**PERSONVERNKONSEKVENSVURDERING (DPIA)**

**Innledning**

En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal sikre at personvernet til de som er registrert i løsningen ivaretas. Dette er en plikt etter den nye personopplysningsloven som trådte i kraft 20. juli 2018.

Artikkel 35 i Lov om behandling av personopplysninger (personopplysningsloven) definerer når det er påkrevd å gjøre en DPIA, hva den skal inneholde og hvem som skal gjennomføre den. Vurderingen av personvernkonsekvenser skal gjennomføres **før** databehandlingen starter.

Artiklene som det er referert til i denne malen henviser til denne loven. Du finner loven i sin helhet [her](https://lovdata.no/dokument/NL/lov/2018-06-15-38). Se også [personvernforordningen](https://lovdata.no/eu/32016r0679) (GDPR).Datatilsynet har skrevet en veileder som går igjennom regelverket. Den finner du [her](https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/).

DPIA malen består av til sammen 5 deler:

1. Behandling av personopplysninger i prosjektet
2. Rettslig grunnlag for behandling av personopplysninger
3. Personvern, risikoanalyse og tiltak
4. Brukermedvirkning
5. Involvering av personvernombudet og forhåndsdrøftelse med Datatilsynet

**Behov for DPIA - Når må DPIA gjennomføres?**

*«Dersom det er sannsynlig at en* ***type behandling****, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens* ***art, omfang, formål og sammenhengen den utføres i****, vil medføre en* ***høy risiko*** *for fysiske personers* ***rettigheter og friheter****, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.»* (GDPR art.35.1)

**Kriterier når DPIA *kan* bli et krav når to eller flere av følgende kriterier er oppfylt:**

1. **Evaluering eller scoring**, spesielt knyttet til arbeidsresultater, økonomisk situasjon, helse, personlige preferanser eller interesser, oppførsel og adferd, lokasjon og bevegelser osv.
2. **Automatiserte beslutninger** med juridisk eller tilsvarende betydning.
3. **Systematisk overvåking** av registrerte.
4. **Særlige kategorier personopplysninger** eller **andre sensitive personopplysninger av høy personlig karakter** (sistnevnte spesielt knyttet de enkeltes «friheter», men kan også omfatte f.eks. økonomiske og finansielle opplysninger).
5. **Databehandling i stort omfang**, som at det er et stort antall registrerte involvert, store mengder data, mange ulike typer data, lang varighet av behandlingen, stor geografisk utbredelse av behandlingen osv.
6. **Kombinering eller sammenstilling av datasett**.
7. Personopplysninger vedrørende **spesielt sårbare registrerte** (som barn, ansatte, psykisk syke, asylsøkere, eldre, pasienter mv.).
8. **Innovativ eller nyskapende bruk av personopplysninger,** som f.eks. bruk av biometriske data for tilgangskontroll, Internet of Things-løsninger, velferdsteknologi osv.
9. Når behandlingen i seg selv **forhindrer eller begrenser de registrertes mulighet til å utøve sine rettigheter** etter loven eller avtale, eller **bruke tjenester**.

**Prosjektopplysninger**

|  |
| --- |
| Prosjekttittel:  |
| PVO nummer: *Saksnummer som genereres ved opprettelse av prosjekt i eSkjema* |
| Prosjektleder: |
| Prosjektets tilhørighet (Avdeling):  |
| Arkivnummer (P-360): *Arkivnummer som opprettes i sykehusets arkivsystem, Public360* |

**Vurderingsspørsmål**

Dersom svaret er "ja" på ett eller flere av spørsmålene nedenfor, kan det bety at det er behov for en DPIA. For bistand til behovsvurdering og/ eller gjennomføring av DPIA kan man kontakte avdeling for forskningsstøtte (forskning.personvern@ahus.no).

