**Mal for databehandleravtaler HiØ**

**Versjon 1.4.1**

**Sist revidert: 15.03.2023**

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

Databehandleravtale

Mellom

**Høgskolen i Østfold**

Organisasjonsnr.: 971 567 376

heretter "Behandlingsansvarlig"

og

**……..**

Organisasjonsnr.: ….

heretter "Databehandler "

## 1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter i henhold til gjeldende norsk personopplysningslovgivning. I henhold til personopplysningsloven med forskrift, er universiteter og høyskoler ansvarlige for å sikre personvernet til enkeltpersoner – studenter, ansatte, gjester og respondenter eller informanter i forskning – når institusjonene behandler personopplysninger om dem.

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.

Avtalen regulerer databehandlers forvaltning av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, i forbindelse med bruk av/behandling i (navn på tjeneste/prosjekt).

Vilkårene i denne avtalen går foran vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler knyttet til (navn på tjeneste/prosjekt).

**2. Formålsbegrensning**

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er (fyll inn formålet).

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål uten at dette på forhånd er godkjent av behandlingsansvarlig.

## Databehandler kan ikke overføre personopplysninger som omfattes av denne avtalen til samarbeidspartnere eller andre tredjeparter uten at dette på forhånd er godkjent av behandlingsansvarlig, jf. punkt 10 i denne avtalen.

## 3. Instrukser

Databehandler skal følge de skriftlige og dokumenterte instrukser for forvaltning av personopplysninger i (navnet på tjeneste/prosjekt) som behandlingsansvarlig har bestemt skal gjelde.

(Navn på institusjon/virksomhet) forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av (navn på tjeneste/prosjekt) til behandling av personopplysninger.

Databehandler forplikter seg til å varsle behandlingsansvarlig dersom databehandler mottar instrukser fra behandlingsansvarlig som er i strid med bestemmelsene i gjeldende norsk personopplysningslovgivning.

* Kommentar: Detaljerte instrukser til databehandler kan legges ved som bilag til databehandleravtalen (Se eksempel i bilag 1).

**4. Opplysningstyper og registrerte**

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige dreier seg primært om (karakteren av behandlingen):

* Kommentar: Beskriv karakteren av behandlingen

Databehandleren forvalter følgende personopplysninger på vegne av behandlingsansvarlig:

* Kommentar: Gi en kort (gjerne punktvis) oversikt over hvilke hovedtyper personopplysninger som tjenesteleverandøren (databehandleren) forvalter på vegne av institusjonen/virksomheten (behandlingsansvarlig).

Eksempel:

Epostadresse, portrettbilder

Bruker- ID

Gruppetilhørighet (fag, foreninger)

Personopplysningene gjelder følgende registrerte:

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

##

## 5. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretakelse av den registrertes rettigheter i henhold til gjeldende norsk personopplysningslovgivning.

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.

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

**6. Tilfredsstillende informasjonssikkerhet**

Databehandler 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.

Databehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske sikringstiltak. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler skal etablere kontinuitets- og beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandleren skal sikre at personopplysninger som behandles for én Databehandlings­ansvarlig holdes atskilt fra egne og andre databehandlingsansvarliges opplysninger og tjenester.

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

* Kommentar: Her kan det være behov for å konkretisere de viktigste sikringstiltakene som databehandleren har iverksatt, eventuelt at det henvises til dokumenter eller publikasjoner som forklarer hvordan databehandleren jobber med informasjonssikkerhet og hvilke sikringstiltak som er etablert for den aktuelle tjenesten. HiØ oppfordrer prosjekter til å lage en datahåndteringsplan, denne kan vedlegges.

**7. Taushetsplikt**

Kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes på vegne av behandlingsansvarlig, kan gis slik tilgang. Databehandler plikter å dokumentere retningslinjer og rutiner for tilgangsstyring. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Ansatte hos databehandler 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 databehandler anvender for å levere tjenesten, jf. punkt 10 i denne avtalen.

Norsk lov vil kunne begrense omfanget av taushetsplikten for ansatte hos databehandler og tredjeparter.

**8. Tilgang til sikkerhetsdokumentasjon**

Databehandler plikter på forespørsel å gi behandlingsansvarlig tilgang til all sikkerhetsdokumentasjon som er nødvendig for at behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til gjeldende norsk personopplysningslovgivning.

