

**AVTALE MELLOM DATABEHANDLER OG**

**UNDERDATABEHANDLER OM BEHANDLING**

**AV PERSONOPPLYSNINGER**

**(UNDERDATABEHANDLERAVTALE)**

I henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016, artikkel 28 nr. 4, jf. nr. 3, inngås følgende underdatabehandleravtale

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

mellom

[navn på underleverandør]

 (heretter kalt «underdatabehandler»)

og

[navn på institusjon/hovedleverandør]

 (heretter kalt «databehandler»)

*Avtaleteksten må tilpasses hver enkelt tjeneste/prosjekt og tjenesteleverandør.*

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

*[MERKNAD OM BRUK AV DENNE AVTALEMALEN:*

*Merk at den enkelte underdatabehandleravtale for å tjene sitt formål må være en direkte speiling av tilsvarende bestemmelser i hoveddatabehandleravtalen mellom behandlingsansvarlig og databehandler. Denne malen tar utgangspunkt i at det er NTNUs standardmal for (hoved)databehandleravtale som er benyttet mellom behandlingsansvarlig og databehandler. I alle tilfeller, uavhengig av hvilken avtalemal som er benyttet for hoveddatabehandleravtalen, er det viktig at alle bestemmelser i underdatabehandleravtalen kvalitetssikres nøye mot alle bestemmelser i hoveddatabehandleravtalen for å verifisere at den enkelte bestemmelse er speilet på riktig måte fra databehandler til underdatabehandler, jf. prinsippet i GDPR artikkel 28 nr. 4.]*

##  1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter i henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger.

Avtalen regulerer underdatabehandlers behandling av personopplysninger på vegne av databehandler, herunder ved innsamling, registrering, sammenstilling, lagring eller utlevering av personopplysninger, eller kombinasjoner av disse, i forbindelse med databehandleroppdraget.

Underdatabehandler er innforstått med at databehandler opptrer på vegne av en behandlingsansvarlig for de personopplysninger som omfattes av avtalen, og at underdatabehandler gjennom denne avtalen er pålagt tilsvarende forpliktelser som databehandler er pålagt i avtalen med behandlingsansvarlig, jf. GDPR artikkel 28 nr. 4.

Avtalen skal sikre at personopplysninger ikke brukes ulovlig, urettmessig eller at opplysningene behandles på måter som fører til uautorisert tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Ved motstrid skal vilkårene i denne avtalen gå foran underdatabehandlers personvernerklæring eller vilkår i andre avtaler inngått mellom databehandler og underdatabehandler i forbindelse med databehandleroppdraget.

Det skal angis i avtalens bilag 1 dersom underdatabehandleren kan benytte egne underleverandører under avtalen, herunder for oppbevaring, bearbeiding eller annen behandling, jf. punkt 8.

Behandlingens formål, typer behandlingsaktiviteter, kategorier av registrerte og hvilke typer personopplysninger som vil bli behandlet, 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.

## 2. Instrukser

Underdatabehandler skal følge de skriftlige og dokumenterte instrukser for behandling av personopplysninger som databehandler har bestemt skal gjelde.

Underdatabehandler forplikter seg til å overholde alle plikter i henhold til gjeldende personvernregelverk som gjelder ved behandling av personopplysninger.

Underdatabehandler forplikter seg til å varsle databehandler dersom underdatabehandler mottar instrukser fra databehandler som er i strid med personvernregelverket.

*Kommentar: Detaljerte instrukser til underdatabehandler kan legges ved som bilag til underdatabehandleravtalen.*

## 3. De registrertes rettigheter

Underdatabehandler plikter å bistå databehandler ved den behandlingsansvarliges ivaretakelse av den registrertes rettigheter i henhold til personvernregelverket.

Den 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 og retten til å kreve at behandlingen av egne personopplysninger begrenses.

I den grad det er relevant, skal underdatabehandler bistå databehandler i forbindelse med den behandlingsansvarliges ivaretakelse av de registrertes rett til dataportabilitet og retten til å motsette seg automatiske avgjørelser, inkludert profilering.

Underdatabehandler er erstatningsansvarlig overfor de registrerte dersom feil eller forsømmelser hos underdatabehandler påfører de registrerte økonomiske eller ikke-økonomiske tap som følge av at deres rettigheter eller personvern er krenket.

**4. Tilfredsstillende informasjonssikkerhet**

Underdatabehandler skal iverksette 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.

Underdatabehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske sikringstiltak. Dokumentasjonen skal være tilgjengelig for databehandler. Databehandler kan gi behandlingsansvarlig tilgang til dokumentasjonen for at behandlingsansvarlig skal kunne ivareta sine plikter etter personvernregelverket.