Formell beslutning for gjennomføring av konsekvensutredningen ligger formelt hos avdelingsleder. Dersom det besluttes at det ikke er behov for å gjennomføre en DPIA, skal det begrunnes hvorfor.

|  |  |  |  |
| --- | --- | --- | --- |
| Nr | Vurderingsspørsmål | Ja  | Nei |
| 1. | Er dette et nytt prosjekt eller prosess? |  |  |
| 2. | Vil prosjektet innebære innsamling av ny informasjon om enkeltpersoner? |  |  |
| 3. | Vil prosjektet be enkeltpersoner om å gi informasjon om seg selv? |  |  |
| 4. | Vil informasjon om enkeltpersoner bli delt med organisasjoner eller personer som ikke tidligere har hatt rutinemessig tilgang til informasjonen? |  |  |
| 5. | Skal du bruke informasjon om enkeltpersoner som er innsamlet for et formål, men der opplysningene for tiden ikke er eller ikke lenger er i bruk (ikke behandles utover lagring)? |  |  |
| 6. | Innebærer prosjektet at du bruker ny teknologi som kan oppfattes som inngripende for personvernet? For eksempel, bruk av biometri eller ansiktsgjenkjenning? |  |  |
| 7. | Vil prosjektet resultere i at du tar beslutninger eller gjennomfører tiltak mot enkeltpersoner på måter som kan ha en betydelig innvirkning på dem? |  |  |
| 8. | Basert på typen informasjon om enkeltpersoner, er det spesielt sannsynlig at bekymringen for eller forventninger til personvernet vil øke? |  |  |
| 9. | Vil prosjektet kreve at du kontakter personer på måter som de kan finne inngripende? |  |  |
| 10 | Vil prosjektet innebære databehandling i stort omfang, som at det er et stort antall registrerte involvert, store mengder data, mange ulike typer data, lang varighet av behandlingen, stor geografisk utbredelse av behandlingen osv? |  |  |

I dette prosjektet er det besluttet at det skal:

[ ]  Gjennomføres en DPIA

[ ]  Ikke gjennomføres en DPIA

|  |
| --- |
| Begrunnelse for hvorfor det skal/ikke skal gjennomføres en DPIA i prosjektet*Begrunn her* |

**Organisering av personvernkonsekvensvurderingen og ansvarsforhold**

Prosjektleder (eventuelt med bistand fra en prosjektgruppe) har gjennomført en DPIA.

Følgende personer har deltatt i DPIA vurderingen:

|  |  |  |
| --- | --- | --- |
| Navn | Rolle/funksjon | Avdeling |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Behandling av personopplysninger i prosjektet

## Formålet med behandlingen av personopplysninger

*Formålene skal være spesifikke, uttrykkelig angitte og berettigede. For forskning innebærer det at det må formuleres konkrete forskningsspørsmål som skal besvares gjennom bruken av opplysningene. Prosjektbeskrivelse/forskningsprotokoll skal vedlegges.*

|  |
| --- |
| Prosjektleders beskrivelse av formålet:*Beskriv her* |

## 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

[ ]  Bildediagnostikk

[ ]  Folkeregisteret

[ ]  SSB

[ ]  NAV

[ ]  Internett

[ ]  Annet, *spesifiser her*:

|  |
| --- |
| Spesifisering av datakildene det er krysset av for ovenfor og beskriv kobling (sammenstilling) dersom det er relevant: *Spesifiser her**F.eks. kobling mellom pasientjournal opp mot reseptregister* |

