

Personvernkonsekvensvurdering (DPIA)

Prosjektopplysninger

Prosjekttittel:
Helseundersøkelsen i Trøndelag
Prosjektleder:
<i>Prosjektleder har ansvaret for at personvern- og informasjonssikkerhetsmessige forhold ivaretas i prosjektet.</i>
Marit Næss, som leder for HUNT forskningscenter
Prosjektets tilhørighet:
<i>Institutt, enhet, helseforetak.</i>
Institutt for samfunnsmedisin og sykepleie, Fakultet for medisin og helsevitenskap, NTNU
Forskningsansvarlig/behandlingsansvarlig¹:
<i>Instituttleder er forskningsansvarlig/behandlingsansvarlig for alle prosjekter på instituttet.</i>
Solveig Kirsti Grudt
Finansiering av prosjektet:
NTNU, Helse- og omsorgsdepartementet, Helse Midt-Norge, Trøndelag fylkeskommune
Prosjektopplysninger
<i>REK-nummer og prosjektperiode (varighet på prosjektet).</i>
Datainnsamling og lagring er hjemlet av Forskrift for befolkningsbaserte helseundersøkelser.
Innsamlede helseopplysninger og humant biologisk materiale kan oppbevares på ubegrenset tid, med mindre annet følger samtykket eller formålet med innsamlingen (§ 4-7 og § 5-3, Forskrift for befolkningsbaserte undersøkelser)

1. Behandling av personopplysninger i prosjektet

1.1 Formålet med behandlingen av personopplysninger

Presenter prosjektet og forklar hvorfor du skal samle inn og analysere personopplysninger. Formålene med bruken av personopplysningene skal være spesifikke, uttrykkelig angitte og berettigede. For forskning innebærer det at det må formuleres konkrete forskningsspørsmål som skal besvares gjennom bruken av opplysningene.

Helseundersøkelsen i Trøndelag (HUNT) behandler personopplysninger for å kunne levere data til forskning og kvalitetssikring av helsetjensten. Formålet med HUNT er å legge til rette for utvikling av kunnskap om årsaker til sykdom og helse i et folkehelseperspektiv og derav bidra til bedre folkehelse. Kombinasjonen av innsamlet data og biologisk materiale gir mulighet til å studere samspillet mellom genetisk og biologisk variasjon, livsstil og miljøpåvirkning som alle har betydning for helse og sykdomsutvikling.

1.2 Datakilder

Kryss av for om det skal innhentes nye personopplysninger (egen datainnsamling) og/eller allerede registrerte opplysninger, og spesifiser i feltet under.

¹ Helseforskning bruker begrepet forskningsansvarlig. Øvrig forskning bruker begrepet behandlingsansvarlig.

- Egen datainnsamling (prosjektet vil innhente direkte fra den opplysning(e) gjelder)
- Sentrale helseregistre
- Helseundersøkelser (eksisterende)
- Kvalitetsregistre
- Pasientjournal
- Folkeregisteret
- SSB
- Internett
- Annet

Spesifisering av datakildene det er krysset av for, og beskriv kobling dersom dette er relevant:

HUNT forskningssenter utvider stadig dataomfanget for deltagere fra Trøndelag, enten ved nye analyser av biologisk materiale, oppfølgingsstudier eller nye hovedundersøkelser. I HUNT1 var det ikke krav om informert samtykke; ellers har deltagere i senere HUNT og oppfølgingsstudier gitt bredt, informert samtykke til innsamling, lagring og forskning på data. Samtykket inkluderer kobling til navngitte nasjonale registre og lokale diagnoseregistre fra primær- og andrelinjetjenesten. Reseptregisteret, fra 2022 Legemiddelregisteret, var ikke eksplisitt nevnt i HUNT2 da det ble opprettet i 2004. Personvernemda har siden godtatt koblinger til dette registeret også for deltagere i HUNT2. Folkeregisteret leverer personopplysninger for invitasjoner til og informasjon til deltagerne, dette inkluderer også registerstatus som bosatt i fylket, utflyttet, død eller i live.

1.3 Registrerte

Registrerte er den/de opplysningene gjelder, ofte kalt prosjektdeltakere.

