**Mal for databehandleravtaler**

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

I henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016 (GDPR), Artikkel 28 og 29, jf. Artikkel 32-36, inngås følgende avtale

mellom

Navn på institusjonen

.……………………….

(behandlingsansvarlig)

og

Navn på tjenesteleverandøren

………………………….

(databehandler)

|  |  |  |
| --- | --- | --- |
| **Endret:** | **Endret av:** | **Dato:** |
|  |  |  |
|  |  |  |

## 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 og om fri utveksling av slike opplysninger, samt om oppheving av direktiv 95/46/EF.

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).

Ved motstrid skal vilkårene i denne avtalen gå foran databehandlers personvernerklæring eller vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler i forbindelse med bruk av/behandling i (navn på tjeneste/prosjekt).

**2. Formålsbegrensning**

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er å levere og administrere/annen type behandling (navn på tjeneste/prosjekt).

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål enn levering og administrasjon av/annen type behandling (navn på tjeneste/prosjekt) 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 9 i denne avtalen.

## 3. Instrukser

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

(Navn på institusjon) forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av/behandling i (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 billag til databehandleravtalen.

**4. Opplysningstyper og registrerte**

Databehandleren forvalter følgende personopplysninger på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av (navn på tjeneste/prosjekt):

* Kommentar: Gi en kort (gjerne punktvis) oversikt over hvilke hovedtyper personopplysninger som tjenesteleverandøren (databehandleren) forvalter på vegne av institusjonen (behandlingsansvarlig).
* Kommentar: Gi en kort oversikt over hvilke opplysninger som databehandler registrer og lagrer i forbindelse med bruk av tjenesten, for eksempel ved bruk av informasjonskapsler.

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 og dokumentasjon**

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 plikter på forespørsel fra behandlingsansvarlig å gi tilgang til dokumentasjon, herunder sikkerhetsdokumentasjon, som er nødvendig for at behandlingsansvarlig kan etterleve sine forpliktelser etter GDPR.

Databehandler plikter på forespørsel fra behandlingsansvarlig å gi tilgang til all øvrig informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i denne avtalen er oppfylt.

* 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. Konkretiseringene kan tas inn i selve avtaleteksten eller i billag til avtalen.

**7. Taushetsplikt**

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 behandler personopplysningene.

**8. Varslingsplikt ved sikkerhetsbrudd**

Databehandler skal uten ubegrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd som innebærer risiko for krenkelser av de registrertes personvern.

Varslet 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 varsler om sikkerhetsbrudd fra databehandler blir videreformidlet til Datatilsynet.

## 9. Underleverandører

Databehandler plikter å inngå egne avtaler med underleverandører til (navn på tjeneste/prosjekt) som regulerer underleverandørenes forvaltning av personopplysninger i forbindelse med levering og administrasjon av/annen type behandling (navn på tjeneste/prosjekt).

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

Databehandler skal kontrollere at underleverandører til (navn på tjeneste/prosjekt) 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 i forbindelse med levering og administrasjon av/annen type behandling (navn på tjeneste/prosjekt):

…………………………………………………………………………………………………... (navn på underleverandører).

Databehandler kan ikke engasjere andre underleverandører enn de som er nevnt ovenfor uten at dette på forhånd er 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 til (navn på tjeneste/prosjekt).

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

* Kommentar: Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig 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 GDPR. Disse reglene innebærer blant annet at overføringen vil være lovlig dersom den skjer til et EU-godkjente 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, for eksempel ved supporttjenester.

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).

## 11. 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.

Behandlingsansvarlig skal gis tilgang til revisjonsrapporter på forespørsel.

* Kommentar: Partene kan avtale at behandlingsansvarlig selv utfører sikkerhetsrevisjoner hos databehandleren, eventuelt også hvordan kostnader som påløper i forbindelse med slike revisjoner skal fordeles.

Databehandler plikter på forespørsel fra behandlingsansvarlig å bistå behandlingsansvarlig dersom bruk av/behandling i (navn på tjeneste/prosjekt) medfører at behandlingsansvarlig har plikt til å utrede personvernkonsekvenser før (navn på tjeneste/prosjekt) tas i bruk/settes i gang, jf. GDPR Artikkel 35 og 36.

## 12. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å slette og tilbakelevere alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av/behandling i (navn på tjeneste/prosjekt). Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

Databehandler skal slette personopplysninger fra alle lagringsmedier som inneholder personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig. Sletting skal skje ved at databehandler skriver over 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.

Databehandler 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.

**13. 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 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, jf. også punkt 5 og 9 ovenfor.

## 14. 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 \_\_\_\_\_\_.

## 15. Kontaktpersoner

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

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

**16. Lovvalg og verneting**

Eventuelle tvister som springer ut av denne avtalen skal først søkes løst gjennom forhandlinger.

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

\*\*\*

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

Sted og dato:

….……………………….. ….…………………………..

(behandlingsansvarlig) (databehandler)