Databehandleravtale for TSD mellom IT-avdelingen og Diakonhjemmet Sykehus

Dokumentet er signert digitalt av følgende undertegnere:

- LARS INGE OFTEDAL, signert 08.05.2023 med ID-Porten: BankID

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

mellom

Diakonhjemmet Sykehus

(behandlingsansvarlig)

og

TSD ved IT-avdelingen, Universitetet i Oslo (Org. Nr. 971 035 854)

(databehandler)

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 (heretter «GJELDENDE PERSONOPPLYSNINGSLOVGIVNING»).

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 Tjenesteavtalen inngått mellom behandlingsansvarlig og databehandler i forbindelse med bruk av og behandling i TSD, når det gjelder forhold spesifikt knyttet til behandling av personopplysninger.

Denne avtalen sammen med Tjenesteavtalen fungerer som en overordnet avtale mellom behandlingsansvarlig institusjon og databehandler.

2. Behandlingens hensikt og formål

Hensikten med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er å tilby TSD med integrerte løsninger slik tjenesten er beskrevet i Tjenesteavtalen, slik at behandlingsansvarlig kan oppfylle formål innenfor innsamling, lagring, bearbeidelse, analyse og samarbeid av data.

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 benytte underleverandører uten at dette på forhånd er godkjent av behandlingsansvarlig, jf. punkt 10 i denne avtalen.

3. Instrukser

Databehandler skal bare behandle personopplysninger i tråd med behandlingsansvarliges dokumenterte instrukser og i henhold til gjeldende personopplysningslovgivning. Hvis annen behandling er nødvendig for å oppfylle forpliktelser som databehandler er underlagt i henhold til gjeldende rett, skal databehandleren underrette den behandlingsansvarlige så langt dette er tillat ved lov.

Behandlingsansvarlig forplikter seg til å overholde alle plikter i henhold til gjeldende personopplysningslovgivning som gjelder ved bruk av TSD til behandling av personopplysninger. Herunder at behandlingen er formålsbestemt og basert på et gyldig rettsgrunnlag.

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

4. Opplysningstyper og registrerte

Databehandleren forvalter følgende personopplysninger på vegne av behandlingsansvarlig:

- Kontaktopplysninger, slik som:
    - Kontaktopplysninger for representant hos behandlingsansvarlig, herunder:
        - Fullt navn
        - E-post
        - Telefonnummer
    - Innloggingsdetaljer ved bruk av FEIDE-innlogging

- Opplysningstyper som kan være både direkte og indirekte identifiserbare alminnelige og særlige kategorier av personopplysninger, herunder opplysninger om helse, som behandlingsansvarlig ved bruk av TSD lagrer og behandler i tjenesten. Nærmere spesifikasjon angis ved prosjektopprettelse.

- I forbindelse med innlogging ved bruk av ID-porten behandles følgende opplysninger:
    - Personnummer
    - Innloggingsdetaljer

Digitaliseringsdirektoratet er behandlingsansvarlig for personopplysninger som behandles i felles innlogging til offentlige tjenester (ID-porten).

- Personnummer behandles som identifikator så lenge en bruker av TSD har et aktivt prosjekt for sikker identifikasjon og adgangskontroll

TSD behandler enkelte opplysninger for fakturering, systemsikkerhet, tjenestekvalitet, oppetid og feilsøking. Opplysninger knyttes til prosjektdeltagere og omfatter:

- Faktureringsopplysninger
- IP-adresse
- Opplysninger om maskinvare
- Tidsbruk
- Inn- og utloggingsdetaljer
- Hvilke tjenester som brukes
- Når tjenester brukes

Universitetet i Oslo er behandlingsansvarlig for behandling for identifikasjon, adgangskontroll, fakturering, systemsikkerhet, tjenestekvalitet, oppetid og feilsøking.

Se TSD sin personvernerklæring tilgjengelig på:
https://www.uio.no/tjenester/it/forskning/sensitiv/mer-om/personvernerklering.html

5. De registrertes rettigheter

Databehandler skal på forespørsel bistå behandlingsansvarlig med oppfyllelse av den registrertes rettigheter i henhold til gjeldende personopplysningslovgivning. Plikten til å bistå gjelder bare i den utstrekning dette er mulig og hensiktsmessig sett hen til karakteren og omfanget av behandlingen av personopplysninger etter Tjenesteavtalen.

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.

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.