Kryss av for hvilke kategorier av registrerte det skal behandles opplysninger om:

- Elever/studenter/barnehagebarn
- Pasienter/klienter/brukere
- Barn, spesifiser aldersgrupper
 - 0-13
 - 13-16
 - 16-18
- Pårørende
- Etniske minoriteter
- Avdøde
- Annet (spesifiser under)

Beskriv utvalget, eventuelt underutvalg, og antall:

HUNT har invitert deltagere i alderen 19 år og eldre i tidligere Nord-Trøndelag (HUNT1-4, n=95,000). UngHUNT har invitert alle ungdommer i alderen 13-19 år på bakgrunn av klasselister i skoler (n=10,000). Under HUNT4 ble også tidligere Sør-Trøndelag inkludert, og alle 18 år og eldre ble invitert (n=256.000). Utvalg ble selektert til ulike tilleggsprosjekt basert på rapporterte symptomer, sykdom, medisinbruk eller tilhørighet til definerte tilfeldige utvalg. Prosjektet HUNT4 70+ innhentet i tillegg helse og funksjonsdata fra pårørende for personer med nedsatte kognitiv funksjon. Data i HUNT databank oppbevares på ubestemt tid,

forskning tillates inkludere også tidligere data for avdøde personer. Planlagt forskning, utvalg og aktuelle koblinger til andre register gjennomføres i henhold til godkjenning fra REK, HUNT og andre registreiere.

1.4 Kategorier av personopplysninger

Kryss av for hvilke kategorier personopplysninger som vil behandles i prosjektet.

Kategorier av personopplysninger

- Navn
- Adresse
- Fødselsdato
- Fødselsnummer (11 siffer)
- Andre opplysninger, for eksempel telefonnummer, e-postadresse, IP-adresse, demografiske variabler, sosioøkonomi (utdanning, inntekt og yrke), familiestatus

Særlige kategorier av personopplysninger (tidligere kalt sensitive opplysninger)

- Rasemessig eller etnisk bakgrunn
- Politisk, filosofisk eller religiøs oppfatning
- At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- Seksuelle forhold
- Medlemskap i fagforeninger
- Biometri
- Helseforhold:
 - Diagnoser
 - Legemiddelbruk
 - Kognitive evner
 - Genetikk
 - Biologisk materiale
 - Annet, spesifiser under

Spesifisering av hvilke opplysninger og nivå på variabler:

Fødselsnummer brukes for å utlede biologisk kjønn og alder ved deltagelse, i tillegg til som grunnlag for koblingsbruer for prosjektspesifikke løpenummer som gis alle data som eksporteres fra HUNT databank. Ytterligere identifiserende opplysninger som navn, adresse og mobiltelefonnummer blir brukt til å informere deltagere eller invitere til nye studier.

Seksuelle forhold: HUNT4 inkluderte spørsmål om seksuell legning og seksuelliv.

Biometri: HUNT måler lengde, vekt, midjemål og flere andre biometriske parametere til helseforskning.

Helseforhold: HUNT har helseforskning som formål og flere spørsmål handler derav om helse og sykdom, diagnoser og bruk av medisiner. Kognitive tester inngår i HUNT4 70+. DNA blir ekstrahert fra alle deltakere som har avgitt blodprøve, og genetiske data utvinnes fra alle som ikke har reservert seg mot genetisk forskning.

Biologisk materiale vil benyttes til nye analyser der data vil bli lagret i HUNT databank

Andre helsedata som samles inn er f.eks. blodtrykkmåling, kondisjon, munnhelsestatus, hørsel, lungefunksjon, beintetthet, m.m.

1.5 Behandling av personopplysninger

Med «behandling» menes enhver bruk eller rekke av handlinger/aktiviteter som gjøres med personopplysninger. Kryss av for hva som skal gjøres med personopplysningene i prosjektet og eventuelt spesifiser. Databehandlingene må være i samsvar med det oppgitte formål.

- Innsamling
- Lagring
- Sammenstilling, kobling
- Analysering
- Utlevering ved overføring
- Tilgjengeliggjøring
- Gjenfinning (*for eksempel ved planlagt tilbakemelding til de registrerte*)
- Sletting, pseudonymiserte data
- Annen bruk (spesifiser under)

1.6 Lagringssted og lagringsmedier

Angi hvor og hvordan personopplysninger skal lagres og håndteres.

