

# **Personvern og informasjonssikkerhet i forsknings- og kvalitetsprosjekter**

Versjon 3.0

Juni 2023

Denne veilederen er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Normen forvaltes av Styringsgruppen for Normen, etter Normens forvaltningsmodell.

Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt. Innbyggere og ansatte skal være trygge på at opplysninger om dem behandles på en sikker måte i helse- og omsorgssektoren. Normen skal bidra til å at virksomheter i helse- og omsorgssektoren kan ha gjensidig tillit til hverandre, ved å etablere mekanismer og regler som sørger for at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Alt om Normen, Normens krav og veiledningsmateriell finnes på [www.normen.no](http://www.normen.no).

En til enhver tid oppdatert versjon av veilederen finnes på [www.normen.no](http://www.normen.no). Dersom du har spørsmål knyttet til veilederen kan du sende spørsmål og kommentarer til:

[sikkerhetsnormen@ehelse.no](mailto:sikkerhetsnormen@ehelse.no)

# Innhold

<b>1. Innledning</b>	<b>6</b>
1.1 Bakgrunn og tema for veilederen	6
1.2 Målgruppe	7
1.3 Avgrensninger	7
1.4 Utvikling av veilederen	7
1.5 Leseveiledning	7
<b>2. Flytskjema for planlegging av prosjekt</b>	<b>8</b>
<b>3. Formål</b>	<b>10</b>
<b>4. Data</b>	<b>11</b>
<b>5. Personopplysninger</b>	<b>12</b>
5.1 Skal du behandle personopplysninger?	12
5.2 Anonyme opplysninger	15
5.2.1 Om anonyme opplysninger	15
5.2.2 Anonymiseringsprosessen og de vanligste risikoene	16
<b>6. Roller og ansvar</b>	<b>17</b>
6.1 Hvorfor er det viktig å avklare roller og ansvar i et prosjekt?	17
6.2 Dataansvarlig institusjon	17
6.3 Når flere institusjoner har felles dataansvar	18
6.4 Databehandler	18
6.5 Prosjektleders ansvar	19
<b>7. Type prosjekt og behandlingsgrunnlag</b>	<b>19</b>
7.1 Hvordan henger type prosjekt og behandlingsgrunnlag sammen?	19
7.2 Type prosjekt	20
7.2.1 Definisjon av type prosjekt	20
7.2.2 Noen vanlige gråsoner	21
7.3 Tabell: prosjekttype og behandlingsgrunnlag	23
7.4 Hva er et behandlingsgrunnlag?	23
7.5 De mest aktuelle behandlingsgrunnlagene etter personvernforordningen	24
7.5.1 Den registrertes samtykke til behandling av personopplysninger	24
7.5.2 Nødvendig for å utføre en oppgave i allmennhetens interesse	28
7.5.3 Nødvendig for å oppfylle en rettslig forpliktelse	28
7.6 De mest aktuelle unntakene fra forbudet mot behandling av personopplysninger i særlig kategori	28