Underdatabehandler skal etablere kontinuitets- og beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser. Dokumentasjonen skal være tilgjengelig for databehandler. Databehandler kan gi behandlingsansvarlig tilgang til dokumentasjonen for at behandlingsansvarlig skal kunne ivareta sine plikter etter personvernregelverket.

Underdatabehandler skal gi egne ansatte tilstrekkelig informasjon om og opplæring i informasjonssikkerhet slik at sikkerheten til personopplysninger som behandles på vegne av databehandler blir ivaretatt.

Underdatabehandler skal dokumentere opplæringen av egne ansatte i informasjonssikkerhet. Dokumentasjonen skal være tilgjengelig for databehandler. Databehandler kan gi behandlingsansvarlig tilgang til dokumentasjonen for at behandlingsansvarlig skal kunne ivareta sine plikter etter personvernregelverket.

*Kommentar: Her kan det være behov for å konkretisere de viktigste sikringstiltakene som underdatabehandleren har iverksatt, eventuelt at det henvises til dokumenter eller publikasjoner som forklarer hvordan underdatabehandleren jobber med informasjonssikkerhet og hvilke sikringstiltak som er etablert for den aktuelle tjenesten. Konkretiseringene kan tas inn i selve avtaleteksten eller i bilag til avtalen.*

**5. Taushetsplikt**

Kun ansatte hos underdatabehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes på vegne av databehandler, kan gis slik tilgang. Underdatabehandler plikter å dokumentere retningslinjer og rutiner for tilgangsstyring. Dokumentasjonen skal være tilgjengelig for databehandler. Databehandler kan gi behandlingsansvarlig tilgang til dokumentasjonen for at behandlingsansvarlig skal kunne ivareta sine plikter etter personvernregelverket.

Underdatabehandler skal sørge for at ansatte hos underdatabehandler pålegges 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 underdatabehandler anvender for å levere tjenesten.

Databehandler skal sørge for tilsvarende tilgangskontroll og taushetsplikt om den dokumentasjon underdatabehandler tilgjengeliggjør overfor databehandler.

Norsk lov vil kunne begrense omfanget av taushetsplikten for ansatte hos underdatabehandler og underleverandører.

**6. Tilgang til dokumentasjon**

Underdatabehandler plikter å gi databehandler tilgang til all dokumentasjon som er nødvendig for at databehandler skal kunne bistå behandlingsansvarlig med å ivareta sine forpliktelser i henhold til personvernregelverket.

Underdatabehandler plikter å gi databehandler tilgang til annen relevant dokumentasjon som gjør det mulig for databehandler å vurdere om underdatabehandler overholder vilkårene i denne avtalen.

Databehandler kan gi behandlingsansvarlig tilgang til dokumentasjonen for at behandlingsansvarlig skal kunne ivareta sine plikter etter personvernregelverket, men har for øvrig taushetsplikt med hensyn til konfidensiell dokumentasjon som underdatabehandler gjør tilgjengelig for databehandler.

**7. Varslingsplikt ved sikkerhetsbrudd**

Underdatabehandler skal uten ubegrunnet opphold varsle databehandler dersom personopplysninger som behandles på vegne av databehandler utsettes for sikkerhetsbrudd som innebærer risiko for krenkelser av de registrertes personvern.

Varslet til databehandler 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.

Databehandler er ansvarlig for at varsler om sikkerhetsbrudd fra underdatabehandler blir videreformidlet til behandlingsansvarlig.

## 8. Underleverandører

Underdatabehandler plikter å inngå egne avtaler med eventuelle underleverandører som regulerer underleverandørens behandling av personopplysninger på vegne av underdatabehandler.

I avtaler mellom underdatabehandler og underleverandører skal underleverandørene pålegges å ivareta alle plikter som underdatabehandleren selv er underlagt i henhold til denne avtalen. Underdatabehandler plikter å forelegge avtalene for databehandler på forespørsel. Databehandler kan forelegge avtalene for behandlingsansvarlig.

Underdatabehandler skal kontrollere at alle underleverandører overholder sine avtalemessige plikter, spesielt at informasjonssikkerheten er tilfredsstillende og at ansatte hos underleverandører er kjent med sine forpliktelser og oppfyller disse.

Databehandler godkjenner at underdatabehandler engasjerer de underleverandører som er angitt i bilag 1 til denne avtalen.

Underdatabehandler kan ikke engasjere andre underleverandører enn de som er nevnt i bilag 1 uten at dette på forhånd er godkjent av databehandler. Ved slik endring skal det utarbeides et endringsbilag som dateres og signeres av begge parter.

