FHI

Folkehelseinstituttet

Databehandleravtale

mellom

Folkehelseinstituttet

(Dataansvarlig)

og

Universitetssykehuset Nord-Norge HF (UNN)
(Databehandler)

om

innsamling og behandling av opplysninger i Norsk overvåkingssystem for antibiotikaresistens hos mikrober (NORM)

1. Avtalens parter

1. Dataansvarlig: Folkehelseinstituttet, org. nr. 983 744 516, Lovisenberggata 8, 0456 Oslo.
2. Databehandler: Universitetssykehuset Nord-Norge HF (UNN), org. nr. 983 974 899, Sykehusvegen 38, 9038 Tromsø

Hver for seg omtalt som «Dataansvarlig», «Databehandler» eller «parten», og i fellesskap omtalt som «partene».

2. Avtalens hensikt

Avtalens hensikt er å sikre at partene oppfyller plikter etter personopplysningsloven (lov om behandling av personopplysninger av 15. juni 2018 nr. 38) slik den gjelder til enhver tid med GDPR (EUs personvernforordning 2016/679 av 27. april 2016) implementert, og tilhørende forskrifter (heretter benevnt *Personvernlovgivningen*), helseregisterloven (lov om helseregistre og behandling av helseopplysninger av 20. juni 2014 nr. 43) og resistensregisterforskriften (forskrift av 14. november 2003 nr. 1353 om innsamling og behandling av helseopplysninger i Norsk overvåkningssystem for resistens hos bakterier, sopp og virus).

Avtalen regulerer Databehandlers behandling av personopplysninger på vegne av den Dataansvarlige. Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

3. Definisjoner

Dataansvarlig: en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, jf. helseregisterloven § 2 bokstav d.

Databehandler: en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den Dataansvarlige, jf. GDPR art. 4 nr. 8.

NORM: Norsk overvåkingssystem for resistens mot legemidler brukt til behandling av infeksjoner med bakterier (antibiotika) og sopp (antimykotika), jf. resistensregisterforskriften § 1-1.

Personopplysning: enhver opplysning om en identifisert eller identifiserbar fysisk person. En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet, jf. GDPR art. 4 nr. 1.

Særlig **kategori av personopplysninger**: personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, jf. GDPR art. 9 nr. 1.

Behandling av personopplysninger: enhver bruk av personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring,

gjenfinning, oppslag, bruk, analyse, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring, GDPR art. 4 nr. 2.

Tredjepart: enhver annen fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ enn den registrerte, den Dataansvarlige, Databehandleren og de personer som under den Dataansvarlige eller Databehandlerens direkte myndighet har fullmakt til å behandle personopplysninger, også selskap innen samme konsern, jf. GDPR art. 4 nr. 10.

Den registrerte: identifisert eller identifiserbar fysisk person som personopplysningen(e) kan knyttes til, jf. GDPR art. 4 nr. 1.

4. Avtalens formål og rammer (instruks)

Avtalens formål er i henhold til resistensregisterforskriften § 1-6 å regulere innsamling og behandling av opplysninger i NORM mellom databehandler og dataansvarlig. Avtalen omfatter også overvåkning og forskning, jf. resistensregisterforskriften § 1-3, drift og kvalitetssikring av registeret, samt tilgjengeliggjøring av data til brukerne. Behandling av opplysninger i RAVN-registeret er ikke omfattet av denne Avtalen.

Avtalen skal omfatte og beskrive innsamling og behandling av opplysninger i NORM med hensyn til blant annet:

- Daglig drift av NORM, rapportering og formidling av resultater fra NORM
- Planlegging av aktiviteter i NORM
- Tilgjengeliggjøring av data i henhold til resistensregisterforskriften
- Partenes ansvar og plikter under avtaleforholdet
- Økonomistyring og finansiering inkludert rutiner for regnskap og revisjon

Databehandler kan ikke behandle helseopplysninger på annen måte enn det som er skriftlig avtalt med Dataansvarlig. Opplysningene kan heller ikke uten avtale overlates til noen andre for lagring eller bearbeidelse. Om slik avtale med underleverandør, se punkt 8.

