**AVTALE OM FELLES BEHANDLINGSANSVAR**

I henhold til gjeldende norsk personverngivning og EU-forordning 2016/679 av 27. april 2016 («GDPR»)

**[*Navn på «Hovedavtale» knyttet til det konkrete samarbeid/prosjekt*]**

mellom

**[*Navn på institusjon/selskap*]**

[*org.nr.*]

 **(«Navn 1»)**

og

**[*Navn på institusjon/selskap*]**

[*org.nr.*]

 **(«Navn 2»)**

[*Flere institusjoner/selskaper kan tilføyes avhengig av underliggende forhold/prosjekt*]

*Tekst markert i gult eller tekst i kursiv skal fjernes og/eller erstattes med relevant tekst, ev. velges ett av flere alternativer.*

## Avtalens hensikt

Denne avtalen om felles behandlingsansvar («Avtalen») angir partenes respektive ansvar for overholdelse av gjeldende personvernlovgivning når den behandling av personopplysninger som finner sted mellom partene i tilknytning til det konkrete samarbeid/prosjekt som angitt på Avtalens førsteside tilsier at det foreligger et felles behandlingsansvar mellom partene.

Partene er felles behandlingsansvarlige for personopplysningene som behandles under denne Avtalen, ettersom partene i fellesskap bestemmer formålet med behandlingen av personopplysningene og hvilke midler som skal benyttes, jf. GDPR artikkel 26.

Avtalen etablerer den avtaleordning som er påkrevd etter GDPR artikkel 26 og fastsetter hver av partenes respektive ansvar for å overholde forpliktelsene i GDPR, særlig med hensyn til utøvelse av de registrertes rettigheter og den plikt partene har til å overholde informasjonskravene i GDPR artikkel 13 og 14 overfor de registrerte.

Ved motstrid skal vilkårene i denne Avtalen gå foran partenes respektive personvernerklæringer eller vilkår i andre avtaler inngått mellom partene i tilknytning til den databehandlingen Avtalen gjelder.

Formålet med databehandlingen, hvilke typer personopplysninger som vil bli behandlet, relevante kategorier av registrerte, samt en overordnet beskrivelse av hver av partenes respektive roller i tilknytning til databehandlingen og de pliktene som gjelder for behandlingsansvarlige etter kapittel 4 i GDPR, er angitt i Avtalens bilag 1. Disse forholdene kan ikke endres av noen av partene uten at ny avtale eller et endringsvedlegg til Avtalen er signert.

## Formålsbegrensning

Partene skal ikke behandle personopplysningene for andre formål enn hva som er angitt i Avtalen, med mindre annet følger av lovpålagte forpliktelser.

## Overholdelse av gjeldende personvernlovgivning

Ved å signere denne Avtalen forplikter hver av partene seg til følgende:

* Partene skal overholde alle krav i gjeldende personvernlovgivning med hensyn til behandling av personopplysninger i relasjon til denne Avtalen, herunder plikten til å gjennomføre risikovurderinger, og å inngå databehandleravtaler med sine leverandører som behandler personopplysninger som omfattes av denne avtalen.
* Partene bekrefter at de i henhold til GDPR artikkel 32 har iverksatt tilfredsstillende tekniske, fysiske og organisatoriske sikringstiltak for å beskytte personopplysninger som omfattes av denne Avtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.
* Hvis en part oppdager feil eller anløp til feil i sammenheng med overføringen av personopplysninger under denne Avtalen, skal den parten som oppdager feilen informere den andre parten omgående.
* Hver part har tilstrekkelig behandlingsgrunnlag for sin respektive behandling av personopplysninger som angitt i denne Avtalen, i henhold til GDPR artikkel 6.
* I samråd med den andre parten overholde plikten i GDPR Artiklene 33 og 34 til å melde avvik til henholdsvis Datatilsynet og til de registrerte, når vilkårene for slik melding foreligger i det enkelte tilfellet.

## De registrertes rettigheter

Hver part skal respektere de registrertes rettigheter, slik disse er regulert i GDPR kapittel 3.

Hver part skal sørge for at tydelig og tilstrekkelig informasjon om behandlingen av personopplysninger er gjort tilgjengelig for de registrerte individene, i henhold til GDPR artikkel 12-14.