## 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

[ ]  Ansatte

[ ]  Pasienter

[ ]  Pasienter uten samtykkekompetanse

[ ]  Barn, spesifiser aldersgrupper

[ ]  0-11

[ ]  12-15

[ ]  16-18

[ ]  Pårørende

[ ]  Etniske minoriteter

[ ]  Avdøde

[ ]  Annet, *spesifiser her:*

|  |
| --- |
| Beskriv utvalget, eventuelt underutvalg:*Beskriv her**F.eks. pasienter mellom 0-18 år som er pasienter ved BUK. Det er tenkt å innhente samtykke fra foreldre/de med foreldreansvar, evt. fra barnet selv når over 16 år eller 12 år når særlige grunner foreligger (jfr. helseforskningslover § 17 i forbindelse med samtykke i helseforskning)*  |

|  |
| --- |
| Antall registrerte: *Oppgi her**Oppgi både antall registrerte ved Ahus og totalt i studien hvis studien går ved flere senter.* |

|  |
| --- |
| Geografisk omfang:*Beskriv her* |

## Kategorier av personopplysninger

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

Kategorier av personopplysninger

[ ]  Navn

[ ]  Adresse

[ ]  Fødselsdato

[ ]  Fødselsnummer (11 siffer)

[ ]  Andre opplysninger, *angi hvilke:* *F.eks. telefonnummer, e-postadresse, IP-adresse, demografiske variabler, sosioøkonomiske opplysninger (utdanning, inntekt, yrke), familiestatus, biometri)*

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 med det formål entydig å identifisere en person *(f.eks. fingeravtrykk, ansiktsgjenkjenning, stemme osv.)*

[ ]  Helseforhold:

[ ] Diagnoser

[ ]  Legemiddelbruk

[ ]  Kognitive evner

[ ]  Genetiske opplysninger

[ ]  Annet, *spesifiser her:*

|  |
| --- |
| Gi en samlet beskrivelse av hvilke opplysninger som skal samles inn og behandles i prosjektet og nivå på variabler som for eksempel svært spesifikke variabler som enkelt kan ledes tilbake til enkeltindivider:*Beskriv her**F.eks. hva er det som er aktuelt å hente ut og undersøke i datasettet for å finne en sammenheng/bekrefte hypotese. Eksempler på variabler kan være alder, vekt og hvorvidt man røyker. Det kan også være spesifikke verdier i prøver.* |

## Behandling av personopplysninger

*Med «behandling» menes enhver prosess eller rekke av prosesser som gjøres med personopplysninger*.

Kryss av for hva som skal gjøres med personopplysningene i prosjektet. Behandlingene må være i samsvar med det oppgitte formål.

[ ]  Innsamling

[ ]  Lagring

[ ]  Sammenstilling, kobling

[ ]  Analysering

[ ]  Utlevering ved overføring

[ ]  Tilgjengeliggjøring (for *eksempel krav om rådata i lukkede databaser ifm. publisering hos enkelte tidsskrifter)*

[ ]  Gjenfinning *(for eksempel ved planlagt tilbakemelding til de registrerte)*

 [ ]  Sletting, anonymisering

[ ]  Annen bruk, *spesifiser her:*

|  |
| --- |
| Beskriv behandlingen av personopplysningene det er krysset av for over:*Beskriv her* |

|  |
| --- |
| Angi frekvens på innsamlingen: *Angi her**F.eks. samles opplysninger inn en gang, flere ganger, regelmessig osv.* |

|  |
| --- |
| Beskriv hvordan opplysningene samles inn: *Beskriv her**F.eks. samles opplysningene inn via applikasjon, lydbånd, ny teknologi, osv.* |

## Lagringssted og lagringsmedier

Angi hvor og hvordan personopplysninger skal lagres og håndteres.

[ ]  Tjenester for Sensitive Data (TSD)

[ ]  Tilgangsbegrenset forskningsfilmappe

[ ]  Sikker sone

[ ]  Kryptert minnepinne (Ironkey):

[ ]  eCRF, *Navngi løsning her:*

[ ]  Annet, *spesifiser her:*

|  |
| --- |
| Spesifiser/Beskriv lagringen av personopplysningene:*Spesifiser/beskriv her**F.eks. hvilke løsninger, hvem har tilgang osv.* |

