PERSONVERNKONSEKVENSVURDERING (DPIA) I FORSKNING

Hilde K. Olav, juridisk rådgiver

Normkonferansen 2019

Kreft registeret

Forskning - begrep

- **Helseforskning;**

- **Medisinsk og helsefaglig forskning;** *Virksomhet som utføres med vitenskapelig metodikk for å skaffe til veie ny kunnskap om helse og sykdom, jf. hfl. § 4 bokstav a.*

- **Annen type forskning;** eks. **helsetjenesteforskning;** *Hvordan organisatoriske strukturer og prosesser, helseteknologi og personalatferd påvirker tilgang til helse- og omsorgstjenester, kvaliteten og kostnadene ved helse- og omsorgstjenester, og helse og velvære.*

Kreft registeret

Hva er personvernkonsekvensvurdering?

- **Systematisk prosess** som har som formål å **identifisere og evaluere mulige personvernkonsekvenser.**
- Skal gjennomføres **før** behandling av personopplysninger påbegynnes.
- Den behandlingsansvarlige skal **rådføre seg** med personvernombudet
- Kommer **i tillegg til** etisk forhåndsgodkjenning fra REK og evt. disp. fra taushetsplikt.

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

Kreft registeret

Når skal det gjennomføres en personvernkonsekvensvurdering?

- Sannsynlig at behandlingen vil kunne resultere i **høy risiko for individets rettigheter og friheter**, særlig ved bruk av ny teknologi, og i det det tas hensyn til behandlingens **art, omfang, formål og sammenhengen** den utføres i, *jf. art. 35 (1).*

- ***Særlig nødvendig**, jf. art. 35(3):*
  - *Behandling i **stor skala** av **særlige kategorier av personopplysninger,** jf. art. 35 (3) b.*

Kreft registeret

Når skal det gjennomføre en personvernkonsekvensvurdering forts.?

- Personvernkonsekvensvurdering kan være nødvendig for **enkeltprosjekter** og for **behandlinger som har generelle forskningsformål**, for eksempel opprettelse av helseregister.

- Datatilsynet kan bestemme at enkelte behandlingsaktiviteter skal være omfattet av kravet til DPIA, og har bestemt at det er krav om å gjennomføre en personvernkonsekvensvurdering, *jf. art. 35(4):*
  - ***Ikke-samtykkebasert behandling av særlige kategorier av personopplysninger for forskningsformål.***
  - ***Se Datatilsynets liste*** ***https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=10360***

Kreft registeret

Når skal det *ikke* gjennomføres en personvernkonsekvensvurdering?

- Behandlingen er **veldig lik en behandling** det allerede er gjennomført en vurdering av personvernkonsekvenser for. I slike situasjoner kan resultatet fra den foreliggende vurderingen for lignende behandlinger brukes.
- Prosjektet har **konsesjon fra Datatilsynet** før juli 2018 og betingelsene ikke har endret seg.
- Behandlingen er **regulert i nasjonal rett**, og det er **gjennomført en vurdering av personvernkonsekvenser** som ledd i utarbeidelse av rettsgrunnlaget (jf. art. 35 nr. 10). *Eks. Utlevering av indirekte identifiserbare helseopplysninger fra lovbestemte helseregistre med hjemmel i helseregisterloven § 20*.
- Se også Datatilsynets liste https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=10360

Kreft registeret

Nærmere om innholdet i vurderingen

- **Minimumskrav**, *jf. art. 35 (7):*

  - **Systematisk beskrivelse** av den planlagte behandlingen og **formålene** med behandlingen.

  - Vurdering av **nødvendighet og forholdsmessighet** av behandlingen i lys av formålene.

  - Vurdering av risiki for **registrertes friheter og rettigheter.**

  - **Risikoreduserende tiltak** som skal iverksettes.

Kreft registeret

Hvem skal gjennomføre personvernkonsekvensanalyse?

- **Behandlingsansvarlig** er ansvarlig for at DPIA gjennomføres og at regelverket etterleves.

- Det **overordnede ansvaret** ligger hos **øverste leder.**

- Det **daglige ansvaret** for helseforskningsprosjekter ligger hos **prosjektleder.**

Kreft registeret

Maler

- Mal for gjennomføring for DPIA https://ehelse.no/personvern-og-informasjonssikkerhet/verktoy-for-implementering-av-gdpr
- Mal for gjennomføring av DPIA https://ehandboken.ous-hf.no/document/131984
- Egenerklæring https://nettskjema.no/a/dpia
- Prosedyre https://ehandboken.ous-hf.no/document/131979/fields/23

Kreft registeret

Systematisering mal OUS

- I Behandling av personopplysninger i prosjektet
  Formål, datakilder, registrerte, kategorier av personopplysninger, lagringssted og lagringsmedier, dataansvarlig, datatilgang og databehandlere, overføring av personopplysninger til andre land og/eller internasjonale organisasjoner, adferdsnormer.
- II Rettslig grunnlag for behandling av personopplysninger
  Rettslig grunnlag for behandling av særlige kategorier av personopplysninger, formålsbegrensning og dataminimering, lagring, de registrertes rettigheter.
- III Personvern, risikoanalyse og tiltak
  Medbestemmelse, åpenhet, forutsigbarhet, tiltak, samlet vurdering av personvernet.
- IV Involvering og drøftelser
  De registrerte, dataforvaltere, personvernombud, forhåndsdrøfting med DT, plan for implementering av tiltak.
- V Godkjenning
  Forskningsansvarlig

Kreft registeret

Fastsettelse av rettslig grunnlag

- Behandling av **særlige kategorier av personopplysninger** må ha lovlig grunnlag **både** i art. 6 nr. 1 og art. 9. nr. 2.