Sikkerhetstiltak implementert i TSD er, blant annet:

- All tilgang er underlagt 2-faktor autentisering
- 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
- Årlig oppdatering av Risiko og Sårbarhetsanalyse
- Helautomatisert brannmurskonfigurasjon for å unngå menneskelige feil
- Utstrakt logging
- Jevnlig penetrasjonstesting
- Tilgang til TSD gis gjennom krypterte remote-desktop-løsninger der all lokal tilknytning til sentrale maskiner er skrudd av
- Ingen åpninger mot internett fra prosjektområdene unntatt svært kontrollert eksport og import av data
- Import og eksport av data er regelstyrt pr bruker
- Prosjektområdene låses når nødvendig godkjenning går ut på dato
- Backup og snapshots tas hver natt

Ytterligere informasjon er tilgjengelig på TSDs nettsider:
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.

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. Universitetet i Oslo er underlagt offentleglova (Lov 19.05.2006 nr. 16) sine bestemmelser om offentlig innsyn.

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 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.

Databehandler skal bistå behandlingsansvarlig med nødvendig informasjon dersom bruk av TSD medfører at behandlingsansvarlig har plikt til å utrede personvernkonsekvenser før behandlingen settes i gang, jf. forordning (EU) 2016/679 av 27. april 2016, Artikkel 35 og 36.

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. 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. Underdatabehandler

Databehandler plikter å ha egne avtaler med underdatabehandlere som regulerer underdatabehandlerenes forvaltning av personopplysninger i forbindelse med denne avtalen.

I avtaler mellom databehandler og underdatabehandler skal underdatabehandler pålegges å ivareta alle plikter som databehandleren selv er underlagt i henhold til denne avtalen og lovverket for den delegerte behadnlingsaktiviteten.

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.

Behandlingsansvarlig godkjenner at databehandler engasjerer underleverandører for å oppfylle denne avtalen. Oppdatert liste over underleverandører foreligger til en hver tid på

https://www.uio.no/tjenester/it/forskning/sensitiv/tilgang/leverandorer/index.html

Behandlingsansvarlig vil varsles tilsvarende oppsigelsesfristen i Tjenesteavtalen når det tas i bruk nye underdatabehandlere.

Dersom underdatabehandleren ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, skal databehandleren overfor den behandlingsansvarlige ha ansvar på samme måte som om databehandler selv sto for behandlingen.

11. Overføring til land utenfor EU/EØS (tredjeland) og 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 overføre personopplysninger til tredjeland og/eller internasjonale organisasjoner, eller selv bruke TSD til å overføre personopplysninger til tredjeland eller internasjonale organisasjoner. Behandlingsansvarlig garanterer ved instruks om overføring og/eller overføring ved bruk av TSD at det foreligger nødvendige garantier for et tilstrekkelig beskyttelsesnivå for personvern i henhold til gjeldende personvernregler, herunder at det foreligger en lovlig overføringsmekanisme og at det foreligger nødvendige tekniske, organisatoriske og/eller juridiske ekstratiltak.

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.

Behandlingsansvarlig kan gjennomføre sikkerhetsrevisjoner hos Databehandler, av informasjonssikkerhetssystemet og tilhørende fasiliteter som benyttes av Databehandler. 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.

Ved bruk av den integrerte tjenesten Nettskjema gjennom TSD vil personopplysninger som epost (for purring / oppfølgning) slettes når det gjeldende Nettskjema ikke lenger er aktivt. Det ryddes halvårlig blant skjema som er åpne, men som burde vært lukket av behandlingsansvarlig.

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.

15. Erstatning

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.

Samlet erstatning per kalenderår er begrenset til et beløp som tilsvarer Tjenesteavtalens samlede årlige vederlag ekskl. merverdiavgift.

16. Avtalens varighet

Avtalen gjelder så lenge databehandler forvalter personopplysninger på vegne av behandlingsansvarlig i henhold til Tjenesteavtalen.

17. Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er:

Gard Thomassen, gardot@usit.uio.no, +47 93674926

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er:

Arild Hagesveen, arild.hagesveen@diakonsyk.no, +47 95792519

18 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 slik dette er bestemt i Tjenesteavtalen.

***

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

Oslo 2/5-23 Sted og dato

På vegne av behandlingsansvarlig	På vegne av databehandler
.....	.....
Navn: Arild Hagesveen	Navn: Lars Oftedal
Tittel: Fungerende fagdirektør	Tittel: IT-direktør
Virksomhet: Diakonhjemmet Sykehus	Virksomhet: Universitetet i Oslo