Databehandleravtale for bruk av 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

Klinisk Institutt 2, Universitetet i Bergen, v prosjekt: **2017/2496 Genetiske faktorer assosiert med feberkramper i barn**

(behandlingsansvarlig)

og

TSD, USIT, Universitetet i Oslo

(databehandler)

13.11.2018

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 systemet Tjenester for Sensitive Data (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.

2. Formålsbegrensning

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er å muliggjøre databehandlingsansvarliges lagring og bruk av dataene i TSD.

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.

Klinisk Institutt 2, forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning 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.

Databehandler forplikter seg til å benytte TSD-eInfrastrukturen og dets tjenester kun slik de har hjemmel til i forbindelse med sin pågående forskning / kliniske virksomhet / kommersielle virksomhet. Herunder ligger også å forholde seg til minimaliseringsprinsippet med tanke på tilgang til, og bruk av personopplysninger.

TSD er en forsknings-eInfrastruktur og fremstår som en slags skytjeneste for sluttbruker (databehandlingsansvarlig). TSD tilbyr et tomt (mtp data) arbeidsrom for forskningsmiljøer der de kan arbeide med data som tilhører et avgrenset forskningsprosjekt. Ingen ved TSD vil benytte databehandlingsansvarliges data til noen formål, og vil i de aller fleste tilfeller ikke en gang ha tilgang til å lese dataene. Unntak vil være når databehandlingsansvarlig eksplisitt ber databehandler om spesiell hjelp ved feilsøking eller lignende.

4. Opplysningstyper og registrerte

Databehandleren forvalter følgende personopplysninger på vegne av behandlingsansvarlig:

Data fra prosjektet : 2017/2496 Genetiske faktorer assosiert med feberkramper i barn

- GWAS-data og spørsmålsdata fra den Norske Mor og Barn undersøkelsen (MoBa) samt data fra Medisinsk fødselsregister (forhold i svangerskapet, svangerskapstermin, morkakevekt, fødselsvekt, fødselslengde, Apgar-score, komplikasjoner) og Norsk pasientregister (feberkramper).

Personopplysningene gjelder følgende registrerte:

Deltakere i MoBa studien

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 forskningsprosjektets leder / TSD
- 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
- Alle forskningsprosjekt er skilt fra hverandre ved hjelp av VLAN separasjon
- Årlig oppdatering av Risiko og Sårbarhetsanalyse
- 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 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.

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.

10. Underleverandører

Ingen underleverandører benyttes i TSD. Skulle dette bli aktuelt vil behandlingsansvarlig kontaktes.

11. Overføring til land utenfor EU/EØS

- Databehandler vil selv aldri overføre data til land utenfor EU/EØS
- Databehandlingsansvarlig kan gi tilgang til data i TSD til utenlandske borgere ved at prosjektleder for forskningsprosjektet autentiserer brukeren(e). Det forutsettes at prosjektleder har behandlingsgrunnlag for utlevering.

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.

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.

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. Behandlingsansvarlig kan selv hente sine data ut av TSD innen utløpet av den gyldige periode for (i de tilfeller behandlingen er tidsbestemt av REK/NSD/Personvernsombud eller andre bestemmelser) tillattdatabehandling i TSD. Behandlingsansvarlig må da ha hjemmel for sine handlinger. Tilgang til TSD lukkes automatisk for databehandlingsansvarlig når tidsrammen for prosjektet løper ut. Denne kan utvides ved dokumentert hjemmel for forlengelsen.

Sletting skal skje ved at databehandler sletter de av behandlingsansvarlige angitte data, eller samtlige data innen (30) dager etter avtalens opphør. Sikkerhetskopier slettes automatisk 90 dager etter rådata slettes. Sikkerhetskopier vil ikke være tilgjengelig for andre enn et fåtall systemadministratorer i perioden. Sletting gjøres etter avtale med databehandlingsansvarlig, eller om databehandler ikke får tak i databehandlingsansvarlig.

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.

15. Avtalens varighet

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

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: Stefan Johansson, stefan.johansson@uib.no / 40855779

17b. 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.

(Dette punktet gjelder når databehandlingsansvarlig er et annet statlig universitet eller høyskole.)

***

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

Bergen 14/11-18 Sted og dato Oslo 3/12-18

På vegne av behandlingsansvarlig

.....

(underskrift)

På vegne av databehandler

.....

(underskrift)

Lars Oftedal
IT-direktør
Universitetet i Oslo