- Tjenester for Sensitive Data (TSD)
- Tilgangsbegrenset forskningsfilmappe på NTNUs filstruktur
- HEMIT/St. Olavs hospital
- Kryptert minnepinne
- Hunt Cloud
- Biobank, spesifiser:

Biologisk materiale lagres ved HUNT biobank (registreringsnummer 4094 i Biobankregisteret)

- Annet, spesifiser:

HUNT databank

Eventuelt spesifiser lagringen av personopplysningene:

HUNT databank oppbevarer alle data innhentet fra spørreskjema, intervju, målinger og analyser av biologisk materiale på en sikker server som er atskilt fra andre nettverk i og utenfor NTNU.

HUNT Cloud oppbevarer genetiske data og andre filer med store mengder data på en sikker server ved NTNU, med autorisert tilgang via en Cloud service.

Det er IT-avdelingen ved NTNU som har fått delegert ansvar for sikkerheten i infrastruktur for datalagring.

1.7 Dataansvarlig, datatilgang og databehandlere

1.7.1 Dataansvarlig og personer med datatilgang

Delegert dataansvarlig (instituttleder, på vegne av NTNU):

Solveig Kirsti Grudt (instituttleder ISM) på vegne av NTNU

Hvordan skal medarbeiderne få tilgang til data (oppgi gjerne navn på medarbeiderne og hvordan de skal behandle datamaterialet)?

Tilgang til HUNT databank er forbeholdt personer som jobber i databanken og IT-avdelingen. Pålogging krever passord, og tilgangen er begrenset til de områdene en ansatt har behov for, for å kunne utføre sitt arbeid. Alle ansatte ved HUNT forskningscenter har signert taushetserklæring.
Tilgang til biologisk materiale er forbeholdt ansatte ved HUNT biobank. Materialet lagres bak låste dører med kodetilgang.
HUNT Cloud i Trondheim er en sikker løsning for datalagring, og er ISO sertifisert av Nemko under ISO27001. (<https://www.ntnu.edu/documents/1267505933/1278525667/iso-27001-certificate-2017/85fdff66-9f58-4b5b-b355-b3506d4c66a0>). Lagringsplass ved HUNT Cloud er prosjektseparert og har adgangsbegrenset styring.

Dersom personopplysninger skal overføres eller på annen måte deles med ekstern institusjon, må punkt 1.7.2 fylles ut. (Unntak ved bruk av TSD eller liknende hvor eksterne ikke har mulighet for lokal lagring.)

1.7.2 Databehandler

En databehandler er en virksomhet som behandler personopplysninger på vegne av (etter instruks fra) en annen institusjon som er behandlingsansvarlig. Se mer info om hva en databehandleravtale er her:

<https://innsida.ntnu.no/wiki/-/wiki/Norsk/Databehandleravtale>

Skal prosjektet benytte en databehandler utenfor NTNU?

- Ja
 Nei

Hvis nei, gå videre til pkt. 1.7.3.

Hvis ja, redegjør for hvilke virksomheter som vil fungere som databehandlere i prosjektet:

Virksomhet	Rolle/funksjon	Land
Eksterne laboratorier	Databehandler	Hovedsakelig til Norge, EU/EØS, Storbritannia og USA
Sikt (FileSender)	Databehandler	Norge

Hvordan skal personopplysninger i så fall utleveres til ekstern institusjon?

HUNT kan ha behov for å overføre humant biologisk materiale til eksterne laboratorier for analyse. Det inngås da en databehandleravtale med det eksterne laboratoriet. Materialet som overføres vil være aidentifisert og koblingsnøkkel lagres hos HUNT databank. Analyseresultat tilbakeføres til HUNT og overskuddsmateriale destrueres etter analyse.

HUNT overfører data til forskere med forskerkompetanse for forskningsprosjekt som er godkjent av Data Access Committee (DAC) ved HUNT og Regional etisk komite for medisinsk og helsefaglig forskning (REK). Forskere har et selvstendig behandlingsansvar for datafilen de behandler, og hvert forskningsprosjekt trenger derfor et eget behandlingsgrunnlag. Dataoverføringen reguleres med en dataoverføringsavtale. Data blir overført passordbeskyttet via Uninett Filesender ved små til mellomstore filer. Genetiske data tilgjengeliggjøres via en sikker tilgang til HUNT Cloud.