- Evt. **supplerende rettsgrunnlag** i nasjonal rett, *jf. art. 6 nr. 3*.
  - ***Art. 6 nr. 1 bokstav e* (nødvendig for å utføre en oppgave i allmennhetens interesse)**
- **Unntak fra forbudet** mot å behandle helseopplysninger må være fastsatt i nasjonal rett, (jf. art. 9 nr. 2)

Kreft registeret

Fastsettelse av rettslig grunnlag forts.

- Aktuelle **unntak** for behandling av **særlige kategorier av personopplysninger** i forskning, *jf. art. 9 nr. 2*:
  - Samtykke (bokstav a) – **hovedregel i forskning**
  - Viktige allmenne interesser (bokstav g)
  - Forebyggende medisin, medisinsk diagnostikk, yting av helsetjenester (bokstav h)
  - Allmenne folkehelsehensyn for å sikre høye kvalitets- og sikkerhetsstandarder for helsetjenester (bokstav i)

Kreft registeret

Eks. supplerende rettsgrunnlag i forskning

- *Hfl §35 (Adgang til bruk av helseopplysninger som er innsamlet i helsetjenesten til forskning)*
- *Hpl § 29 (Tilgjengeliggjøring til bruk for forskning)*
- *Hregl § 20 (Unntak fra taushetsplikten for indirekte identifiserbare opplysninger til forskning)*
- *Pol § 8 (Behandling av personopplysninger for formål knyttet til vitenskapelig forskning)*
- *Pol § 9 (Behandling av personopplysninger uten samtykke for formål knyttet til vitenskapelig forskning*

- Kan være **flere supplerende rettsgrunnlag** og **bestemmelser som gir unntak fra forbudet mot å behandle helseopplysninger** i et forskningsprosjekt.
  Typisk; Skal behandle både helseopplysninger om deltakere, fra flere lovbestemte helseregistre, sosioøkonomiske opplysninger fra SSB.

Kreft registeret

Dataminimeringsprinsippet

- Personopplysninger skal være **adekvate, relevante og begrenset til det som er nødvendig for formålene** de behandles for, *jf. art. 5 (1) c*.

- ***Store datasett – mange variabler – kan være bakveisidentifiserbart selv om personopplysningene er pseudonymiserte.***

- *<u>Vurderinger:</u> Nødvendig med fødselsnummer eller nok med fødselsdato evt. kun måned og fødselsår – eller kan fødselsdag erstattes med den 15. i hver måned eller bare måned og år?*

Kreft registeret

Vurdering av risiko for registrertes rettigheter

- Hvis ikke risikoen kan håndteres av BA på en tilfredsstillende måte, skal **forhåndsdrøftelser** med DT igangsettes, *jf. art. 36.*
- **Informasjon**, *jf. art. 13 og 14*
- **Innsyn**, *jf. art 15*
- **Begrensning av behandling**, *jf. art. 18*
- **Retting og sletting**, *jf. art. 16*
- **Sletting**, *jf. art. 17*

  - *Unntak:* ***Innsyn, retting og begrensning av behandling,*** *jf. pol § 17*
    Sletting, *jf. art. 17 nr. 3*

Kreft registeret

Informasjon – fortalepunkt 63

- En registrert bør ha **rett til å få innsyn i personopplysninger som er samlet inn om vedkommende**, og til på **en enkel måte og med rimelige intervaller** å utøve denne retten for å **forvisse seg om og kontrollere at behandlingen er lovlig**. Dette omfatter de registrertes rett til å få innsyn i egne helseopplysninger, f.eks. opplysninger i egen pasientjournal om diagnoser, undersøkelsesresultater, behandlende leges vurderinger og enhver behandling som er gitt, eller enhver intervensjon som er utført. Alle registrerte bør derfor ha rett til å kjenne til og bli informert **om formålene med behandlingen** av personopplysninger, om mulig om **perioden som personopplysningene behandles i**, **hvem mottakerne av personopplysningene er, logikken som ligger bak en eventuell automatisk behandling** av personopplysningene, og konsekvensene av nevnte behandling, i det minste dersom den er basert på profilering. Dersom det er mulig, bør den behandlingsansvarlige kunne gi **fjerntilgang til et sikkert system** der den registrerte kan få direkte tilgang til egne personopplysninger.

Kreft registeret

Risikoreduserende tiltak

- *Art. 89 nr. 1 – **Nødvendige garantier** som skal sikre at det er innført tekniske og organisatoriske tiltak for særlig å sikre at prinsippet om **dataminimering** overholdes.*

  - Pseudonymisering evt. anonymisering hvis mulig.

  Andre risikoreduserende tiltak:
  - Kryptering
  - Fuzzifisering (matematisk metode som kan brukes for å ytterligere redusere bakveisidentifisering)

Kreft registeret

Oppsummering

- Behandling av helseopplysninger innebærer alltid en **høy risiko** for individets rettigheter og friheter.
- Personvernkonsekvensanalyse SKAL gjennomføres med mindre et av unntakene kommer til anvendelse.
- DB skal rådføre seg med PVO i forbindelse med utførelsen av en vurdering om DPIA.
- DPIA skal godkjennes av forskningsansvarlig.
- Behandlingsaktivitetene skal dokumenteres.

Kreft registeret