##  Dataansvarlig, datatilgang og databehandlere

### Dataansvarlig og personer med datatilgang

|  |
| --- |
| Dataansvarlig (Navn på institusjon):*Oppgi her* |

|  |
| --- |
| Dersom studien gjennomføres som en multisenterstudie med felles dataansvar: |
| Hvilke institusjoner som deltar:*Oppgi her* |
| Hvilke opplysninger overføres:*Oppgi her* |
| Hvordan opplysningene vil overføres:*Oppgi her* |

**Følgende prosjektmedarbeidere og annet personell vil ha tilgang til data i prosjektet:**

|  |  |  |
| --- | --- | --- |
| Navn | Rolle/funksjon | Virksomhet |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| Beskriv hvordan medarbeiderne skal få tilgang til data:*Beskriv her* |

### Databehandler

**Dersom det benyttes databehandler(e), fyll inn informasjon (eks. eksternt laboratorium, kjernefasiliteter, ekstern lagring osv.):**

|  |  |  |
| --- | --- | --- |
| Virksomhet | Rolle/funksjon | Land |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| Beskriv hvordan personopplysninger utleveres til ekstern institusjon:*Beskriv her**F.eks. dersom man skal utlevere både opplysninger og samtykke og/eller koblingsnøkkel, vil det være relevant å oppgi hvordan også samtykke og koblingsnøkkel utleveres. Sendes det separat i post osv.*  |

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 (*Det er tilstrekkelig å benytte* [mal](https://www.ahus.no/fag-og-forskning/forskning-og-innovasjon/personvern#databehandlingsansvarlig-og-databehandler) *som ligger tilgjengelig på Ahus sin nettside*)

[ ]  Mottatt og gjennomgått Risiko Og Sårbarhetsanalyse (ROS) (vedlegges). *Der hvor det er gjennomført ROS, som f.eks. for TSD, er det tilstrekkelig å vise til hvilken. Dersom det er nye løsninger, eller løsninger som ikke har vært benyttet tidligere, bør man kontakte informasjonssikkerhetsansvarlig for gjennomgang.*

[ ]  Mottatt beskrivelse av tekniske og organisatoriske tiltak (*Dette dekkes* av [databehandleravtalen](https://www.ahus.no/fag-og-forskning/forskning-og-innovasjon/personvern#databehandlingsansvarlig-og-databehandler))

[ ]  Mottatt oversikt over underleverandører (*Dette dekkes av* [databehandleravtalen](https://www.ahus.no/fag-og-forskning/forskning-og-innovasjon/personvern#databehandlingsansvarlig-og-databehandler)) 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?**

[ ]  Nei

[ ]  Ja

|  |
| --- |
| Hvis ja; Beskriv hvordan databehandler(e) har vært involvert:*Beskriv her* |

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

**Skal personopplysninger utleveres til personer/institusjoner utenfor Norge?**

[ ]  Nei

[ ]  Ja

**Hvis ja:**

Skal personopplysninger føres til tredjeland (land utenfor EU/EØS) og/eller internasjonale organisasjoner?

[ ]  Nei, gå videre til kapittel 1.8.

[ ]  Ja

**Dersom ja, besvar under:**

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 (kryss av og beskriv i tekstboksen under):

[ ]  Beslutning om at det aktuelle land har et tilstrekkelig beskyttelsesnivå (Artikkel 45). *Det er 12 land utenfor EU hvor det er beslutning om tilstrekkelig beskyttelsesnivå (per 18.12.2018)*

[ ]  Overføringen er omfattet av nødvendige garantier, slik som EUs standardavtaler (Artikkel 46)

[ ]  Overføringen er underlagt bindende virksomhetsregler, (Artikkel 47):

[ ]  Unntak for særlige situasjoner, (Artikkel 49):

*Det ligger to standardavtaler for databehandling, i dansk og engelsk versjon, på Datatilsynets sider: Der ligger det også oversikt over hvilke land utenfor EU/EØS hvor det er beslutning om tilstrekkelig beskyttelsesnivå.*

[*https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overfore/*](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overfore/)