Underdatabehandler er erstatningsansvarlig overfor databehandler i henhold til punkt 13 for økonomiske tap som påføres databehandler og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandører.

**9. Overføring til land utenfor EU/EØS**

Overføring av personopplysninger til land utenfor EU/EØS må godkjennes av databehandler, og må fremgå av bilag 1 til denne avtalen.

## 10. Sikkerhetsrevisjoner og konsekvensutredninger

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

Sikkerhetsrevisjoner skal omfatte underdatabehandlers 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 databehandler ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner.

Underdatabehandler skal dokumentere sikkerhetsrevisjonene. Databehandler skal gis tilgang til revisjonsrapportene. Databehandler kan gi behandlingsansvarlig tilgang til dokumentasjonen for at behandlingsansvarlig skal kunne ivareta sine plikter etter personvernregelverket.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos underdatabehandler, skal databehandler informeres om hvilken revisor som benyttes og få tilgang til oppsummeringer av revisjonsrapportene. Databehandler kan gi behandlingsansvarlig tilgang til oppsummeringer av revisjonsrapportene for at behandlingsansvarlig skal kunne ivareta sine plikter etter personvernregelverket. Underdatabehandler skal, etter forespørsel fra databehandler, bistå databehandler dersom bruk av tjenesten medfører at behandlingsansvarlig har plikt til å vurdere personvernkonsekvenser, jf. forordning (EU) 2016/679, artikkel 35 og 36. Underdatabehandler kan bistå ved iverksetting av personvernfremmende tiltak dersom konsekvensutredningen viser at dette er nødvendig.

*Kommentar: Partene kan avtale at databehandler selv utfører sikkerhetsrevisjoner hos underdatabehandleren, eventuelt også hvordan kostnader som påløper i forbindelse med slike revisjoner skal fordeles. Dette kan tas inn her, evt. i tjenesteavtalen.*

*Dette punktet skal ivareta mulighet for å kontrollere underdatabehandlers oppfyllelse av personvernregelverket. Underdatabehandler forplikter seg til gjennomføring av sikkerhetsrevisjoner av personvernarbeidet for å sikre overholdelse av GDPR. Dette kan f.eks. være en kontroll av om underdatabehandleren har egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personvernforordningen og verner de registrertes rettigheter. Dersom det benyttes underleverandører kan dette også være en kontroll av at det foreligger databehandleravtale med dem.*

*Det kan avtales at partene gjennomfører en slik sikkerhetsrevisjon selv, eller det kan avtales at en uavhengig tredjepart gjennomfører det. I så fall kan man sette inn følgende tekst: «Partene har avtalt at [databehandler ev. navn på firma] utfører sikkerhetsrevisjon hos underdatabehandleren. Kostnader skal fordeles slik: [fyll inn]»*

*Hvor omfattende en slik revisjon skal være avhenger av databehandleroppdragets art og omfang, men poenget er at databehandler skal ha adgang til å kontrollere at underdatabehandler oppfyller sine plikter.*

## 11. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter underdatabehandler å slette og/eller tilbakelevere alle personopplysninger som underdatabehandleren behandler på vegne av databehandler i forbindelse med databehandleroppdraget. Databehandler bestemmer hvordan tilbakelevering av personopplysninger skal skje, herunder hvilket format som skal benyttes.

Underdatabehandler skal slette personopplysninger fra alle lagringsmedier som inneholder personopplysninger som underdatabehandler behandler på vegne av databehandler innen *[fyll inn antall]* dageretter avtalens opphør. Dette gjelder også for sikkerhetskopier av personopplysningene. Databehandler skal benytte et sletteverktøy som godkjennes av behandlingsansvarlig.

Underdatabehandler skal dokumentere at sletting av personopplysninger er foretatt i henhold til denne avtalen. Dokumentasjonen skal gjøres tilgjengelig for databehandler. Databehandler kan gi behandlingsansvarlig tilgang til dokumentasjonen for at behandlingsansvarlig skal kunne ivareta sine plikter etter personvernregelverket.

Underdatabehandler dekker alle kostnader i forbindelse med tilbakelevering og sletting av de personopplysninger som omfattes av denne avtalen.

*Kommentar: Partene kan eventuelt avtale nærmere hvordan kostnader som påløper i forbindelse med sletting eller tilbakelevering av personopplysninger skal fordeles, enten her eller i Hovedavtalen.*

**12. Mislighold**

Ved vesentlig mislighold av vilkårene i denne avtalen som skyldes feil eller forsømmelser fra underdatabehandlers side, kan databehandler si opp avtalen med øyeblikkelig virkning. Underdatabehandler vil fortsatt være pliktig til å tilbakelevere og/eller slette personopplysninger som behandles på vegne av databehandler i henhold til bestemmelsene i punkt 11 ovenfor.