- Typen personopplysninger som skal behandles, er indirekte identifiserbare og listet opp i resistensregisterforskriften § 1-7
- Alle personer som har avgitt prøve der det er påvist bakterie- eller soppisolat som er besluttet inkludert i NORM, blir registrert av medisinsk mikrobiologisk laboratorium eller referanselaboratorium som har resistensbestemt isolatet.
- Databehandler skal behandle opplysningene, f.eks. registrere, sammenstille, lagre, kvalitetssikre, tilgjengeliggjøre opplysninger i henhold til NORM sitt internkontrollsysten, jf. **vedlegg 1**

Databehandler skal omgående underrette Dataansvarlig dersom Databehandler mener at instruksen er i strid med Personvernlovgivningen.

5. Angivelse av behandlingsgrunnlag

Behandlingsgrunnlaget er GDPR art. 6 bokstav nr. 1 bokstav c og e, jf. art. 9 nr. 2 bokstav g og i. Supplerende rettsgrunnlag er gitt i følgende lover og forskrift:

resistensregisterforskriften, helseregisterloven *§ 9* og smittevernloven *§7-9*.

6. Dataansvarliges rolle og ansvar

Dataansvarlig bestemmer formålet med og rammene for behandlingen av personopplysningene og er blant annet ansvarlig for at:

- det foreligger et lovlig behandlingsgrunnlag for personopplysningene,
- Databehandler gis skriftlige instrukser for behandling av personopplysninger, jf. punkt 4, 7 og 8.
- Databehandler (UNN) foreta en vurdering av personvernkonsekvenser ved behov i henhold til GDPR artikkel 35, som godkjennes av dataansvarlig (FHI)
- varsle Datatilsynet ved brudd på personopplysningssikkerheten, ref. avtalens punkt 10.

Dataansvarlig skal påse at kravene er oppfylt i forbindelse med oppbevaring og bruk av personopplysningene hos Databehandleren, se nærmere punkt 7 og revisjon punkt 11.

7. Databehandlers plikter

Databehandler skal utføre sine oppgaver i tråd med de til enhver tid gjeldende lover og regler, og følge de rutiner og instrukser for databehandlingen som Dataansvarlig til enhver tid har bestemt skal gjelde.

Databehandler skal gjennomføre egnede lovpålagte tekniske og organisatoriske sikkerhetstiltak og plikter, og gi Dataansvarlig tilgang til sin sikkerhetsdokumentasjon.

Databehandler skal bistå, slik at Dataansvarlig kan ivareta sitt eget ansvar etter Personvernlovgivningen, jf. bla. GDPR artikkel 32 til 36.

Databehandleren skal bistå Dataansvarlig med å oppfylle vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter (f.eks. om innsyn, retting og sletting).

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.

I den grad Databehandler mottar anmodninger fra de registrerte selv, plikter Databehandleren, så snart som mulig, å varsle Dataansvarlig om slike anmodninger og å redegjøre for hvordan Databehandler vil følge dem opp.

Databehandler har ikke anledning til å overføre, eller inngå avtale om overføring, av personopplysningene som behandles på vegne av Dataansvarlig, til Tredjepart uten etter dokumentert instruks fra Dataansvarlig.

Dataansvarlig (Folkehelseinstituttet) har plikt til å utlevere (tilgjengeliggjøre) statistikk av avidentifiserte data fra NORM i henhold til forskriften § 3-1. Slik tilgjengeliggjøring er delegert til databehandler i medhold av denne avtalen, jf. punkt 15.

I den grad Databehandler er forpliktet til å overføre personopplysninger etter unionsretten eller nasjonal rett, ref. art. 28 nr. 3 bokstav a) plikter Databehandler å underrette Dataansvarlig skriftlig om slik utlevering før utlevering finner sted.

Dataansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til, informasjon om og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til denne avtalen, ref. helsepersonelloven § 21 flg. og forvaltningsloven § 13 flg., og skal sikre at kun personer som er autorisert, behandler personopplysninger og at personopplysninger som behandles for Dataansvarlig, holdes atskilt fra andre opplysninger og tjenester. Autorisasjon kan kun gis til personer som har forpliktet seg til å behandle personopplysninger fortrolig (taushetserklæring) eller er underlagt lovfestet taushetsplikt. Denne bestemmelsen gjelder også etter avtalens opphør.

Dersom Databehandler overtrer bestemmelsene i Personvernlovgivningen ved å fastsette formålene med og midlene for behandlingen, skal Databehandleren anses for å være dataansvarlig med hensyn til nevnte behandling, jf. GDPR art. 28 pkt. 10.

I tilfeller der det er behov for kontakt med Helse- og omsorgsdepartementet, Datatilsynet eller andre utenforstående etater om forhold som berører denne avtalen, håndteres dette ved direkte kontakt mellom Databehandler og de aktuelle etater. Dataansvarlig skal holdes løpende orientert om slik kontakt, og Dataansvarlig kan selv avgjøre om de vil delta aktivt i denne kontakten.

8. Bruk av underleverandør

Dersom Databehandler benytter seg av underleverandør, eller andre som ikke normalt er ansatt hos Databehandler, til å utføre behandling av personopplysninger som er omfattet av denne avtalen, skal det innhentes særlig eller generell skriftlig tillatelse fra Dataansvarlig før behandlingen av personopplysninger starter.

Databehandler er ansvarlig for utførelsen av behandlingsaktiviteter hos underleverandøren på samme måte som om Databehandler selv stod for utførelsen av disse. Det skal inngås skriftlig databehandleravtale mellom Databehandler og underleverandør som speiler Databehandlers plikter og ansvar etter denne avtalen, gjeldene underleverandøravtaler og kontaktpersoner jf. **vedlegg 2**.

Gjeldende underleverandøravtaler er:

1. Avtale om behandling av helse- og personopplysninger (databehandleravtale) mellom Universitetssykehuset Nord-Norge (databehandler hovedleverandør) og St. Olavs hospital (databehandler underleverandør)
2. Avtale mellom Universitetssykehuset Nord-Norge (databehandler hovedleverandør) og Helse Nord IKT

3. Avtale mellom St.Olav hospital (databehandler underleverandør) og Helse Midt-Norge IKT (Hemit)

Databehandler skal sikre at Dataansvarlig og tilsynsmyndighetene har samme rett til innsyn og kontroll med behandling av personopplysningene hos underleverandør som de har etter denne avtalen.

Samtlige som på vegne av Databehandler utfører oppdrag som innebærer behandling av de personopplysningene som er omfattet av denne avtalen, skal være kjent med Databehandlers avtalemessige og lovmessige forpliktelser og oppfylle kravene etter disse.

Databehandler er erstatningsansvarlig overfor Dataansvarlig for økonomiske tap som påføres Dataansvarlig og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandør.

9. Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter Personvernlovgivningen, helseregisterloven, herunder særlig §§ 21 og 22, og resistensregisterforskriften kapittel 4. I tillegg til de sikkerhetstiltak som Dataansvarlig ellers mener er nødvendig. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på Dataansvarliges forespørsel.

Databehandleren skal utarbeide sikkerhetsmål, -strategi, -organisering og redegjøre for roller og ansvar i samsvar med Personvernlovgivningen og nødvendig internkontrollsystem.

Databehandler skal også utarbeide risikovurdering av egen, og eventuelle underleverandørers informasjonssikkerhet, og forelegge den for Dataansvarlig på forespørsel.

Databehandler skal etter særskilt avtale bistå Dataansvarlig i dennes arbeid med gjennomføring av risikoanalyse og utarbeiding av sikkerhetsstrategi.

10. Avvik

Databehandleren skal umiddelbart varsle Dataansvarlig om avvik hvilket vil si en hendelse som har betydning for konfidensialitet, integritet eller tilgjengelighet av personopplysninger, som er av betydning for informasjonssikkerheten og den registrertes personvern, og så snart som mulig iverksette tiltak for å avhjelpe (lukke) avvikene og begrense skadevirkningene av dem.