*For å undersøke om selskapet har tilsluttet seg Privacy Shield, og på hvilke vilkår:*

[*https://www.privacyshield.gov/list*](https://www.privacyshield.gov/list)

|  |
| --- |
| Hva er rettslig grunnlag for overføring utenfor EØS?*Beskriv her**Artikkel 44 oppstiller et generelt prinsipp for overføring til utlandet. Det rettslige grunnlaget vil kunne være angitt ovenfor, sammen med artikkel 44.* |

|  |
| --- |
| Redegjør for hvordan personopplysningene overføres og lagres ved overføringen:*Redegjør her* |

##  Adferdsnormer – det er foreløpig ikke etablerte godkjente adferdsnormer. Dette punktet er ikke obligatorisk å besvare

I den grad det finnes godkjente adferdsnormer for den aktuelle behandling, f.eks. NORMEN eller BBMRI Code of Conduct, skal disse angis og det skal opplyses om de vil følges i behandlingen av personopplysninger i prosjektet.

|  |
| --- |
| Oppgi dersom adferdsnorm skal følges i behandlingen av personopplysninger:*Oppgi her* |

# Rettslig grunnlag for behandling av personopplysninger

## Rettslig grunnlag for behandling av personopplysninger

|  |  |  |
| --- | --- | --- |
| Nr | Vurderingsspørsmål | Svar (forklar svar) |
| 1 | Er behandlingen av personopplysninger lovlig etter personvernforordningen artikkel 6?*Obs – dette er personopplysninger som ikke er «sensitive»* | *Relevant:* *Nr. 1 a) den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål**Nr. 1 e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt, jf. nr. 3.* |
| 2 | Er behandlingen av særlige kategorier av personopplysninger lovlig etter personvernforordningen artikkel 9? | *Relevant:* *Nr. 2 a) Den registrerte har gitt uttrykkelig samtykke til behandling av slike personopplysninger for ett eller flere spesifikke formål, unntatt dersom det i unionsretten eller medlemsstatenes nasjonale rett er fastsatt at den registrerte ikke kan oppheve forbudet nevnt i nr. 1.**Nr. 2 g) Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser* |
| 3 | Finnes det hjemmelsgrunnlag i forskrift eller lov for behandlingen av personopplysninger? | *Se* [*Helseforskningsloven*](https://lovdata.no/dokument/NL/lov/2008-06-20-44) *§32.* |
| 4 | Finnes det forhåndsgodkjenning fra REK, konsesjon fra Datatilsynet, og/eller dispensasjon fra taushetsplikten? | *Hvis ja, vis til saksnummer eller vedlegg.* |

## De registrertes rettigheter

### Samtykke

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

**Vurder og svar i tabellen under:**

|  |  |  |
| --- | --- | --- |
| Nr | Vurderingsspørsmål | Svar (forklar svar) |
| 1 | Forutsettes det samtykke for databehandlingen? |  |
| 2 | Beskriv hvordan samtykke vil bli innhentet? |  |
| 3 | Er alle kravene til samtykke oppfylt? Samtykke fra den registrerte må være frivillig, spesifikk, informert og utvetydig (GDPR art.4). |  |
| 4 | Hvordan dokumenteres samtykke?  | *Vil samtykket f.eks. være skriftlig, og vil det tydelig fremgå hva det er samtykket til* |
| 5 | Kan samtykke trekkes tilbake like enkelt som det gis? |  |
| 6 | Foreligger det informasjon til den registrerte om muligheten til å trekke tilbake samtykke? |  |
| 7 | Omfatter samtykket alle databehandlinger og behandlingsformål som nevnt i kapitel 1? |  |

