Personvernkonsekvensvurdering (DPIA)

**Prosjektopplysninger**

|  |
| --- |
| **Prosjekttittel:** |
|  |
| **Prosjektleder:**  *Prosjektleder har ansvaret for at personvern- og informasjonssikkerhetsmessige forhold ivaretas i prosjektet.* |
|  |
| **Prosjektets tilhørighet:** *Institutt, enhet, helseforetak.* |
|  |
| **Forskningsansvarlig/behandlingsansvarlig[[1]](#footnote-2):**  *Instituttleder er forskningsansvarlig/behandlingsansvarlig for alle prosjekter på instituttet.* |
|  |
| **Finansiering av prosjektet:** |
|  |
| **Prosjektopplysninger**  *REK-nummer og prosjektperiode (varighet på prosjektet).* |
|  |

# Behandling av personopplysninger i prosjektet

## 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.

|  |
| --- |
|  |

## Datakilder

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

Egen datainnsamling (prosjektet vil innhente direkte fra den opplysningen(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:

|  |
| --- |
|  |

## 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:

|  |
| --- |
|  |

## 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:

|  |
| --- |
|  |

## 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)

## 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:

|  |
| --- |
|  |

Annet, spesifiser:

|  |
| --- |
|  |

Eventuelt spesifiser lagringen av personopplysningene:

|  |
| --- |
|  |

## Dataansvarlig, datatilgang og databehandlere

### Dataansvarlig og personer med datatilgang

Delegert dataansvarlig (instituttleder, på vegne av NTNU):

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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.)

### 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 |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Hvordan skal personopplysninger i så fall utleveres til ekstern institusjon?

|  |
| --- |
|  |

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/informasjonssikkerhet, og kontakten bør beskrives. Er databehandlerne involvert i personvernkonsekvensvurderingen? Beskriv hvordan databehandler(e) har vært involvert:

|  |
| --- |
|  |

### 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:

|  |
| --- |
|  |

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:

|  |
| --- |
|  |

## 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](https://innsida.ntnu.no/wiki/-/wiki/Norsk/Politikk+for+informasjonssikkerhet)

# Rettslig grunnlag for behandling av personopplysninger

## 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:

|  |
| --- |
|  |

## 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) Helseforskningsloven §35: Regional etisk komite kan gi dispensasjon fra taushetsplikten. Dette kan bare skje dersom slik forskning er av vesentlig interesse for samfunnet og hensynet til deltakernes velferd og integritet er ivaretatt.

d) Annet. Lov- eller forskriftshjemmel må angis og eventuelt begrunnes nærmere:

|  |
| --- |
|  |

**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:

|  |
| --- |
|  |

## 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:

|  |
| --- |
|  |

## 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:

|  |
| --- |
|  |

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

## De registrertes rettigheter

### 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:

|  |
| --- |
|  |

### 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:

|  |
| --- |
|  |

### 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.*

|  |
| --- |
|  |

**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.*

|  |
| --- |
|  |

# Personvern, risikoanalyse og tiltak

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

## 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:

|  |
| --- |
|  |

## 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)

|  |
| --- |
|  |

## Samlet vurdering av personvernet

Prosjektleder skal gjøre en oppsummering av personvern og personopplysningssikkerheten:

|  |
| --- |
|  |

# Involvering og drøftelser

## 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

# Godkjenning

*Signatur fra instituttleder.*

|  |
| --- |
| Dato:  Sted:  Signatur: |

Ferdig utfylt og signert personvernkonsekvensvurdering sendes til administrasjonen ved din enhet/institutt for arkivering i ePhorte (saksnr. 2021/1374).

1. Helseforskning bruker begrepet forskningsansvarlig. Øvrig forskning bruker begrepet behandlingsansvarlig. [↑](#footnote-ref-2)