Slike alvorlige avvik skal varsles til kontaktperson hos Dataansvarlig som angitt i punkt 22, både per e-post og telefon, med kopi til folkehelseinstituttet@fhi.no. Dataansvarliges Personvernombud skal også varsles, personvernombud@fhi.no.

Datainnbrudd og omfattende forsøk på datainnbrudd, distribusjon av personopplysninger til uautoriserte mottakere, tyveri og annet tap av lagringsmedier (uavhengig av om disse er kryptert eller ikke) skal alltid meldes til Dataansvarlig.

Dataansvarlig melder avviket til Datatilsynet innen 72 timer med mindre det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter. Dataansvarlig er ansvarlig for å varsle de registrerte.

Databehandler skal bistå Dataansvarlig med varsling til Datatilsynet og registrerte ved avvik.

11. Sikkerhetsrevisjoner

Databehandler plikter å gjennomføre sikkerhetsrevisjoner jevnlig. Databehandler skal dokumentere at de har gjennomført sikkerhetsrevisjoner og skal sende kopi av revisjonsrapporten til Dataansvarlig.

Dataansvarlig kan også selv gjennomføre sikkerhetsrevisjon hos Databehandler. Sikkerhetsrevisjonen kan omfatte gjennomgang av rutiner, stikkprøver, mer omfattende stedlige kontroller og andre egnede kontrolltiltak. Databehandler skal bistå Dataansvarlig ved gjennomføring av slike sikkerhetsrevisjoner i tråd med kravene i GDPR Art. 28 nr. 3 bokstav h).

12. Fagrådet for NORM

NORM skal organiseres i samsvar med resistensregisterforskriften og på en slik måte at den ivaretar interessene til både de deltagende laboratorier og brukerne av NORM-registeret. For å oppnå dette er det opprettet et fagråd for NORM. Fagrådet har til oppgave å gi råd til Databehandler og Dataansvarlig som kan sikre god faglig aktivitet i NORM i forståelse med det samlede medisinsk mikrobiologiske og infeksjonsmedisinske miljøet. Fagrådet har en rådgivende funksjon. Se **vedlegg 3** for nærmere beskrivelse av Fagrådet for NORM.

13. Drift og planlegging av aktiviteter i NORM

NORM skal drives i samsvar med resistensregisterforskriften for å oppfylle formålene med NORM, jf. resistensregisterforskriftens § 1-3. Fagrådet bistår NORM-sentralen med å finne fram til hvordan NORM-registeret best kan løse disse oppgavene jf. Fagrådets mandat.

14. Formidling av resultatene fra overvåkningen

Resultatene fra overvåkingen i NORM skal sammenfattes skriftlig og skal publiseres på nettstedet for NORM-registeret. Årlige oversikter skal inngå i en aktiv informasjonsstrategi og -plan rettet mot så vel helseforvaltningen, helsetjenesten og øvrige forvaltning, som mot aktører innen medisinsk forskning, helsetjenesteforskning og samfunnsforskning jf. resistensregisterforskriftens § 3-3, og til internasjonale samarbeidsorganer. Eksempelvis skal NORM tilrettelegge for rapportering av resistensdata fra norske medisinsk mikrobiologiske laboratorier til internasjonale overvåkingsprogram, herunder Det europeiske senter for forebygging av og kontroll med sykdommer (ECDC) sitt EARS-Net, og Verdens helseorganisasjon (WHO) sitt GLASS-overvåkingssystem, jf. resistensregisterforskriften § 2-5.

Dataansvarlig og Databehandler er gjensidig forpliktet til å samordne informasjonsarbeidet vedrørende antibiotikaresistens der dette måtte være naturlig.