I forbindelse med overholdelsen av denne informasjonsplikten skal hver av partene gjøre det vesentligste innholdet i avtaleordningen mellom de felles behandlingsansvarlige slik det fremgår av denne Avtalen, tilgjengelig for de registrerte i henhold til GDPR artikkel 26. Dette innebærer at det som minimum gis følgende informasjon:

* informasjon om at det foreligger et felles behandlingsansvar
* hvem de felles behandlingsansvarlige er
* informasjon om de respektive behandlingsansvarliges vesentligste roller ved behandlingen av personopplysningene om de registrerte
* at hver av de behandlingsansvarlige er forpliktet til å oppfylle de registrertes rettigheter i henhold til GDPR kapittel 3
* kontaktpunktet for de registrerte, jf. pkt. 10

## Taushetsplikt

Avtalens innhold og de opplysninger som behandles er underlagt taushetsplikt mellom partene. Hver av partene kan imidlertid dele informasjon om Avtalen og opplysningene med rådgivere og underleverandører i den utstrekning det anses nødvendig for oppfyllelsen av deres oppgaver for respektive part, forutsatt at mottakende part pålegges en tilsvarende forpliktelse om konfidensialitet som angitt i denne bestemmelsen. Hver part kan også dele slike opplysninger som fremgår av pkt. 4 med de registrerte.

Norsk lov vil kunne begrense omfanget av taushetsplikten for hver av partene.

## Informasjons- og møteplikt

Hver av partene plikter å holde den annen part løpende orientert om relevant informasjon i tilknytning til partenes respektive behandlingsansvar under Avtalen. Dette gjelder i særlig grad ved mottak av henvendelser fra registrerte individer vedrørende utøvelse av de registrertes rettigheter til retting og sletting mv. etter GDPR kapittel 3, eller ved en parts iverksettelse av egne tiltak for å overholde disse rettighetene i den grad det må antas at dette kan ha betydning for den annen part. Det gjelder videre ved eventuelle henvendelser fra Datatilsynet med forespørsel om informasjon, varsel om inspeksjon e.l.

Hver av partene har rett til å innkalle den annen part til et møte for å diskutere forhold ved utøvelsen av det felles behandlingsansvaret med minimum 10 arbeidsdagers skriftlig varsel. Med varselet skal det følge et forslag til møteagenda. Møter kan ikke kreves hyppigere enn én gang i kvartalet, med mindre det foreligger særlige grunner som begrunner hyppigere møter.

## Varslingsplikt ved sikkerhetsbrudd

Hver av partene skal uten ugrunnet opphold varsle den annen part dersom personopplysninger som behandles av den respektive part utsettes for sikkerhetsbrudd som innebærer risiko for krenkelser av de registrertes personvern (GDPR Artikkel 33 og 34).

Varslet til den annen 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.

Den part som er ansvarlig for det systemet eller den prosessen som lå til grunn for det aktuelle sikkerhetsbruddet er ansvarlig for at varsel om sikkerhetsbruddet blir meldt som avvik til Datatilsynet der dette er påkrevd etter GDPR artikkel 33, eller til de registrerte etter artikkel 34. I den grad tiden tillater det ut ifra lovmessige tidsfrister, skal den annen part konfereres før varsel sendes. Kopi av varselet skal sendes den annen part.

## Bruk av databehandlere

Hver av partene plikter å inngå egne databehandleravtaler med eventuelle leverandører som regulerer deres behandling av personopplysninger i egenskap av databehandler på vegne av respektive part. Databehandleravtaler skal tilfredsstille alle krav etter GDPR artikkel 28 og for øvrig videreføre alle plikter som er nødvendige for at den respektive behandlingsansvarlige kan overholde sine forpliktelser overfor den annen part.

Hver av partene skal kontrollere at egne databehandlere overholder sine avtalemessige plikter, spesielt at informasjonssikkerheten er tilfredsstillende og at ansatte hos databehandlere er kjent med sine forpliktelser og oppfyller disse.

Partene er på avtaletidspunktet enige om bruk av databehandlere som angitt i Avtalens bilag 1. Endringer i bruk av databehandlere skal forhåndsgodkjennes av den annen part før nye avtaler inngås. Kopi av inngåtte databehandleravtaler skal fremlegges for den annen part på forespørsel.