Samtykkeerklæring skal vedlegges

|  |
| --- |
| Eventuelle kommentarer:*Oppgi her* |

### Informasjon om behandlingen av personopplysninger

*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

[ ]  Generell informasjon om forskning i innkallingsbrev

[ ]  Informasjon på nett

[ ]  Nyhetsbrev

[ ]  Brev

[ ]  Sosiale medier

[ ]  Offentlig informasjonskampanje

[ ]  Annet, *spesifiser her:*

**Utarbeidet informasjonsmateriell skal vedlegges.**

|  |
| --- |
| Dersom relevant for prosjektet, oppgi lenke til informasjonen på nett:*Oppgi her**Dersom det er gitt/ skal gis fritak fra samtykke, bl.a. fordi det vil være uforholdsmessig krevende å innhente, vil det være relevant for vurderingen om det gis informasjon til de registrerte på annen måte. F.eks. om det gis informasjon på hjemmeside e.l. Dette vil kunne ivareta den registrertes rettigheter etter kap. III i forordningen* |

### Rett til innsyn, databehandlingsbegrensning, retting, sletting og portabilitet

Hvilke virkemidler er etablert for å ivareta de registrertes rett til innsyn, innsigelser (databehandlingsbegrensning), retting og sletting og (eventuelt) hvordan retten til dataportabilitet oppfylles, samt hvordan eventuelle krav som dataansvarlig mottar vil følges opp overfor databehandlere.

For de prosjektene som ikke har direkte personidentifiserbare data eller tilgang til koblingsnøkkel, skal henvendelser henvises til forvalter av eventuell koblingsnøkkel.

Følgende virkemidler er etablert, kryss av under:

[ ]  Kontaktinformasjon for innsynskrav – *skal stå i informasjonsskriv*

[ ]  Skjema for å be om innsyn – *kan utarbeides for forskningsprosjektet med egen innsamling*

[ ]  Retningslinje for behandling av innsynskrav (jf. EQS rutine *Ahus - Den registrertes rettigheter i kvalitets- og forskningsprosjekter*)

[ ]  Retningslinje for retting og sletting (jf. EQS rutine *Ahus - Den registrertes rettigheter i kvalitets- og forskningsprosjekter)*

 [ ]  Mal for standardsvar *– dette kan utarbeides ved planlagt tilbakemelding til deltakere eksempelvis om analyseresultat*

[ ]  Databehandleravtale med klausuler som sikrer de registrertes rettigheter – *aktuelt ved bruk av databehandler(e)*

[ ]  Annet, *beskriv her:*

### Ivaretakelse av de registrertes rettigheter og friheter

Personvernskonvensjonens fortale pkt. 4:

*«Behandling av personopplysninger bør ha som formål å tjene menneskeheten. Retten til vern av personopplysninger er ikke en absolutt rettighet; den må ses i sammenheng med den funksjon den har i samfunnet, og veies mot andre grunnleggende rettigheter i samsvar med forholdsmessighetsprinsippet.»*

|  |  |
| --- | --- |
| Vurder hvordan de registrertes friheter i forhold til Den europeiske menneskerettskonvensjonen (EMK) er tatt hensyn til:  | Svar (forklar svar) |
| Retten til privatliv og kommunikasjonsvern | *Dette punktet er mest aktuelt. Retten til privatliv følger både av EMK og av grunnloven. Her er det nok tilstrekkelig å vise at man er bevisst problemstillingen, evt. hvordan man søker å minimere en evt. krenkelse* |
| Retten til ikke å bli diskriminert | *Vurdere om det vil være sider av studien som vil kunne være/ oppfattes å være diskriminerende. F.eks. om man velger å gjøre en legemiddelstudie kun på barn, ikke voksne, slik at man potensielt ekskluderer en brukergruppe osv* |
| Tanke-, tros- og religionsfrihet |  |
| Ytrings-, og informasjonsfrihet |  |