For hver databehandler skal det godtgjøres at de gir tilstrekkelige garantier for at behandlingen oppfyller kravene i forordning og vern av den registrertes rettigheter.

For databehandler(e) er følgende oppfylt:

- Databehandleravtale som oppfyller forordningens krav
- Mottatt og gjennomgått risiko- og sårbarhetsanalyse (ROS)
- Mottatt beskrivelse av tekniske og organisatoriske tiltak
- Mottatt oversikt over underleverandører

Hvis man benytter databehandlere, er det viktig at disse selv bidrar med informasjon om blant annet personopplysningsvern/informasjonsikkerhet, og kontakten bør beskrives. Er databehandlerne involvert i personvernkonsekvensvurderingen? Beskriv hvordan databehandler(e) har vært involvert:

Databehandlere er ikke involvert i personvernkonsekvensvurderingen.

1.7.3 Overføring av personopplysninger til andre land og/eller internasjonale organisasjoner

Skal personopplysninger utleveres/overføres til:

- Personer/institusjoner utenfor Norge
- Tredjeland (utenfor EU/EØS)
- Internasjonale organisasjoner
- Det skal ikke utleveres/overføres personopplysninger

Dersom personopplysninger skal føres til tredjeland og/eller internasjonale organisasjoner:

I den grad personopplysninger skal overføres til land utenfor EØS-området eller internasjonale organisasjoner, må det beskrives hvordan pliktene etter kapittel V i personvernforordningen skal oppfylles.

Overføringene vil skje på følgende grunnlag:

- Beslutning om at det aktuelle land har et tilstrekkelig beskyttelsesnivå

- Overføringen er omfattet av nødvendige garantier, slik som EUs standardavtaler, beskriv under:

Når data skal overføres til utlandet, eller når humant biologisk materiale skal analyseres i andre land enn Norge inngås en dataoverføringsavtale på lik linje med dataoverføring i Norge når det gjelder EU/EØS land eller godkjente tredjeland.

For biologisk materialet som blir sendt ut fra HUNT biobank inngås det i tillegg en Databehandler avtale (DPA) eller en Material Transfer Agreement (MTA) som har samme formål, men omfatter noen paragrafer om biologisk materiale.

Om overføring ikke er i tråd med gjeldende regelverk, forutsetter det at det inngås avtaler der dette blir ivaretatt. For alle overføringer til land utenfor EU/EØS som ikke er godkjente tredjepartsland inngås det en avtale som omfatter standard klausuler om datasikkerhet og personvern iht. GDPR.

Om dette ikke er mulig, vil ikke data/biologisk materiale bli overført.

- Overføringen er underlagt bindende virksomhetsregler, slik som registrering under Privacy Shield, beskriv under:

Unntak for særlige situasjoner, beskriv under:

Redegjør for hvordan personopplysningene overføres og lagres ut av Norge:

Det overføres kun aidentifiserte data/biologisk materiale, der koblingsnøkkel lagres hos HUNT databank. Elektroniske data blir overført passordbeskyttet via Uninett Filesender. Biologisk materiale sendes per post. Databehandleren skal i henhold til avtale overholde alle forpliktelser til gjeldende personopplysningslovgivning som regulerer bruken og behandling av overleverte personopplysninger. Databehandleren skal iverksette passende tekniske, fysiske og organisatoriske sikkerhetstiltak for å beskytte overførte personopplysninger mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet. Kun ansatte hos databehandleren, som trenger tilgang til personopplysninger i forbindelse med sitt arbeid, skal gis slik tilgang. Databehandleren skal også forsikre seg om at ansatte har taushetsplikt med hensyn til dokumentasjon og personopplysninger som de får tilgang til. Dette skal dokumenteres og kunne tilgjengeliggjøres på forespørsel.

1.8 NTNUs politikk for informasjonssikkerhet

Er databehandlingen i samsvar med NTNUs politikk for informasjonssikkerhet?

- Ja
 Nei
 Ikke aktuelt

[Se også NTNUs politikk for informasjonssikkerhet på INNSIDA](#)

2 Rettslig grunnlag for behandling av personopplysninger

2.1 Rettslig grunnlag for behandling av personopplysninger

Se også: <https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=Personopplysningsloven>

Hjemmel i EUs personvernforordning for behandling av personopplysninger.

