.

MF og [*navn på ekstern part*] er enig om at det i forbindelse med [*navn på behandling/prosjekt*] foreligger et felles behandlingsansvar. I vurderingen av hvorfor ansvaret skal være delt, er det blant annet lagt vekt på at begge institusjoner bidrar med [*type kompetanse o.l.*] og i fellesskap bestemmer behandlingens/prosjektets formål og midler.

De felles behandlingsansvarlige skal på en åpen måte fastsette sitt respektive ansvar for å overholde forpliktelsene i personvernforordningen, særlig med hensyn til utøvelse av den registrertes rettigheter og den plikt de har til å framlegge informasjonen nevnt i artikkel 13 og 14, ved hjelp av en ordning seg imellom, med mindre og i den grad de behandlingsansvarliges respektive ansvar er fastsatt i unionsretten eller medlemsstatenes nasjonale rett eller norsk rett som de behandlingsansvarlige er underlagt.

Ordningen, ved denne avtalen, skal etter personvernforordningen artikkel 26 nr. 2 på behørig måte gjenspeile de felles behandlingsansvarliges respektive roller og forhold til de registrerte. Det vesentlige innholdet i ordningen, ved denne avtalen, skal gjøres tilgjengelig for den registrerte.

Uavhengig av vilkårene for ordningen, ved denne avtalen, kan den registrerte utøve sine rettigheter i henhold til personvernforordningen med hensyn til og overfor hver av de behandlingsansvarlige.

Ansvarsfordelingen i denne avtalen om felles behandlingsansvar hindrer ikke tilsynsmyndigheten i å forfølge både MF og [*navn på ekstern part*].

1. **Ansvarsfordeling**
	1. MFs ansvar:

Veiledning: Gi en beskrivelse av MFs ansvar når det gjelder oppbevaring og eventuell innsamling og koding av data (f.eks. oppbevaring av kodenøkkel, datafiler, analyser og dokumenter), hvordan data lagres og eventuelle sikringstiltak, samt tilgang til data.

[*Navn på ekstern parts*] ansvar:

Gi en beskrivelse av den eksternes ansvar når det gjelder oppbevaring og eventuell innsamling og koding av data (f.eks. oppbevaring av kodenøkkel, datafiler, analyser og dokumenter), hvordan data lagres og eventuelle sikringstiltak, samt tilgang til data.

1. **Prinsipper og behandlingsgrunnlag**
	1. Både MF og [*navn på ekstern part*] er ansvarlige for at det foreligger et gyldig behandlingsgrunnlag og for at dette kan dokumenteres.

Velg et av alternativene eller eventuelt begge:

Alternativ 1: Forskningsprosjektet skal være vurdert av Sikt (tidl. NSD) og evt. REK.

Alternativ 2: Behandlingen skal vurderes ved egen institusjon og inngå i institusjonens oversikt over behandling av personopplysninger.

* 1. MF og [*navn på ekstern part*] er begge ansvarlige for å overholde prinsippene for behandling av personopplysninger i artikkel 5, i den grad bestemmelsene får anvendelse på de beskrevne ansvarsområder i henhold til denne avtalen.
1. **De registrertes rettigheter**
	1. Begge parter er ansvarlig for sikringen av de registrertes rettigheter i personvernforordningen gjennom overholdelse av følgende:
* opplysningsplikt ved innsamling av personopplysninger fra den registrerte,
* opplysningsplikt, hvis personopplysninger er innsamlet fra andre enn den registrerte,
* den registrertes innsynsrett,
* rett til retting,
* rett til sletting,
* rett til begrensning av behandling,
* underretningsplikt i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling,
* rett til dataportabilitet og
* rett til å protestere mot en behandling

krav om ny innhentning av godkjennelse hos (pasient, ansatt, student, forskningsdeltaker o.l.) ved ny, endret eller utvidet bruk av data, prøver m.m.

rett til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering, som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker den registrerte, med mindre dette er tillatt etter art. 22

