



AVTALE OM BEHANDLING AV PERSONOPPLYSNINGER (DATABEHANDLERAVTALE)

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

Stoffkartotek og eksponeringsregister

mellom

NTNU

.....

(behandlingsansvarlig)

og

[Navn på databehandler]

.....

(databehandler)

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter etter Lov av 15. juni 2018 nr. 38 om behandling av personopplysninger og EUs personvernforordning (GDPR). Norsk lov og EUs forordning omtales heretter som personvernregelverket.

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 behandling av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, i forbindelse med bruk av/behandling i *stoffkartotek og eksponeringsregister*.

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

2. Formålsbegrensning

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er å levere stoffkartotek og eksponeringsregister.

Personopplysninger som databehandler behandler på vegne av behandlingsansvarlig kan ikke brukes til andre formål enn beskrevet ovenfor, 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 databehandleroppdraget som behandlingsansvarlig har bestemt skal gjelde.

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

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

4. Opplysningstyper og registrerte

Databehandleren behandler følgende personopplysninger på vegne av behandlingsansvarlig i forbindelse med *databehandleroppdraget*:

Kommentar: Gi en kort (gjærne punktvis) oversikt over hvilke hovedtyper personopplysninger som tjenesteleverandøren (databehandleren) behandler på vegne av behandlingsansvarlig. Angi om de er f.eks. er sensitive. Angi hvorvidt disse data er direkte identifiserbare eller aidentifiserte/pseudonymiserte (dvs. om data fremstår som anonyme, men hvor man faktisk kan gå tilbake og finne ut hvem dataene/informasjonen gjelder.)

Kommentar: Gi en kort oversikt over hvilke opplysninger som databehandler registrerer 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 forskningsdeltakere, studenter og ansatte.

5. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretagelse 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 databehandler bistå behandlingsansvarlig med å ivareta de registrertes rett til dataportabilitet og retten til å motsette seg automatiske avgjørelser, inkludert profilering.

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.

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

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

Databehandler skal dokumentere opplæringen av egne ansatte i informasjonssikkerhet. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

7. Taushetsplikt

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

Databehandler skal sørge for at ansatte hos databehandler 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 databehandler anvender for å levere tjenesten.

Behandlingsansvarlig skal sørge for tilsvarende tilgangskontroll og taushetsplikt om den dokumentasjon databehandler tilgjengeliggjør overfor behandlingsansvarlig.

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

8. Tilgang til sikkerhetsdokumentasjon

Databehandler plikter å gi behandlingsansvarlig tilgang til all sikkerhetsdokumentasjon som er nødvendig for at behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til personvernregelverket.

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

Ansatte hos behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

9. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ubegrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som behandles 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 Datatilsynet blir varslet når dette er påkrevd etter personvernregelverket.

10. Underleverandører

Databehandler plikter å inngå egne avtaler med underleverandører som regulerer underleverandørenes behandling av personopplysninger i forbindelse med databehandleroppdraget.

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 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.

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

[Alternativ 1: Hvis det skal brukes underleverandører]

Behandlingsansvarlig godkjenner at databehandler engasjerer følgende underleverandører i forbindelse med databehandleroppdraget

[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 jf. pkt. 14 overfor behandlingsansvarlig for økonomiske tap som påføres behandlingsansvarlig og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandører.

[Alternativ 2: Hvis det ikke skal brukes underleverandører]

Databehandler skal ikke benytte underleverandør for å oppfylle denne avtalen.

Om det blir behov for å engasjere underleverandører for å oppfylle denne avtalen, må dette skriftlig godkjennes av behandlingsansvarlig på forhånd.

Databehandler er erstatningsansvarlig jf. pkt. 14 overfor behandlingsansvarlig for økonomiske tap som påføres behandlingsansvarlig og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandører, som blir engasjert og godkjent etter avtalens inngåelse.

11. Overføring til land utenfor EU/EØS

Kommentar: Personopplysninger som databehandler behandler 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 EUs personvernforordning. 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. Reglene gjelder også for sikkerhetskopiering og annen overføring av personopplysninger som skjer i forbindelse med administrasjon av den aktuelle tjenesten, for eksempel support.

[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.

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 tilknyttet databehandleroppdraget. 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.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandler, skal behandlingsansvarlig informeres om hvilken revisor som benyttes og få tilgang til oppsummeringer av revisjonsrapportene på forespørsel. Databehandler skal bistå behandlingsansvarlig dersom databehandleroppdraget medfører at behandlingsansvarlig har plikt til å utrede personvernkonsekvenser før oppdraget settes i gang, jf. forordning (EU) 2016/679 av 27. april 2016, Artikkel 35 og 36. Databehandler kan bistå behandlingsansvarlig ved iverksetting av personvernforebyggende tiltak dersom konsekvensutredningen viser at dette er nødvendig.

13. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å slette og/eller tilbakelevere alle personopplysninger som behandles på vegne av behandlingsansvarlig i forbindelse med databehandleroppdraget. 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 behandler på vegne av behandlingsansvarlig, innen *rimelig tid* etter avtalens opphør. Dette gjelder også for sikkerhetskopier av personopplysningene. Databehandler skal benytte et sletteverktøy som godkjennes av behandlingsansvarlig.

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.

14. Mislighold

Ved vesentlig 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 behandles på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 13 ovenfor.

Behandlingsansvarlig kan kreve erstatning for direkte økonomiske tap som klanderverdige feil eller forsømmelser fra databehandlers side, inkludert mislighold av vilkårene i denne avtalen, har påført behandlingsansvarlig, jf. også punkt 5 og 10 ovenfor.

15. Avtalens varighet

Denne avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig, i henhold til hovedavtale for levering av stoffkartotek og eksponeringsregister.

16. Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er:

Se ssa-I bilag 5 Administrative bestemmelser

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er:

Se ssa-I bilag 5 Administrative bestemmelser

17. Lovvalg og verneting

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

Denne avtalen er inngår som vedlegg til hovedavtalen, og signeres digitalt samme med denne.

Navn på signatar og dato for signering fremkommer av signeringsbilaget.