Databehandler plikter på forespørsel å gi behandlingsansvarlig tilgang til annen relevant dokumentasjon som gjør det mulig for behandlingsansvarlig å vurdere om databehandler overholder vilkårene i denne avtalen.

Behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

**9. Varslingsplikt ved sikkerhetsbrudd**

Databehandler skal uten ugrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd, jf. personopplysningsforskriften §2-6.

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 de registrerte, Datatilsynet og personvernombud blir varslet når dette er påkrevd.

## 10. Underleverandører

Databehandler plikter å inngå egne avtaler med underleverandører som regulerer underleverandørenes forvaltning av personopplysninger i forbindelse med denne avtalen.

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

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

Behandlingsansvarlig godkjenner at databehandler engasjerer følgende underleverandører for å oppfylle denne avtalen:

|  |  |  |  |
| --- | --- | --- | --- |
| NAVN | ORG. NR.  | ADRESSE/LOKASJON | BESKRIVELSE AV BEHANDLING |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Databehandler kan ikke engasjere andre underleverandører enn de som er nevnt ovenfor uten at dette på forhånd er skriftlig godkjent av behandlingsansvarlig.

Databehandler er erstatningsansvarlig overfor behandlingsansvarlig for økonomiske tap som påføres behandlingsansvarlig og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandører.

## 11. Overføring til land utenfor EU/EØS – tredjeland

Enhver overføring av personopplysninger til tredjestater eller internasjonale organisasjoner må kun foretas av databehandleren på bakgrunn av dokumentert instruks fra den behandlingsansvarlige og skal alltid skje i overensstemmelse med personvernforordningens kapittel V.

## 12. Sikkerhetsrevisjoner og konsekvensutredninger

Databehandler 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 databehandlers sikkerhetsmål og sikkerhetsstrategi, sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, etablerte tekniske, fysiske og organisatoriske sikringstiltak og arbeidet med informasjonssikkerhet hos underleverandører til denne avtalen. Det skal i tillegg omfatte rutiner for varsling av behandlingsansvarlig ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner.

Databehandler skal dokumentere sikkerhetsrevisjonene. Behandlingsansvarlig skal gis tilgang til revisjonsrapportene på forespørsel.

Evt. tillegg: Partene kan avtale at behandlingsansvarlig selv, eller en uavhengig tredjepart som behandlingsansvarlig selv velger, utfører sikkerhetsrevisjoner hos databehandleren, eventuelt også hvordan kostnader som påløper i forbindelse med slike revisjoner skal fordeles.

## 13. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å tilbakelevere og slette alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til denne avtalen. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

Sletting skal skje ved at databehandler sletter personopplysninger innen (fyll inn antall) dager etter avtalens opphør. Dette gjelder også for sikkerhetskopier av personopplysningene.

Databehandler skal dokumentere at sletting av personopplysninger er foretatt i henhold til denne avtalen. Dokumentasjonen skal gjøres tilgjengelig for behandlingsansvarlig på forespørsel.

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

**14. Mislighold**

Ved mislighold av vilkårene i denne avtalen som skyldes feil eller forsømmelser fra databehandlers side, kan behandlingsansvarlig si opp avtalen med øyeblikkelig virkning. Databehandler vil fortsatt være pliktig til å tilbakelevere og slette personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 12 ovenfor.

Behandlingsansvarlig kan kreve erstatning for økonomiske tap som feil eller forsømmelser fra databehandlers side, inkludert mislighold av vilkårene i denne avtalen, har påført behandlingsansvarlig.

## 15. Avtalens varighet

Denne avtalen gjelder så lenge databehandler forvalter personopplysninger på vegne av behandlingsansvarlig

eller

avtalen gjelder til \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Avtalen kan sies opp av begge parter med en gjensidig frist på \_\_\_\_\_\_.

##

## 16. Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er: \_\_\_\_\_\_\_\_\_\_\_.

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er: \_\_\_\_\_\_\_\_\_\_\_.