15. Tilgjengeliggjøring av data til statistikk og forskning m.v.

Databehandler skal på vegne av Dataansvarlig på forespørsel tilgjengeliggjøre statistikk fra NORM innen 30 dager fra den dagen forespørselen kom inn og etter søknad tilgjengeliggjøre avidentifiserte data fra NORM, dersom opplysningene skal brukes til et uttrykkelig angitt formål innen registerets formål, jf. resistensregisterforskriften § 3-1.

Databehandler skal holde oversikt over søknader om data og utlevering av statistikk og avidentifiserte data, og redegjøre for dette i den årlige driftsrapporten for NORM-registeret.

16. Finansiering

Hver av Partene dekker sine utgifter i forbindelse med sine arbeidsoppgaver, og står ansvarlig for egen regnskapsføring.

17. Rapportering

Databehandler skal innen 31. januar hvert år avgi driftsrapport til Dataansvarlig etter mal fra Dataansvarlig.

18. Avtalens varighet

Avtalens varighet er fem år fra signeringsdato.

19. Oppsigelse

Avtalen kan sies opp skriftlig av begge parter med en gjensidig oppsigelsesfrist på to (2) år. Uenighet mellom Dataansvarlig og Databehandler avgjøres av Helse- og omsorgsdepartementet.

20. Mislighold

Hver av partene kan si opp avtalen med øyeblikkelig virkning med skriftlig varsel til den andre dersom den ene parten misligholder en bestemmelse i avtalen, og misligholdet ikke rettes opp innen 30 dager etter mottak av skriftlig varsel som spesifiserer misligholdet og krever at det rettes opp.

Dataansvarlig kan kreve erstatning for økonomisk tap som feil eller forsømmelser fra Databehandlers side har påført Dataansvarlig, inkludert mislighold av vilkårene i denne avtalen.

21. Ved opphør

Ved opphør av denne avtalen plikter Databehandler å tilbakelevere alle personopplysninger som behandles på vegne av Dataansvarlig. Dette gjelder også for eventuelle sikkerhetskopier. Databehandler skal tilbakelevere personopplysninger innen rimelig tid etter avtalens opphør og skal skriftlig bekrefte dette overfor Dataansvarlig.

22. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til:

Hos Dataansvarlig (FHI):
Karianne Johansen
Adresse: Postboks 222 Skøyen, 0213 Oslo
E-postadresse:
Karianne.Johansen@fhi.no
Telefon: 97 49 80 04

Hos Databehandler (UNN):
Gunnar Skov Simonsen
UNN, Postboks 100, 9038 Tromsø
Gunnar.Skov.Simonsen@unn.no
91 84 86 80

23. Lovvalg og verneting

Tvist i forbindelse med denne avtalen skal søkes løst ved forhandlinger mellom partene. Fører ikke slike forhandlinger frem, skal saken bringes inn for fagdepartement til avgjørelse. Partene forplikter seg til å rette seg etter departementets avgjørelse.

Dersom en tvist ikke avgjøres ved behandling i fagdepartementene, skal den være underlagt norsk rett og partene velger Oslo tingrett som verneting. Dette gjelder også etter opphør av avtalen.

24. Signaturer

Denne avtalen er i to – 2 – eksemplarer, hvorav partene beholder hvert sitt.

Sted og dato
Oslo 8/3-21

Gun Peggy Strømstad Knudsen
Fungerende direktør for
Område smittevern, miljø og helse
Folkehelseinstituttet

Anita Schumacher
Direktør
UNN HF

Vedlegg 1: Kvalitetsdokumenter og internkontrollsystem hos Databehandler vedlagt kopi.

Vedlegg 2: Underleverandøravtaler:

- Databehandleravtalen mellom UNN (databehandler) og St. Olavs Hospital (databehandler underleverandør),
- Driftsavtalen mellom St. Olav Hospital (databehandler underleverandør) og Helse Midt-Norge IKT,
- Driftsavtalen mellom UNN (databehandler) og Helse-Nord IKT og Tjenesteavtale for NORM mellom UNN (databehandler) og Helse-Nord IKT

Vedlegg 3: Mandat for Fagrådet for NORM