Artikkel 6, Behandlingen er lovlig og oppfyller følgende vilkår (gjelder dersom minst ett er oppfylt):

- a) den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål.
- b) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse
- c) behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige
- d) behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser

- e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt
- f) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.
- Annet, spesifiser:

§8 i Personopplysningsloven: Personopplysninger kan behandles på grunnlag av personvernforordningen artikkel 6 nr. 1 bokstav e dersom det er nødvendig for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål. Behandlingen skal være omfattet av nødvendige garantier i samsvar med personvernforordningen artikkel 89 nr. 1.

Helseregisterloven §19 e og Helsepersonelloven §29: Regional etisk komite kan gi dispensasjon fra taushetsplikten

2.2 Rettslig grunnlag for behandling av særlige kategorier av personopplysninger (sensitive personopplysninger)

Gjelder behandlingen av særlige kategorier av personopplysninger, må det i tillegg angis om behandling av slike opplysninger er omfattet av unntakene i EUs personvernforordning artikkel 9 og supplerende grunnlag i norsk lovgivning:

- 1. Den registrerte har gitt uttrykkelig samtykke til behandlingen av særlige kategorier av personopplysninger.**
- 2. Behandlingen av særlige kategorier opplysninger er nødvendig for vitenskapelig forskning på grunnlag av følgende lovverk:**

- a) 9.2 j: Behandlingen er nødvendig for vitenskapelig forskning.
- b) Personopplysningsloven § 9/EUs personvernforordningen 9.2 g: Samfunnets interesse i at behandlingen finner sted overstiger klart ulempene for den enkelte (forskningsdeltakerne)
- c) Annet. Lov- eller forskriftshjemmel må angis og eventuelt begrunnes nærmere:

Personopplysningsloven § 9: Personopplysninger som nevnt i personvernforordningen artikkel 9 nr. 1 kan behandles uten samtykke fra den registrerte dersom behandlingen er nødvendig for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål og samfunnets interesse i at behandlingen finner sted, klart overstiger ulempene for den enkelte. Behandlingen skal være omfattet av nødvendige garantier i samsvar med personvernforordningen artikkel 89 nr. 1.

Helseregisterloven §19 e og Helsepersonelloven §29: Regional etisk komite kan gi dispensasjon fra taushetsplikten

- 3. Behandlingen av særlige kategorier av opplysninger er nødvendig til annet formål enn forskning.**
Riktig henvisning til forordningen artikkel 9 nr. 2 bokstav b) tom. bokstav i) må angis og ved tilleggskrav om regulering i nasjonal rett må også lov eller forskriftshjemmel presiseres:

2.3 Formålsbegrensning og dataminimering

Formålet med behandlingen er oppgitt i punkt 1.1. Personopplysningene som behandles skal være adekvate, relevante, nødvendige og begrenset til det som er nødvendig for formålene.

Følgende tiltak planlegges for å sikre dataminimering:

HUNT leverer ut data etter søknad som må godkjennes av Data Access Committee ved HUNT. Kun data som er relevant for forskningsprotokollen blir utlevert til prosjekt. Prosjektleder gis tilbakemelding og anmodes redusere dataomfanget dersom dette åpenbart ikke er nødvendig for å besvare forskningsspørsmålene. På denne måten tilstrebes dataminimering, og at variabler ikke kan utnyttes utover det prosjektet har tillatelse til.

Når prosjektet er fullført skal forskere slette sin utleverte datafil, men sørge for lagring i ytterligere 5 år om REK krever dette. HUNT databank eller HUNT Cloud tilbyr slik lagring etter prosjektslutt.

2.4 Lagring

Lagringstid skal beskrives og begrunnes.

Prosjektleder må ta stilling til hvor lenge det vil være behov for behandling av personopplysningene:

- Forhåndsfastsatte slettedatoer (spesifiser, og begrunn med tid for analyse, etterfølgende oppbevaring for dokumentasjon/arkivformål).
- Tidsbegrenset, men uten fastsatt dato (angi kriterier for fastsetting av varighet)

Spesifiser lagringstid og dato for pseudonymisering/sletting av data:

Data lagret i HUNT databank og HUNT Cloud som er innsamlet i regi av HUNT forskningscenter er i henhold til Forskrift for befolkningsbaserte helseundersøkelser godkjent for ubegrenset lagring, dette inkluderer også lagring og bruk av prosjektdeltagers data etter ens død.