**13. Erstatning**

Databehandler kan kreve erstatning for økonomiske tap som feil eller forsømmelser fra underdatabehandlers side, inkludert mislighold av vilkårene i denne avtalen, har påført databehandler, jf. også punkt 3 og 8 ovenfor.

*[Følgende avsnitt inntas hvis NTNU er underdatabehandler:]*

[*Underdatabehandler er erstatningsansvarlig for direkte økonomisk tap, herunder administrative overtredelsesgebyr og erstatningskrav som rettes mot databehandler, som kan tilbakeføres til brudd på underdatabehandlerens forpliktelser i henhold til denne avtalen.]*

Samlet erstatning per kalenderår er begrenset til et beløp som tilsvarer Hovedavtalens samlede årlige vederlag ekskl. merverdiavgift.

Har underdatabehandler eller noen denne svarer for utvist grov uaktsomhet eller forsett, gjelder ikke de ovennevnte erstatningsbegrensningene.

## 14. Avtalens varighet

Denne avtalen gjelder så lenge underdatabehandler behandler personopplysninger på vegne av databehandler i henhold til *[hovedavtale av xx.yy.ZZZZ]*

## 15. Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er:

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

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er:

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

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

*[Alternativ 1]*

**16. Lovvalg og verneting**

Avtalen er underlagt norsk rett og partene vedtar Trøndelag tingrett som verneting. Dette gjelder også etter opphør av avtalen.

*Kommentar: Dette punktet gjelder når databehandler eller behandlingsansvarlig er en privat aktør, eller andre aktører som ikke er statlig universitet eller høyskole. Trøndelag tingrett er skrevet inn som standard. Denne kan endres om ønskelig.*

*[Alternativ 2]*

## 16. 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 både databehandler og underdatabehandler er et annet statlig universitet eller høyskole.*

\*\*\*

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

Sted og dato

 På vegne av databehandler På vegne av underdatabehandler

……………………….. ………………………

(underskrift) (underskrift)

**BILAG 1 – SPESIFIKASJON AV BEHANDLINGSAKTIVITETER**

**1. Formål og typer behandlingsaktiviteter**

Formålet med underdatabehandlers behandling av personopplysninger på vegne av databehandler, er å [*angi et klart formål med behandlingen i henhold til Hovedavtalen*].

*Kommentar: MÅ fylles ut, det må angis klart og tydelig hva data skal brukes til. Eventuelle koblinger med andre datasett må være godkjent av databehandler. Dersom formålet fremgår av andre avtaler, for eksempel kontrakter, som er inngått mellom databehandler/underdatabehandler og kvalitetssikret av jurist ved NTNU, kan det isteden henvises til disse avtalene når formålet for behandling av opplysningene skal beskrives.*

Følgende typer behandlingsaktiviteter er aktuelle under avtalen:

*[Angi relevante typer behandlingsaktiviteter, som f.eks. registrering, analyse, bruk som grunnlag for fakturering, arkivering etc.]*

**2. Typer personopplysninger og kategorier av registrerte**

Underdatabehandler behandler følgende kategorier personopplysninger på vegne av databehandler i forbindelse med Hovedavtalen:

* List opp kategorier av personopplysninger

Personopplysningene gjelder følgende kategorier registrerte:

* List opp hvem personopplysningene gjelder for (studenter, ansatte, osv.)

**3. Overføring til land utenfor EU/EØS**

*Kommentar: Personopplysninger som underdatabehandler behandler på vegne av databehandler kan bli overført til land utenfor EU/EØS (tredjeland). Slik overføring kan skje på visse vilkår. Reglene om overføring til tredjeland finnes i Artikkel 45-47 og 49 i EUs personvernforordning. Reglene gjelder også for sikkerhetskopiering og annen overføring av personopplysninger som skjer i forbindelse med administrasjon av den aktuelle tjenesten, for eksempel support. 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 (EUs «Standard Contractual Clauses»). Bruk av sistnevnte krever at avtalen inngås direkte mellom behandlingsansvarlig og underdatabehandler, noe som ofte ordnes ved en avtalefullmakt fra behandlingsansvarlig til databehandler. Personvernjurist i virksomheten bør konfereres i disse tilfellene.*

*[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 databehandler på forhånd.

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

Personopplysninger som underdatabehandler behandler 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.*

**4. Godkjente underleverandører**

Databehandler har godkjent at underdatabehandler benytter følgende underleverandører under avtalen:

*[Angivelse av eventuelle godkjente underleverandører.]*