* 1. Prosjektleder ved MF eller prosjektleder ved [*navn på ekstern part*] er kontaktperson for deltakerne i studien/behandlingen og har hovedansvaret for at prosjektdeltakernes/de registrertes rettigheter overholdes. [*Navn på ekstern part*] eller MFhar allikevel et selvstendig ansvar for å sørge for at deltakernes/de registrertes rettigheter ivaretas. Herunder plikter begge parter å påse at data håndteres som beskrevet i 1.1, samt at alle opplysninger slettes hos begge behandlingsansvarlige dersom en deltaker/registrert ønsker å trekke seg fra studien/behandlingen.
	2. Dersom MF mottar en anmodning eller henvendelse fra en registrert vedrørende de forhold som er omfattet av [*navn på ekstern part*] sitt ansvar (der personopplysningene behandles), jf. over, oversendes denne til besvarelse hos [*navn på ekstern part*] snarest mulig.
	3. Dersom [*navn på ekstern*] mottar en anmodning eller henvendelse fra en registrert vedrørende de forhold, som er omfattet av MFs ansvar (der personopplysningene behandles), jf. over, oversendes denne til besvarelse hos MF snarest mulig.
	4. 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. Hver behandlingsansvarlig er individuelt erstatningsansvarlig overfor de registrerte, dersom feil eller forsømmelser hos den enkelte behandlingsansvarlige påfører de registrerte økonomiske eller ikke-økonomiske tap som følge av at deres rettigheter eller personvern er krenket.
1. **Sikkerhet ved behandlingen og dokumentasjon på overholdelse av personvernforordningen**
	1. Begge parter er ansvarlige for å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen er i samsvar med personvernforordningen. Tiltakene skal ta hensyn til den aktuelle behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter. Tiltakene gjennomgås på nytt og skal oppdateres ved behov, jf. personvernforordningen artikkel 24. Dette kan eksempelvis omfatte at begge parter iverksetter egnede retningslinjer for håndtering av sikkerhetsbrudd, innsynsbegjæringer eller oppfyllelse av opplysningsplikten i henhold til gjeldende lov.
	2. Begge parters tiltak skal, hvis det står i et rimelig forhold til behandlingsaktivitetene, omfatte gjennomføring av egnede beskyttelsestiltak.
	3. Begge parter er ansvarlig for overholdelse av bestemmelsen om innebygd personvern og personvern som standardinnstilling i artikkel 25.
	4. Begge parter er ansvarlig for å overholde kravet i personvernforordningen artikkel 32 om sikkerhet ved behandlingen. Dette innebærer at begge parter, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, gjennomfører egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoene.

Begge parter skal derfor gjennomføre og dokumentere en risikovurdering, samt gjennomføre og dokumentere tiltak for å begrense identifiserte risikoer.

1. **Personvernkonsekvensvurdering**
	1. Begge parter er ansvarlig for overholdelse av kravet i personvernforordningen artikkel 35 om personvernkonsekvensvurdering (DPIA – data protection impact assessment). Dette innebærer at begge parter, hvis en type behandling, idet det tas hensyn til den aktuelle behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal før behandlingen sørge for en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet.
	2. Begge parter er tilsvarende forpliktet til å overholde kravet i personvernforordningen artikkel 36 om forhåndsdrøftinger med tilsynsmyndigheten når dette er aktuelt.
	3. Dersom det er et behov, i forbindelse med felles behandling, skal begge parter bistå hverandre med gjennomføringen av en DPIA og forhåndsdrøftelse med tilsynsmyndigheten. Begge parter plikter å underrette hverandre om innholdet i og konklusjonen av en eventuell forhåndsdrøfting.
2. **Bruk av databehandlere og underdatabehandlere**
	1. [*Navn på ekstern part*] eller MF er ikke berettiget til å benytte seg av databehandlere og/eller eventuelle underdatabehandlere i tilknytning til den felles behandling, med mindre dette er avtalt direkte med MFs prosjektleder eller [*navn på ekstern part*] sin prosjektleder.
	2. Ved eventuell bruk av databehandlere og/eller underdatabehandlere er begge parter ansvarlig for å etterleve kravene i personvernforordningen artikkel 28. Begge parter er bl.a. forpliktet til:
* å bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personvernforordningen og vern av den registrertes rettigheter.
* å sikre at det foreligger en gyldig databehandleravtale med databehandleren og/eller underdatabehandleren.