## Personvernsprinsippene

|  |  |  |
| --- | --- | --- |
| Nr. | Vurderingsspørsmål | Svar (forklar svar) |
| 1 | Er behandlingen basert på lovlighet, rettferdighet og åpenhet (GDPR art.5.1 bokstav a og art.6 og 9)? |  |
| a. | Kommer det rettslige grunnlaget/databehandlingsgrunnlaget tydelig frem? | *F.eks. i samtykke- og/ eller informasjonsskriv* |
| b. | Vurder rimeligheten av databehandlingen: *Hva er forventede fordeler ved databehandlingen? For virksomheten, den registrerte, samfunnet for øvrig osv.* | *Fordeler opp i mot ulemper* |
| c. | Hva vil konsekvensene være dersom databehandlingene ikke gjennomføres? |  |
| 2 | Formålsbegrensninger |  |
| a. | Er formålet definert slik at det samsvarer med forventningene til de registrerte? | *Ut fra samtykke- og/ eller informasjonsskriv. Om det ikke er samtykket – hva forventer registrerte at disse opplysningene brukes til* |
| B | Har det vært vurdert andre alternativer for å oppnå formålet med behandlingen? | *Hvis ja, beskriv* |
| c. | Finnes det mindre personverninngripende alternativer for å oppnå det samme formålet?  | *Hvis ja, beskriv.* |
| 3 | Dataminimering.Kan formålet oppnås ved for eksempel: |  |
| a. | Begrense innsamling av personopplysninger? |  |
| b. | Med mindre detaljerte personopplysninger? |  |
| c. | Uten fortrolige eller sensitive personopplysninger? |  |
| Begrunn nødvendighet og relevans relatert til formål for alle opplysninger som behandles. |  |
| 4 | Riktighet |  |
|  | Vurder hvordan personopplysninger holdes korrekte og oppdaterte, med og uten den registrertes involvering. | *Er det gode rutiner for kvalitetskontroll. Korreksjoner fra den registrerte. Monitorering. Korrekte data. Ikke punsjefeil.* |
| 5 | Lagringsbegrensning |  |
| a. | Vurder om personopplysninger lagres etter at formålet er oppnådd og når opplysningene slettes. |  |
| b. | Vurder når personopplysninger anonymiseres eller pseudonymiseres som muliggjør videre lagring.  |  |
| c. | Vurder hvilke garantier som må være plass dersom personopplysninger skal lagres i lenger perioder grunnet arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål (GDPR art.89 nr.1).  | *F.eks. innhenting av nytt samtykke dersom behov for lengre lagring. Gjøre vurderinger underveis om det er behov for å lagre personopplysninger lengre?* |

|  |
| --- |
| Beskriv følgende tiltak som planlegges for å sikre formålsbegrensning og dataminimering: *Beskriv her**For eksempel: Dokumentasjon av hvilke data som hentes ut fra kliniske systemer, og at dette er i tråd med forskningsspørsmålet. Data må avidentifiseres, og kodeliste lagres på adskilt område fra dataene.* |

## 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)

|  |
| --- |
| Angi kriterier for fastsetting av varighet: *Her må det fastsettes en foreløpig slettedato eller dato for ny vurdering av behov for videre oppbevaring.* |

|  |
| --- |
| Beskriv lagringstid og dato for sletting/fjerning av direkte identifiserbare kjennetegn: |

|  |
| --- |
| Beskriv om det er vurdert ulik lagringstid for ulike data, både i prosjektperioden og av hensyn til etterprøving, i tilfelle hvordan er dette vurdert: *Dette har med formålsbegrensning og dataminimering å gjøre. Dvs. at prosjektleder bør være bevisst på om alle opplysningene er nødvendige gjennom hele studien og av hensyn til etterprøving, eller om enkelte opplysninger kan slettes tidligere. Opplysninger skal ikke behandles/lagres lengre enn nødvendig.* |

# 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; beskriv hvordan følgende har relevans for prosjektet:

|  |
| --- |
| Gi en samlet avklaring av de tre punktene under med tanke på potensielle konsekvenser; anslå alvorlighetsgrad, identifiser trusler og anslå sannsynlighet:1. Manglende reell medbestemmelse
2. Manglende reell åpenhet
3. Manglende forutsigbarhet
 |

