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

Oslo Universitetssykehus HF v/Kreftregisteret

(behandlingsansvarlig)

og

TSD, USIT, Universitetet i Oslo

(databehandler)

06.12.2018

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 dataminimeringsprinsippet 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. Tilgang til dataene vil kun være nødvendig for lagringsadministratorene, eller ved feilsøking eksplisitt ønsket av databehandlingsansvarlig.

4. Opplysningstyper og registrerte

Databehandleren forvalter følgende personopplysninger på vegne av behandlingsansvarlig:

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

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.

06.12.2018

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.

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er:
Trine B Rounge

17a. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar (fyll inn navn på tingrett) som verneting. Dette gjelder også etter opphør av avtalen.

(Dette punktet gjelder når databehandlingsansvarlig er en privat aktør.)

***

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

Sted og dato

På vegne av behandlingsansvarlig

..... (underskrift)

På vegne av databehandler

..... (underskrift)

06.12.2018