Eksempel:

* TSD på UiO anses for å oppfylle alle disse kriteriene
	1. Begge parter skal på anmodning underrettes om personopplysningene behandles av databehandlere og ev. underdatabehandlere hos den ene parten*.*
	2. Hvis personopplysningene behandles av databehandlere og ev. underdatabehandlere, skal begge parter på anmodning underrettes om innholdet i avtalene mellom den ene parten og databehandleren/underdatabehandleren.
1. **Protokoll - oversikt over behandlingsaktiviteter**
	1. Begge parter er ansvarlig for å overholde kravet i personvernforordningen artikkel 30 om protokoll over behandlingsaktiviteter. Dette innebærer at begge parter fører en protokoll over den behandlingen som partene er felles behandlingsansvarlig for.
	2. Begge parter orienterer hverandre om innholdet i sine ovenfor nevnte protokoller.
	3. Begge parter utarbeider – på bakgrunn av innholdet i hverandres protokoll - egen protokoll over den behandlingsaktivitet som er regulert i avtalen.
2. **Melding til tilsynsmyndigheten om brudd på personopplysningssikkerhet**
	1. MF eller [*navn på ekstern part*] er ansvarlig for overholdelse av personvernforordningen artikkel 33 om melding av brudd på personopplysningssikkerhet til tilsynsmyndigheten.
	2. [*Navn på ekstern part*] eller MF skal uten ugrunnet opphold varsle MF eller [*navn på ekstern part*] dersom personopplysninger utsettes for sikkerhetsbrudd. Varselet til MF eller [*navn på ekstern part*] 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.

MF eller [*navn på ekstern part*] er ansvarlig for at Datatilsynet blir varslet når dette er påkrevd.

1. **Underretning av den registrerte om brudd på personopplysningssikkerhet**
	1. Begge parter er ansvarlig for overholdelse av personvernforordningen artikkel 34 om underretning av den registrerte om brudd på personopplysningssikkerheten.
	2. [*Navn på ekstern part*] eller MF skal uten ugrunnet opphold varsle MF eller [*navn på ekstern part*] som beskrevet i 9.2. MF eller [*navn på ekstern part*] er ansvarlig for at den registrerte blir varslet når dette er påkrevd.
2. **Overførsel av personopplysninger til tredjeland eller internasjonale organisasjoner**
* Kommentar: Personopplysninger som en eller begge parter forvalter, kan bli overført til land utenfor EU/EØS (tredjeland). Slik overføring kan skje på visse vilkår og reglene om overføring til tredjeland finnes i Artikkel 45-47 og 49 i EUs personvernforordning. Disse reglene innebærer blant annet at overføringen vil være lovlig dersom den skjer til et EU-godkjent tredjeland eller på grunnlag av EUs standardkontrakter for overføring av personopplysninger til databehandlere i tredjeland. Merk at det må foretas en vurdering av tredjelandets beskyttelsesnivå og eventuelt iverksettes ytterligere tiltak for at lovlig overføring på grunnlag av EUs standardkontrakter skal kunne skje. Reglene gjelder for blant annet lagring av personopplysninger i tredjestater og tilgang til personopplysninger fra tredjestater, også for sikkerhetskopiering og annen overføring av personopplysninger som skjer i forbindelse med administrasjon av den aktuelle tjenesten, for eksempel support.

Velg ett av alternativene:

* 1. Alternativ 1: Personopplysninger skal ikke overføres til tredjeland eller internasjonale organisasjoner.

Alternativ 2: Personopplysninger som databehandler forvalter i henhold til denne avtalen, vil bli overført til følgende mottakerland utenfor EU/EØS:

……………………………………………………………………………………………………………………………………………

[*navn på mottakerland*].

Det rettslige grunnlaget for overføring av personopplysninger til de nevnte mottakerland utenfor EU/EØS er:

……………………………………………………………………………………………………………………………………………

[kort redegjørelse for overføringsgrunnlaget].