For data utlevert til forskningsprosjekt avtales prosjektvarighet og slettedato.

Her må det fastsettes en foreløpig slettedato eller dato for ny vurdering av behov for videre oppbevaring.

2.5 De registrertes rettigheter

2.5.1 Samtykke

Dette punktet gjelder for de prosjektene hvor det skal innhentes eget samtykke eller benyttes opplysninger fra allerede innsamlede befolkningsbaserte helseundersøkelser.

Spesifiser og vurder prosess for innhenting av samtykke:

Det har vært ulik praksis for innhenting av samtykke i de ulike datainnsamlingsrundene.
I HUNT1 ble det ikke innhentet samtykke, men oppmøte ble vurdert som samtykke til deltakelse, lagring og forskning på data.

I HUNT2 og HUNT3 ble informasjon og samtykkeerklæring utsendt ved invitasjon til undersøkelsen. Samtykke ble innhentet skriftlig ved oppmøte på feltstasjonene. HUNT2 har ikke et samtykke som dekker kobling til alle registre eller elektronisk pasientjournal.

I HUNT4 ble informasjon om undersøkelsen og samtykkeerklæring utsendt sammen med invitasjon til undersøkelsen. Samtykket ble registrert ved elektronisk besvarelse av spørreskjema før oppmøte på feltstasjonen, om dette ikke var gjort, ble deltager spurt ved oppmøte og svaret ble registrert elektronisk. I HUNT i Sør-Trøndelag ble det sendt ut SMS invitasjon til å besvare et elektronisk spørreskjema. Samtykket ble innhentet elektronisk hos de fleste. Noen eldre deltakere fikk tilsendt et papirbasert spørreskjema, og samtykket skriftlig.

I HUNT 70+ kunne nære pårørende samtykke til deltakelse for den aktuelle, om denne manglet samtykkekompetanse. I alle slike tilfeller ble undersøkelsen gjennomført kun når deltakeren selv ikke viste tegn til ubehag eller motsatte seg deltakelse.

I Ung-HUNT ble informasjon om undersøkelsen sendt til både foreldre og potensiell deltaker. Lagring av data i HUNT databank for deltakere yngre enn 16 år forutsetter samtykke fra både foreldre/foresatte og deltager. For ungdom under 16 år med samtykke fra foreldre/verge gjelder samtykket også etter fylte 16 år.

Det er diverse tilleggundersøkelser knyttet til HUNT hoveddelen. Samtykket har blitt hentet inn separat for hvert tilleggprosjekt av prosjektledere for disse undersøkelsene.

Vår vurdering er at samtykket er i samsvar med kravene i art. 4 nr. 11 og art. 7 i personvernforordningen (GDPR), ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse, som kan dokumenteres, og som den registrerte kan trekke tilbake.

I HUNT1 og HUNT2 der det ikke foreligger tilstrekkelig samtykke er formålet med behandling av personopplysninger å utføre en oppgave i allmennhetens interesse.

Lovlig grunnlag for behandlingen er dermed

- 1) den registrertes uttrykkelige samtykke jf. personvernforordningen art. 6 nr. 1 bokstav a. og art. 9 nr. 2 bokstav a., jf. personopplysningsloven § 8 og §10.
- 2) en oppgave i allmennhetens interesse jfr artikkel 6, nr.1, bokstav e., knyttet til vitenskapelig forskning eller statistiske formål der samfunnsnyttens klart overstiger ulempen for deltakeren jf. personvernforordningen art. 9 nr. 2 bokstav j., art. 89 nr.1 og nr. 2 jf. Personopplysningsloven § 9.

2.5.2 Informasjon om behandlingen

Det må beskrives hvordan informasjon om behandling av personopplysninger vil gis til de registrerte. Informasjonsplikten gjelder for alle forskningsprosjekter uavhengig om det er samtykkebasert eller det kun benyttes registerdata.