## Overføring til land utenfor EU/EØS

*Kommentar: Dersom Avtalen innebærer at personopplysninger som behandles kan bli overført til land utenfor EU/EØS (tredjeland), kan slik overføring kun skje på visse vilkår. Reglene om overføring til tredjeland finnes i GDPR artikkel 45-47 og 49. 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 tredjeland.*

*[Stryk det alternativet nedenfor – alternativ 1 eller 2 – som ikke passer]*

*[Alternativ 1: Hvis det ikke skal overføres personopplysninger til land utenfor EU/EØS]*

Personopplysninger skal ikke overføres til land utenfor EU/EØS.

Om det blir behov for å overføre personopplysninger utenfor EU/EØS for å oppfylle denne avtalen, må dette skriftlig godkjennes av behandlingsansvarlig på forhånd

*[Alternativ 2: Hvis personopplysninger skal overføres til land utenfor EU/EØS]*

Personopplysninger som behandles i henhold til denne Avtalen, vil bli overført til, eller aksessert fra, 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).

*Kommentar: Her må man opplyse om hvilket overføringsgrunnlag som benyttes, jf. GDPR artikkel 45-47 og 49.*

## Sikkerhetsrevisjoner

Partene skal jevnlig gjennomføre sikkerhetsrevisjoner av eget arbeid med sikring av personopplysninger mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Partene skal gjennomføre sikkerhetsrevisjoner av informasjonssikkerheten i virksomheten. Sikkerhetsrevisjoner skal omfatte partens sikkerhetsmål og sikkerhetsstrategi, sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, etablerte tekniske, fysiske og organisatoriske sikringstiltak og arbeidet med informasjonssikkerhet hos underleverandører. Det skal i tillegg omfatte rutiner for varsling av felles behandlingsansvarlige ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner.

Partene skal dokumentere sikkerhetsrevisjonene. Hver av de behandlingsansvarlige skal på forespørsel gis tilgang til den andre behandlingsansvarliges revisjonsrapporter.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos en part, skal den andre parten informeres om hvilken revisor som benyttes og på forespørsel få tilgang til oppsummeringer av revisjonsrapportene.

*Kommentar: Dette punktet skal ivareta mulighet for å kontrollere egen oppfyllelse av personvernregelverket og ha mulighet for å kontrolle at den andre parten sikrer slik oppfyllelse. De respektive behandlingsansvarlige (Partene) forplikter seg til å gjennomføre sikkerhetsrevisjoner for å sikre overholdelse av GDPR. Dette kan f.eks. være en kontroll av om det foreligger egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personvernforordningen og verner de registrertes rettigheter.*

*Det kan avtales at partene gjennomfører en slik sikkerhetsrevisjon selv, eller det kan avtales at en uavhengig tredjepart gjennomfører det.*

*Hvor omfattende en slik revisjon skal være avhenger av behandlingens art og omfang, men poenget er at partene skal kontrollere egen oppfyllelse, samt ha mulighet til å kontrollere at den andre parten oppfyller sine plikter.*

## Mislighold

Ved vesentlig mislighold av vilkårene i denne Avtalen som skyldes feil eller forsømmelser fra en parts side, kan den annen part si opp Avtalen med øyeblikkelig virkning.

## Erstatning

Hver av partene kan kreve erstatning for ethvert direkte økonomisk tap som kan tilbakeføres til brudd på den annen parts forpliktelser etter Avtalen. Erstatning kan ikke kreves for indirekte tap. Indirekte tap omfatter, men er ikke begrenset til, tapt fortjeneste, tapte besparelser, tap som følge av tap av data og krav fra tredjepart.

Samlet erstatning per kalenderår er begrenset til

*Kommentar: Velg passende alternativ avhengig av prosjekt/avtale. Det må vurderes hvilken risiko partene er villige til å ta, og eventuelt «økonomien» i avtalen. Partene må vurdere risikoen opp mot innholdet i prosjektet og risikoen for brudd på de registrertes rettigheter. Beløpene i alternativene er forslag, men partene står fritt til å velge et annet beløp:*

*[Stryk det alternativet nedenfor – alternativ 1 eller 2 – som ikke passer]*

*[Alternativ 1]:* et beløp som tilsvarer samlet årlig vederlag ekskl. merverdiavgift under Hovedavtalen.

*[Alternativ 2]:* et beløp fastsatt til én million norske kroner (1 MNOK).