1. **Klager**
	1. Partene er selvstendig ansvarlige for behandlingen av eventuelle klager fra registrerte, om brudd på bestemmelser i personvernforordningen, i forbindelse med den behandling av personopplysninger som den aktuelle parten er ansvarlig for i henhold til denne avtalen.
	2. Den parten som mottar en klage, skal underrette den andre parten snarest mulig dersom klagen gjelder prosjektet/felles behandling som sådan. Det skal også opplyses om parten som mottok klagen, skal behandle klagen selv og i hvilken utstrekning.

* 1. Hvis én av partene mottar en klage som bør behandles av den andre parten, oversendes klagen til denne behandlingsansvarlige snarest mulig.
	2. Hvis én av partene mottar en klage, hvor en del av klagen bør behandles av den andre parten, oversendes denne delen til besvarelse av den andre parten snarest mulig.
	3. 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.
1. **Taushetsplikt**
2. 1 Kun ansatte hos en av partene som har tjenstlige behov for tilgang personopplysninger

som forvaltes på vegne av behandlingsansvarlig, kan gis slik tilgang. Parten plikter å dokumentere retningslinjer og rutiner for tilgangsstyring. Dokumentasjonen skal være tilgjengelig for den andre parten.

1. 2 Ansatte hos partene har 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 levere eller administrere/annen type behandling (*navn på tjeneste/prosjekt*).
2. **Mislighold**

Ved vesentlig mislighold av vilkårene i denne Avtalen som skyldes feil eller forsømmelser fra en parts side, kan de andre partene si opp Avtalen og Hovedavtalen med øyeblikkelig virkning.

1. **Erstatning**

Personvernforordningen art. 82 gjelder for rett til erstatning og erstatningsansvar ved skade overfor fysiske personer som følge av brudd på personvernforordningen.

Partene er hver for seg ansvarlige for overtredelsesgebyr ilagt i henhold til personvernforordningen art. 83.

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.

1. **Orientering av den andre parten**

Partene orienterer hverandre om vesentlige forhold av betydning for den felles behandling og av betydning for denne avtalen.

1. **Ikrafttredelse og opphør**
	1. Denne avtalen er godkjent av leder i linjen [*tittel*] ved MF eller [*tittel + navn på ekstern part*] og [*tittel + navn på ekstern part*]eller leder i linjen [*tittel*]ved MF. Godkjennelsen skal foreligge før arbeidet kan startes. Alle føringer fra Sikt (tidl. NSD), REK, andre godkjennelsesinstanser og leder i linjen [*tittel*] ved MF eller [*tittel + navn på ekstern part*] må følges av begge parter. Forhold som kan innebærer brudd på dette, skal uten opphold meddeles prosjektansvarlig og behandles i henhold til MFs eller [*navn på ekstern part*] sine til enhver tid gjeldende avviksrutiner.
	2. Denne avtale trer i kraft ved begge parters underskrift.
	3. Avtalen er gjeldende så lenge de omhandlede opplysninger behandles, eller inntil avtalen erstattes av en ny avtale som fastsetter ansvarsfordelingen i forbindelse med behandlingen av personopplysninger.
2. **Kontaktpersoner**

Kontaktpersoner hos MF for spørsmål knyttet til denne avtalen er \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Kontaktperson hos [*navn på ekstern part*] for spørsmål knyttet til denne avtalen er \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Lovvalg, verneting og tvisteløsning**

Kommentar: Stryk det alternativet nedenfor – A eller B – som ikke passer.

1. **Lovvalg og verneting.**

Avtalen er underlagt norsk rett og partene vedtar [*fyll inn navn på tingrett*] som verneting. Dette gjelder også etter opphør av avtalen.

* Kommentar: Dette punktet gjelder når ekstern part er en privat eller utenlandsk aktør.
1. **Lovvalg og tvisteløsning**

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 Kunnskapsdepartementet. Hver av partene kan forlange at tvisten oversendes departementet.

* Kommentar: Dette punktet gjelder når ekstern part er et statlig universitet eller en annen høyskole i Norge.

\*\*\*

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

Sted og dato

På vegne av MF vitenskapelig høyskole På vegne av [*navn på ekstern part*]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Navn: Navn:

Stilling: Stilling: