Databehandleravtale med Folkehelseinstituttet

Dette dokumentet er signert digitalt av følgende undertegnere:

- LARS INGE OFTEDAL, signert 23.04.2021 med ID-Porten: BankID Mobil

Dokumentet innholder

- En forside med informasjon om signeringen
- Originaldokumentet med signaturdetaljer på hver side
- Digitalt integrerte signaturer

Dokumentet er forseglet av Posten Norge

Signeringen er gjort med en signaturtjeneste fra Posten Norge AS. Posten garanterer dermed for autentisiteten og forseglingen av dette dokumentet.

Slik ser du at signaturen er gyldig

Hvis du åpner dokumentet i Adobe Reader, skal det stå øverst at dokumentet er sertifisert av Posten Norge AS. Dette garanterer at innholdet i dokumentet ikke er endret etter signering.

Samleavtale for databehandling i TSD – Tjenester for Sensitive Data

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

mellom

Folkehelseinstituttet
(behandlingsansvarlig)

og

TSD, USIT, Universitetet i Oslo
(databehandler)

22.04.2021

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 Tjenester for Sensitive Data med integrerte løsninger (heretter TSD).

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 TSD.

Denne avtalen sammen med Tjenesteavtalen fungerer som en overordnet avtale mellom behandlingsansvarlig institusjon og databehandler. For hvert enkelt prosjekt som skal omfattes av denne overordnede avtalen skal et eget vedlegg fylles ut.

2. Formålsbegrensning

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er å muliggjøre behandlingsansvarliges lagring i og bruk av TSD i henhold til Tjenesteavtalen.

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 TSD som behandlingsansvarlig har bestemt skal gjelde.

Behandlingsansvarlig forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning, vedtak og godkjenninger som gjelder ved bruk av TSD 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.

Behandlingsansvarlig (ved prosjektleder) autoriserer prosjektmedarbeidere og/eller gir prosjektmedarbeidere tilgang til de enkelte arbeidsrommene på TSD.
Databehandler forplikter seg til å gi behandlingsansvarlig oversikter over prosjekter og medarbeidere ref. Tjenesteavtale Punkt 6 bestemmelse av periodiske møter mellom kunde og leverandør.

22.04.2021

4. Opplysningstyper og registrerte

Databehandleren forvalter følgende kategorier og typer personopplysninger på vegne av behandlingsansvarlig:

- Se vedlegg pr enkeltprosjekt i TSD knyttet til denne avtalen under bilag 1.

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.

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 på forespørsel.

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

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.

I TSD er følgende sikkerhetstiltak til implementert (listen er ikke uttømmende):

- All tilgang er underlagt 2-faktor autentisering
- Alle autentiserte brukere skal være godkjent av behandlingsansvarlig ved prosjektets leder Admin-tilgang på maskiner gis ikke til sluttbrukere
- Admin-tilgang til system-administratorer gir ikke tilgang til data
- Antallet system-administratorer holdes på et minimum
- Antallet administratorer av lagringen holdes på et minimum

22.04.2021

- Alle forskningsprosjekt er skilt fra hverandre ved hjelp av VLAN separasjon
- Årlig oppdatering av Risiko og Sårbarhetsanalyse (FHI informeres om oppdateringene i faste tertialmøter, ref Tjenesteavtalen punkt 6)
- Helautomatisert brannmurskonfigurasjon for å unngå menneskelige feil
- Utstrakt logging og overvåkning
- Ingen åpninger mot internett fra prosjektområdene unntatt svært kontrollert eksport og import av data
- Import og eksport av data er regelstyrt pr bruker
- Jevnlig penetrasjonstesting
- Tilgang til TSD gis gjennom krypterte remote-desktop-løsninger der all lokal tilknytning til sentrale maskiner er skrudd av
- Prosjektområdene låses når forskningsløyve går ut på dato
- Backup og snapshots tas hver natt

Se ellers: https://www.uio.no/english/services/it/research/sensitive-data/about/index.html

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 etter forvaltningsloven (Lov 10. februar 1967) § 13, 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.

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.

22.04.2021

9. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ugrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd.

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 Datatilsynet blir varslet når dette er påkrevd. Databehandler skal yte rimelig bistand til at behandlingsansvarlig kan oppfylle sine forpliktelser til å gi utfyllende informasjon til Datatilsynet og de registrerte, og å svare på spørsmål.

10. Underleverandører

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

- Uninett
- Unit
- DigDir – eSignering
-

Endringer i bruk av underleverandører etter inngåelse av denne avtale legges inn i bilag 2 med signert godkjenning fra behandlingsansvarlig.

11. Overføring til land utenfor EU/EØS og/eller internasjonale organisasjoner

Databehandler overfører ingen personopplysninger til land utenfor EU/EØS og/eller internasjonale organisasjoner.

Behandlingsansvarlig kan gjennom bruk av TSD instruere databehandler til å tilgjengeliggjøre personopplysninger til tredjeland og/eller internasjonale organisasjoner.

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.

22.04.2021

Databehandler skal dokumentere sikkerhetsrevisjonene. Behandlingsansvarlig skal gis tilgang til revisjonsrapportene på forespørsel (FHI informeres om rapportene i faste tertialmøter, ref Tjenesteavtalen punkt 6).

Behandlingsansvarlig kan gjennomføre sikkerhetsrevisjoner hos Databehandler, av informasjonssikkerhetssystemet og tilhørende fasiliteter som benyttes av Databehandler eller godkjente underleverandører for behandling av personopplysninger på vegne av den Behandlingsansvarlige. Databehandler skal bistå Behandlingsansvarlig med nødvendig informasjon dersom behandling i TSD medfører at Behandlingsansvarlig har plikt til å utrede personvernkonsekvenser før behandling av personopplysninger i TSD settes i gang (DPIA), jf. personvernforordningen artikkel 35 og 36.

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.

Hver av Partene dekker sine egne kostnader forbundet med revisjon.

13. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å slette alle data inkludert personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til denne avtalen.

For hvert enkelt prosjekt i TSD vil prosjekteiere hos behandlingsansvarlig motta beskjed fra databehandler når sluttdato eller oppbevaringsdato for et prosjekt nærmer seg, med anmodning om å slette data. Sletting av data tilhørende et prosjekt skjer 30 dager etter oppbevaringsdato som settes ved prosjektopprettelse, med mindre databehandler mottar dokumenterte instrukser om at personopplysningene skal lagres ut over opprinnelig fastsatt dato.

Behandlingsansvarlig kan selv hente ut sine data av TSD innen utløpet av en prosjektperiode. Hvis data ikke hentes ut og/eller slettes innen 30 dager etter oppbevaringsdato for et prosjekt, godtar behandlingsansvarlig at alle data databehandler forvalter på vegne av behandlingsansvarlig i prosjektet blir slettet av databehandler.

Sikkerhetskopier vil oppbevares i 90 dager etter sletting.

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

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 13 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 10 ovenfor.

22.04.2021

15. Avtalens varighet

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

Avtalen kan sies opp av begge parter med en gjensidig frist på 6mnd.

16. Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er: Gard Thomassen, tsd-drift@usit.uio.no / 22840934/ 93674926.

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er: Ole Trygve Stigen, Ole.Trygve.Stigen@fhi.no / 41242604.

17. 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 norske domstoler.

***

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)
Ole Trygve Stigen	Lars Oftedal
Fagdirektør	IT-direktør
Folkehelseinstituttet	Universitetet i Oslo

22.04.2021

Bilag 1 – Databehandlinger

Vedlegg nr. _____

Vedlegg til Databehandleravtale for prosjekter der organisasjonen er knyttet til USIT/TSD med en overordnet databehandleravtale.

Prosjektnavn
[oppgis]
Prosjektleder
(navn, kontaktinformasjon) [oppgis]
Forskningsansvarlig person
[oppgis]
Prosjektadministrator
(den som registrerer prosjektet i TSD, og er prosjektets koordinator for bruk av TSD) [oppgis]
Prosjektadministrator e-post
[oppgis]
Prosjektadministrator telefon
[oppgis]
Formell referanse til prosjektet
(Institusjonens saksnummer for prosjektets hjemmel) [oppgis om det finnes]
Internt saksnummer
(Institusjonens saksnummer for prosjektets hjemmel
REK-nr / NSD godkjenning:
Personvernombud:
Type personopplysninger:
Direkte identifiserbart?:
Indirekte identifiserbart?:
Overføring utenfor EØS/EU eller internasjonale organisasjoner:
Navn og institusjon på prosjektets registrerte medlemmer (brukere) utenfor EØS/EU og i internasjonale organisasjoner som skal ha tilgang til TSD.
Sluttdato for prosjektet
(maksimal varighet på lagring må samsvare med sluttdato for REK/personvernombud godkjenning) [oppgis]
Informasjon inkludert tilhørende linker bekreftes lest og forstått ved signatur på dette dokumentet
USIT vil ikke under noen omstendigheter levere ut data fra prosjektet til andre enn prosjektets registrerte medlemmer (brukere). USIT må forsikre seg om at REK-vedtak foreligger. Prosjektets registrerte medlemmer (brukere) er de eneste som vil kunne behandle data i henhold til tillatelser fra Prosjektleder.

Prosjektleder kan kun gi brukere tilgang i samsvar med REK-søknad og godkjenningen hos behandlingsansvarlig institusjon. Prosjektleder skal påse at ingen andre av prosjektets registrerte medlemmer (brukere) enn Prosjektleder og eventuelt data manager ansatt ved FHI som Prosjektleder har utpekt, har rettigheter til å eksportere data ut fra TSD. Dersom Prosjektleder gir prosjektets registrerte medlemmer (brukere) utenfor EØS/EU og i internasjonale organisasjoner tilgang til TSD, skal Prosjektleder sørge for at det foreligger et overføringsgrunnlag etter GDPR.

Prosjektleder er ansvarlig for at man benytter direkte identifiserbare data så lite som overhodet mulig inne i TSD, iht. dataminimeringsprinsippet. Ved bruk av Nettskjema + minID/BankID skal personnummer vaskes bort og koblingsnøkkel lagres slik at den er tilgjengelig for så få prosjektdeltakere som mulig. Ved ferdigstilt inklusjon av forskningsobjekt, bør koblingsnøkkel vurderes fjernet fra prosjektet og eventuelt arkivert i TSD uten prosjektets direkte tilgang.

Prosjektleder bekrefter med dette at avtaleskrivet om lagring av forskningsdata i TSD er lest og forstått.

Dato :

Signatur prosjektleder : _____

for forskningsansvarlig
(Nivå 2- eller Nivå 3 -leder (signatur) : _____

(blokkbokstaver) : _____

Bilag 2 – Underleverandører

Følgende endringer i bruk av underleverandører er godkjent av behandlingsansvarlig:

Leverandør navn	Fra og med dato	Sluttdato

Dato : _____

På vegne av behandlingsansvarlig

Signatur : _____

(blokkbokstaver) : _____