De ovennevnte erstatningsbegrensningene gjelder ikke ved grov uaktsomhet eller forsett.

## Avtalens varighet

Denne Avtalen gjelder så lenge Hovedavtalen er i kraft og deretter så lenge minst én av partene fortsatt behandler personopplysninger med utspring i Hovedavtalen.

Når all behandling av partenes respektive behandling av personopplysninger under Avtalen er opphørt, plikter hver av partene å dokumentere overfor den annen part at de aktuelle personopplysningene er slettet i samsvar med GDPR artikkel 17.

## Kontaktpersoner

Kontaktperson hos [*Navn 1*] for spørsmål knyttet til denne Avtalen er:

[*Enhet, stilling, kontaktinformasjon, adresse, telefon og e-post*]

Kontaktperson hos [*Navn 2*] for spørsmål knyttet til denne Avtalen er:

[*Enhet, stilling, kontaktinformasjon, adresse, telefon og e-post*]

*[Følgende avsnitt inntas hvis partene finner det hensiktsmessig . Merk at hver av partene uansett er ansvarlige for å overholde de registrertes rettigheter ved henvendelser fra de registrerte, jf. pkt. 4.]*

Kontaktpunkt for de registrerte for behandling av personopplysninger knyttet til denne Avtalen skal være: [*Enhet, stilling, kontaktinformasjon, adresse, telefon og e-post*] *[Fyll ut eller slett.]*

## Lovvalg og verneting

*Kommentar: Velg passende alternativ avhengig av avtalemotpart. Slett det andre alternativet:*

*Alternativ 1 - gjelder når NTNUs avtalemotpart er en privat aktør/ikke-statlig universitet eller høyskole. Trøndelag tingrett er skrevet inn som standard. Denne kan endres om ønskelig:*

Avtalen er underlagt norsk rett. Partene vedtar Trøndelag tingrett som verneting.

*Alternativ 2 – gjelder når NTNUs avtalemotpart er et annet statlig universitet eller høyskole.*

Avtalen er underlagt 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.

\*\*\*

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

Sted og dato

 På vegne av [Navn 1] På vegne av [Navn 2]

……………………….. ………………………

(underskrift) (underskrift)

**BILAG 1 – SPESIFIKASJON AV DATABEHANDLINGEN**

## 1. Formål

Formålet med partenes behandling av personopplysninger under Avtalen er:

*Kommentar: Angi klart og tydelig hva som er partenes formål med databehandlingen. Dersom formålet fremgår av annen avtale mellom partene, kan det henvises til denne.*

## 2. Typer personopplysninger

Følgende typer personopplysninger vil bli behandlet av partene under Avtalen*:*

*Kommentar: Gi en kort (gjerne punktvis) oversikt over hvilke hovedtyper personopplysninger som vil bli behandlet av partene. Angi om de er sensitive og hvorvidt dataene er direkte identifiserbare eller avidentifiserte/pseudonymiserte (dvs. om data fremstår som anonyme, men hvor man faktisk kan gå tilbake og finne ut hvem dataene/informasjonen gjelder).*

## 3. Kategorier av registrerte

Personopplysningene som behandles under Avtalen angår følgende kategorier av registrerte:

*Kommentar: Gi en kort oversikt over hvem opplysningene gjelder, for eksempel forskningsdeltakere, studenter og ansatte.*

## 4. Beskrivelse av roller

[*Navn 1*] vil i hovedsak ha følgende rolle og utføre følgende behandlingsaktiviteter under Avtalen:

*Kommentar: Innta en overordnet beskrivelse av partens rolle i tilknytning til databehandlingen og hvilke hovedtyper behandlingsaktiviteter vedkommende vil utføre.*

[*Navn 2*] vil i hovedsak ha følgende rolle og utføre følgende behandlingsaktiviteter under Avtalen:

*Kommentar: Innta en overordnet beskrivelse av partens rolle i tilknytning til databehandlingen og hvilke hovedtyper behandlingsaktiviteter vedkommende vil utføre.*

## 5. Godkjente databehandlere

Partene har avtalt at følgende databehandlere kan benyttes av respektive part under Avtalen:

[Navn 1]s databehandlere:

*[Angivelse av eventuelle godkjente databehandlere.]*

[Navn 2]s databehandlere:

*[Angivelse av eventuelle godkjente databehandlere.]*