## Tiltak

Beskriv tiltak for å håndtere risikoene for de registrerte og andre berørte personers rettigheter og berettigede interesser som du har identifisert i prosjektet.

|  |
| --- |
| Beskriv tiltak her:*Tiltak kan f.eks. innebære følgende:* * *spesifikke garantier for å minimere inngripe;*
* *spesifikke sikkerhetstiltak som angår personopplysninger som skal behandles;*
* *generelle sikkerhetstiltak som iverksettes på systemet hvor behandlingen utføres;*
* *organisatoriske tiltak (styring);*
* *informasjon i innkallingsbrevet om at opplysningene kan benyttes til forskningsprosjekter der det er gitt dispensasjon for samtykke;*
* *fjerne direkte identifiserbare kjennetegn;*
* *sletting etter et gitt antall år;*
* *lagring på godkjente lagringsområder;*
* *garantier: krav til fornyet samtykke, rett til reservasjon osv.;*
* *sikkerhetstiltak: tilgangskontroll, kryptering osv.;*
* *mekanismer: funksjonalitet som er personvernfremmende for eksempel logging og sperring av tilgang eller sperring av informasjon.*
 |

**Ut fra tiltakene beskrevet over, vurder følgende:**

|  |  |
| --- | --- |
| Ut fra tiltakene beskrevet over, vurder følgende:  | Forklar |
| Er sikringen av vernet av personopplysninger tilstrekkelig? |  |
| Er de registrertes og andre berørte personers rettigheter og berettigede interesser hensyntatt? |  |
| Er identifiserte risikoer håndtert og akseptable? |  |
| Er det restrisiko etter at alle planlagte tiltak er implementert? |  |

## Samlet vurdering av personvernet

|  |
| --- |
| Sammenfatt og vurder her:*Prosjektleder skal her gjøre en oppsummering av personvern og personopplysningssikkerheten.* |

# Brukermedvirkning

Som utgangspunkt skal man innhente synspunkter på databehandlingen fra de registrerte eller representanter for de registrerte når det er relevant. Dette kan eksempelvis være brukerutvalg, pasientforeninger, fokusgrupper, pasientombud, mv.

**Synspunkter er innhentet:**

[ ]  Nei

[ ]  Ja

|  |
| --- |
| Beskriv hvordan synspunkter er innhentet: |

# Involvering av personvernombudet og forhåndsdrøftelse med Datatilsynet – Del 5 fylles ut av personvernombudet og/eller Datatilsynet

## Personvernombudet

|  |
| --- |
| Vurdering fra personvernombudet:*Dette punktet skal fylles inn av personvernrådgiver* |

## Forhåndsdrøfting med Datatilsynet

Vurdering av hvorvidt Datatilsynet kontaktes for forhåndsdrøfting. Dette er aktuelt når prosjektet innebærer høy risiko for personvernet.

Prosjektet skal forhåndsdrøftes med Datatilsynet:

[ ]  Ja

[ ]  Nei

|  |
| --- |
| Begrunnelse for hvorfor prosjektet skal/ikke skal forhåndsdrøftes med Datatilsynet: |

|  |
| --- |
| Konklusjon:  |

## Plan for implementering av tiltak

|  |
| --- |
| De tiltak som er identifisert som hensiktsmessige for oppfølging av denne personvernkonsekvensvurderingen er følgende: |

|  |
| --- |
| Oppsummering av supplerende risikoreduserende tiltak fra risikoregisteret og tiltak fra eventuelt andre kapitler. |

For å ivareta personopplysningssikkerheten i prosjektet, vil følgende tiltak iverksettes:

|  |  |  |
| --- | --- | --- |
| Tiltak | Tidsfrist | Ansvar |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

DPIA godkjennes av avdelingsleder etter at tilrådning med aktuelle tiltak er gitt av PVO. Dokumentet sendes til godkjenning i P360.