7.6.1	Nødvendig for arkivformål, forskning og statistikk.....	28
7.6.2	Nødvendig for forebyggende medisin, yting og/eller forvaltning av helsetjenester mm. ....	29
7.6.3	Nødvendig av hensyn til viktige allmenne interesser .....	29
7.6.4	Nødvendig av allmenne folkehelsehensyn.....	29
7.6.5	Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte selv har offentliggjort .....	29
7.7	Unntak fra forbudet mot å behandle personopplysninger om straffedommer og lovovertridelser .....	30
7.8	Supplerende rettsgrunnlag .....	30
7.8.1	Personopplysningsloven § 8 – behandlingen av personopplysninger er nødvendig for arkivformål, forskning og statistikk .....	30
7.8.2	Personopplysningsloven § 9 – særlige kategorier personopplysninger er nødvendig for arkivformål, forskning og statistikk .....	31
7.8.3	Personopplysningsloven § 11 – unntak fra forbudet mot å behandle personopplysninger om straffedommer og lovovertridelser .....	32
7.8.4	Helseregisterloven § 19b – vedtak fra Helsedataservice om tilgjengeliggjøring av helseopplysninger fra lovbestemte helseregistre .....	32
7.8.5	Helsepersonelloven § 29 og helseregisterloven § 19e – vedtak om dispensasjon fra taushetsplikten.....	33
7.8.6	Pasientjournalloven § 6 og helsepersonelloven § 26 – intern kvalitetssikring	33
7.8.7	Forskrift om medisinske kvalitetsregistre .....	34
7.8.8	Forskrift om befolkningsbaserte helseundersøkelser .....	34
7.8.9	REK-godkjenning etter helseforskningsloven gir ikke behandlingsgrunnlag	35
<b>8.</b>	<b>Dataflyt og sikkerhet .....</b>	<b>36</b>
<b>9.</b>	<b>Dele data? .....</b>	<b>37</b>
9.1	Hva vil det si å dele data? .....	37
9.2	Hvilke mottakere skal data deles med, for hvilke formål? .....	37
9.3	Dele personopplysninger eller anonyme opplysninger?.....	37
9.4	Når du skal dele personopplysninger for prosjektformålet .....	38
9.5	Når du eller andre skal bruke personopplysninger fra prosjektet til andre formål ..	39
<b>10.</b>	<b>Varighet – Hva skjer med personopplysningene etter prosjektslutt?.....</b>	<b>40</b>
10.1	Hvor lenge er det nødvendig å behandle personopplysninger i prosjektet? .....	40
10.2	Hvordan skal du håndtere personopplysningene etter prosjektslutt? .....	41
10.2.1	Sletting .....	41
10.2.2	Anonymisering .....	41
10.2.3	Viderebehandling .....	42
10.3	Publisering .....	42

<b>11. Informasjon til den registrerte</b> .....	<b>43</b>
11.1 Prosjektet er forpliktet til å gi den registrerte informasjon .....	43
11.2 Når skal prosjektet gi informasjon? .....	43
11.3 Unntak fra retten til informasjon .....	44
<b>12. Den registrertes rettigheter</b> .....	<b>45</b>
<b>13. Personvernkonskvensvurdering (DPIA)</b> .....	<b>47</b>
<b>14. Tillatelser</b> .....	<b>49</b>
14.1 Oversikt over tillatelser .....	49
14.2 Noen tips til søknadsprosessen .....	51
<b>15. Etabler nødvendige avtaler</b> .....	<b>51</b>
15.1 Hvilke avtaler trenger du? .....	51
15.2 Avtale om felles dataansvar .....	52
15.3 Databehandleravtale .....	52
15.4 Andre avtaler som kan være relevante .....	52
<b>16. Dokumentasjon</b> .....	<b>53</b>
<b>17. Klart for datainnsamling</b> .....	<b>53</b>
<b>18. Endringer og vurderinger underveis i prosjektet</b> .....	<b>53</b>
<b>Vedlegg 1: Definisjoner</b> .....	<b>54</b>
<b>Vedlegg 2: Flytskjema og steg-for-steg veiledning til flytskjema</b> .....	<b>55</b>
Formål .....	56
Data	57
Personopplysninger? .....	58
Roller og ansvar .....	59
Type prosjekt og behandlingsgrunnlag .....	60
Dataflyt og sikkerhet .....	63
Dele data? .....	63
Varighet. Hva skjer med personopplysningene etterpå? .....	65
Informasjon til den registrerte .....	66
Registrertes rettigheter .....	67
Personvernkonskvensvurdering (DPIA) .....	68
Tillatelser .....	69
Avtaler .....	71
Dokumentasjon .....	72
Klart for datainnsamling .....	72

# 1. Innledning

## 1.1 Bakgrunn og tema for veilederen

Ved oppstart av forsknings- og kvalitetsprosjekter i helse- og omsorgssektoren er det mange regler og instanser å forholde seg til. For en prosjektleder som har fokus på “komme i gang” kan dette fort bli en krevende øvelse. For hvordan går man egentlig frem for å sikre personvern og informasjonssikkerhet i prosjektet på en mest mulig effektiv måte? Og hvorfor må man i det hele tatt følge så mange regler for å gjennomføre et prosjekt som kan besvare viktige samfunnsspørsmål og bør være i alles interesse?