**17. Lovvalg og verneting**

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

\*\*\*

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

Sted og dato

 På vegne av behandlingsansvarlig På vegne av databehandler

……………………….. ………………………

(underskrift) (underskrift)

**Bilag 1: Instruks vedrørende behandling av personopplysninger**

1. **Behandlingens gjenstand/instruks**

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skjer ved at databehandleren utfører følgende:

<beskriv behandlingen, som databehandleren instrueres til å foreta>

1. **Behandlingssikkerhet**

Sikkerhetsnivået skal avspeile:

<beskriv – under hensyn til behandlingens karakter, omfang, sammenheng og formål, samt risikoene av varierende sannsynlighet og alvor for fysiske personers rettigheter – elementene som er avgjørende for sikkerhetsnivået>

*Eksempelvis: Behandlingen omfatter en større mengde personopplysninger som faller inn under personvernforordningen artikkel 9 hva angår “særlige kategorier av personopplysninger”. Av den grunn stilles det krav til at det etableres et høyt sikkerhetsnivå.*

Databehandleren er heretter berettiget og forpliktet til å treffe beslutninger om hvilke tekniske og organisatoriske sikkerhetstiltak som skal gjennomføres for å etablere det nødvendige og avtalte sikkerhetsnivå. Databehandleren skal likevel – under alle omstendigheter og som minimum – gjennomføre følgende tiltak, som er avtalt med den behandlingsansvarlige:

*Fyll inn hvilke tiltak din virksomhet har utført. Tiltakene opplistet er eksempler. Ved ytterligere/andre tiltak iverksatt vennligst beskriv disse.*

<beskriv kravene til psedonymisering og kryptering av personopplysninger>

<beskriv kravene som gjelder å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og –tjenester>

<beskriv kravene som gjelder evnen til å gjenopprette tilgjengeligheten av og adgangen til personopplysninger i tilfelle av en fysisk eller teknisk hendelse>

<beskriv kravene som gjelder prosedyrer for regelmessig testing, vurdering og evaluering av de tekniske og organisatoriske tiltak til sikring av behandlingssikkerheten>

<beskriv kravene som gjelder adgang til opplysningene via internett>

<beskriv kravene som gjelder beskyttelse av opplysninger under overføring>

<beskriv kravene hva angår beskyttelse av opplysninger under oppbevaring>

<beskriv kravene som gjelder fysisk sikring av lokaliteter hvor det behandles personopplysninger>

<beskriv kravene som gjelder anvendelse av hjemme-/fjernarbeidsplasser>

<beskriv kravene hva angår loggføring>

1. **Rutine for oppbevaring/Rutine for sletting**

<beskriv eventuell oppbevaringsperiode/sletterutiner for databehandleren>

*Eksempelvis: Personopplysninger oppbevares i [angi tidsperiode], hvoretter de slettes hos databehandleren.*

1. **Lokalitet for behandling**

Behandling av de av Bestemmelsene omfattende personopplysninger kan ikke uten den behandlingsansvarliges forutgående skriftlige godkjennelse skje på andre lokaliteter enn følgende:

<angi hvor behandlingen finner sted. angi hvilken databehandler eller underdatabehandler som anvender adressen>

1. **Instruks vedrørende overføring av personopplysninger til tredjestater**

<beskriv instruksen hva angår overførsel av personopplysninger til tredjestater eller internasjonale organisasjoner>

<angi grunnlaget for overførselen som omhandlet i personvernforordningen kapittel v>

1. **Prosedyre for den behandlingsansvarliges revisjoner, herunder inspeksjoner, med behandlingen av personopplysninger som er overlatt til databehandleren**

<beskriv prosedyrene for den behandlingsansvarliges revisjoner, herunder inspeksjoner, med behandlingen av personopplysninger som er overlatt til databehandleren>

*Eksempelvis;*

*Den behandlingsansvarlige eller en representant for den behandlingsansvarlige fortar [angi tidsperiode] en fysisk inspeksjon av lokalene hvor databehandleren fortar behandling av personopplysningene fra, herunder fysiske lokaler og systemer, som benyttes til eller i forbindelse med behandling av personopplysninger, med det formål om å fastslå databehandlerens overholdelse av personvernforordningen, personvernbestemmelser i annen EU-rett eller medlemsstatenes nasjonale rett og bestemmelsene som fremgår av denne avtale.*

*Ut over det planlagte tilsyn, kan den behandlingsansvarlige gjennomføre en inspeksjon hos databehandlere når den behandlingsansvarlige finner det nødvendig.*