Informasjonen gis på følgende måte(r):

- Informasjonsskriv i forbindelse med samtykke
- Informasjon på nett
- Nyhetsbrev
- Brev
- E-post
- Individuell informasjon per e-post eller brev
- Sosiale medier

Offentlig informasjonskampanje

Annet, spesifiser:

2.5.3 Rett til innsyn, behandlingsbegrensning, retting, sletting og portabilitet

Kriterier for sletting av data

- Data om alle registrerte slettes en bestemt dato
- Data om alle registrerte slettes etter et fast intervall
- Data om den enkelte slettes etter en bestemt hendelse
- Ingen systematisk sletting av data

Utdyp nærmere basert på det som er avkrysset i feltet over:

Eksempelvis hvilket tidsintervall eller hvilken hendelse som fører til at data blir slettet. Henvis også til gjeldende sletterutiner dersom slettingen er basert på manuelle aktiviteter.

I henhold til § 4-7 og § 5-3 Forskrift for befolkningsbaserte undersøkelser kan innsamlede helseopplysninger og humant biologisk materiale oppbevares på ubegrenset tid, med mindre annet følger samtykket eller formålet med innsamlingen.

Er det mulighet for den registrerte til å rette og slette sine opplysninger?

- Ja
- Nei

Er det mulighet for registrerte til å komme med innsigelser og krav om begrensninger i databehandlingen?

- Ja
- Nei

Dersom den registrertes rettigheter ikke kan oppfylles, beskriv hva og hvorfor:

Begrunn hvorfor samfunnsinteresser her skal veie tyngre enn personvernet til den enkelte.

Beskriv forhold mellom den registrerte og datainnsamler:

Eksempel pasient og behandler, ansatt og arbeidsgiver.

Deltager og forskningsansvarlig

3 Personvern, risikoanalyse og tiltak

Vurdering av risiko for de registrertes rettigheter og friheter, og planlagte tiltak for å håndtere risikoene.

3.1 Medbestemmelse, åpenhet, forutsigbarhet

Vurdering av risikoens opprinnelse, art, særegenhet og alvorlighetsgrad. Vurderingen skal gjøres fra de registrertes perspektiv for hver risiko:

- Manglende reell medbestemmelse

- Manglende reell åpenhet
- Manglende forutsigbarhet

Avklar potensielle konsekvenser, anslå alvorlighetsgrad, identifiser trusler og anslå sannsynlighet:

OM HUNT ikke ville kunne overholde personvern kan det ha følgende konsekvenser:

1. Risiko: personopplysninger kommer på avveie. Dette ville være svært alvorlig. Den største trusselen ligger i utlevering av datafiler som blir koblet til opplysninger fra andre registre. På den måten har ikke HUNT oversikt over hvilke opplysninger som inngår i et prosjekt til slutt og om det er fare for bakveidentifisering av deltakere. Utlevering av datafiler er også basert på tillitt til at forskere bruker opplysningene som avtalt og sletter filen etter bruk. HUNT anser det som lite sannsynlig at forskere med vilje skal prøve å få tilgang til personidentifiserende data og bruke datafilen for andre formål enn avtalt.

Det er lite risiko for at data blir snappet opp av andre under dataoverføringer- her bruker HUNT en sikker løsning og to-faktor autentisering.

2. Risiko: Data fra deltakere inngår i forskningsprosjekt som er ukjente og uønsket av deltager. Dette er svært uheldig og innebærer at deltager ikke har hatt grunnlag for å gi informert samtykke. Det er ikke mulig å ha oversikt over alle framtidige prosjekt som skal bruke HUNT-data og biologisk materiale ved innsamling av dette. Informasjon om nye prosjekt kan gis ved skriftlig eller webbasert informasjon til deltagere, men også jevnlig nyhetsoppslag om løpende forskning og forskningsresultat fra HUNT. De fleste deltakere er innstilt på å bidra maksimalt til forskning om helse og sykdom og vil nok stille seg positive til forskningsprosjektene som utføres. Hvis de ikke lenger ønsker å være med, kan de alltid trekke sitt samtykke uten nærmere begrunnelse. Sannsynlighet for at deltakere blir med på forskning uten at de ønsker det anser vi derfor som lav.

3.2 Tiltak

Spesifiser tiltak for å håndtere risikoene for de registrerte og andre berørte personers rettigheter og berettigede interesser.

- Spesifikke garantier for å minimere inngripen
- Spesifikke sikkerhetstiltak som angår personopplysninger som skal behandles
- Generelle sikkerhetstiltak som iverksettes på systemet hvor behandlingen utføres
- Organisatoriske tiltak (styring)

Direkte identifiserende opplysninger blir ikke utlevert til forskningsprosjekt, men mulighet for indirekte identifisering kan ikke helt utelukkes. HUNT forskningssenter er nøye på å utlevere kun variabler som er nødvendig for å besvare forskningsspørsmål beskrevet i protokoller til godkjente forskningsprosjekt og tar en helhetsvurdering om samlet størrelse av datamaterialet og type variabler.

Variabler som, i sammenheng med andre variabler, innebærer mulighet for å identifisere deltakere blir gruppert i kategorier som omfatter flere deltakere der dette er mulig. Dette gjelder bl.a. bostedskrets- og kommuner, yrke og alder.

Lagring av data er underlagt NTNUs retningslinjer for sikker lagring, og ansvaret for datasikkerhet er delegert til NTNUs IT avdeling. Overføring av datafiler til prosjektledere skjer gjennom sikker filoverføring HUNT forskningssenter er ISO-sertifisert og utfører en årlig risikovurdering på informasjonssikkerhet, og utfører tiltak når dette er nødvendig.

Alle prosjektledere som bruker HUNT data skriver under en avtale som bekrefter deres ansvar for datasikkerhet.

3.3 Samlet vurdering av personvernet

Prosjektleder skal gjøre en oppsummering av personvern og personopplysningsikkerheten:

HUNT data omfatter mange opplysninger, noen av sensitive art.
Alle ansatte ved HUNT forskningscenter som forvalter og behandler HUNT- materiale har taushetsplikt og er seg bevisst viktigheten av personvern.
HUNT forskningscenter benytter seg av sikre lagringsmuligheter og dataoverføringstjenester og stiller krav til brukere av HUNT- data om sikker håndtering av data.
Det at andre enn HUNT-ansatte får utlevert datafiler med personopplysninger kan innebære en viss risiko for personvernet, men HUNT tilstreber å minimere og kategorisere data som ikke skulle begrense viktig forskning.
Personopplysninger blir kun utlevert til forskningsprosjekt som er innenfor formålet for HUNT og deltakernes samtykke, eller hvor prosjekt har blitt vurdert å være samfunnsnyttig forskning.
Når opplysningene blir levert ut til prosjekt utenfor Norge, så overholder HUNT forskningscenter kravene fra GDPR. For land utenfor EU uten avtaleverk som sikrer personvern, inngås avtaler hvor krav for personvern er spesifisert.
Deltakere har mulighet å kontakte HUNT og få opplysninger om hvilke personopplysninger HUNT databank har lagret og behandler, hvordan personopplysninger blir behandlet, lagret og brukt og til hvilke formål.
Deltakere kan reservere seg mot deltakelse i deler av HUNT eller trekke sitt samtykke ved å kontakte HUNT.
HUNT forskningscenter tar utgangspunkt i lagring av personopplysninger i ubestemt tid, også etter at deltakere dør. Dette blir det opplyst om i samtykkeskrivet deltakere får ved deltakelse.
HUNT er avhengig av at også prosjektledere som behandlingsansvarlig forholder seg til personopplysningsloven. Dette blir prosjektledere opplyst om i avtalen om bruk av HUNT- materiale.
Samlet mener HUNT forskningscenter at personvernet ivaretas på en god måte, men at vi samtidig ønsker å utvikle oss og forbedre oss på dette området. Utover dagens prosedyrer, så jobbes det med å få bedre oversikt over samlet datamengde og variabeltyper forskere har i sine prosjekt; vi ønsker ikke bare oversikt over data utlevert fra HUNT, men også type variabler fra andre register Personvern har høy prioritet ved HUNT forskningscenter.

4 Involvering og drøftelser

4.1 Forhåndsdrøfting med Datatilsynet

Når den behandlingsansvarlige ikke kan finne tilstrekkelige tiltak for å begrense risikoen til et akseptabelt nivå (det vil si at restrisikoen fremdeles er høy), er det krav om forhåndsdrøftelse med tilsynsmyndigheten (Datatilsynet).

Er det behov for forhåndsdrøftelse med Datatilsynet?

- Ja
 Nei

5 Godkjenning

Signatur fra instituttleder.

Dato: 21.12.23,
Sted: Trondheim
Signatur: *Solveig K. Grudt*

Ferdig utfylt og signert personvernkonsekvensvurdering sendes til administrasjonen ved din enhet/institutt for arkivering i ePhorte (saksnr. 2023/24702).