I forsknings- og kvalitetsprosjekter er det ofte nødvendig å behandle personopplysninger for å oppnå prosjektformålet. Dette innebærer et inngrep i privatlivet til “de registrerte”. For å ivareta deres behov og interesser, må prosjektene følge personvern- og helselovgivningen. Det kan være litt arbeidskrevende, særlig i planleggingsfasen. Men det er viktig å huske at alle prosjekter er tjent med å følge regelverket, og at dette regelverket er utformet slik at det ikke bare ivaretar de registrerte, men også behovene for forskning og kvalitetssikring.

Når forsknings- og kvalitetsprosjekter følger reglene og sikrer godt personvern og informasjonssikkerhet, gir det høy tillit i befolkningen. Høy tillit fører gjerne til at flere vil delta i prosjekter og at datakvaliteten øker. God planlegging bidrar også til at man får gjennomført forskningen eller kvalitetssikringen slik man ønsker, på lovlig måte.

Alle prosjekter som behandler personopplysninger må følge personvernforordningens prinsipper og ivareta de registrertes rettigheter. Prosjektene må blant annet sikre et tydelig og avgrenset formål, lovlig behandlingsgrunnlag, dataminimering, lagringsbegrensning og god informasjonssikkerhet og lagringsbegrensning. Det er viktig med klarhet i roller og ansvar, særlig der flere institusjoner er involvert i prosjektet. Og det er viktig å identifisere “type prosjekt” og hvilke data man trenger, for å finne ut hvilke lover man må følge, og om man må innhente ulike tillatelser.

Denne veilederen beskriver hvordan en prosjektleder kan gå frem for å planlegge og gjennomføre et prosjekt med forsknings- eller kvalitetsformål i samsvar med lovpålagte krav til personvern og informasjonssikkerhet. Formålet er med andre ord å gi deg som prosjektledere praktisk veiledning som gjør deg bedre rustet til å ivareta kravene til personvern og informasjonssikkerhet, uavhengig av hvilken tilgang du har til forskningsstøtte og andre veiledningsressurser i virksomheten.

Veilederen tar prosjektlederens perspektiv, og er bygget som en bruksanvisning eller sjekkliste, med utgangspunktet i det pragmatiske spørsmålet “Jeg skal starte opp et prosjekt, hva må jeg gjøre?”. Veilederen forklarer hvilke steg du som prosjektleder bør ta i planleggingen av prosjektet, og i hvilken rekkefølge, og gir deg praktiske råd og anbefalinger. Innledningsvis i veilederen finner du et flytskjema, og i vedlegg 2 en steg-for-steg-veiledning til dette flytskjema. Flytskjema med steg-for-steg-veiledningen kan du bruke som sjekkliste etter å ha lest veilederen, ettersom flytskjemaet følger de samme stegene som veilederen.

Veilederen vil være nyttig ved oppstart av ulike prosjektyper som helseforskning, annen forskning, kvalitetssikring og ved etablering av medisinske kvalitetsregistre eller befolkningsbaserte helseundersøkelser.

## 1.2 Målgruppe

Målgruppen for veilederen er prosjektledere i forsknings- og kvalitetsprosjekter i helsesektoren. Men den vil også være nyttig for prosjektledere i forskningsprosjekter utenfor helsesektoren, og for prosjektmedarbeidere, forskningsstøttefunksjoner, personvernressurser og ledere ved institusjoner som driver forskning og kvalitetssikring.

Videre er veilederen rettet mot virksomheter som omfattes av Normen og som skal sikre etterlevelse av Normens krav, herunder dataansvarlig.

## 1.3 Avgrensninger

Når anbefalingene i veilederen tas i bruk i virksomheten, må de tilpasses med utgangspunkt i virksomhetens kompleksitet og størrelse, samt konkrete behov og oppgaver.

Veilederen vil ikke behandle spørsmål knyttet til forskningsetikk eller immateriell rett, som f.eks. eierskap til data og resultater, forfatterskap og patentering mv.

## 1.4 Utvikling av veilederen

Dette er en revidert utgave av Normens veileder i personvern og informasjonssikkerhet i forskningsprosjekter. Revisjonen har tatt sikte på å gjøre veilederen mer brukervennlig. Det er også laget et flytskjema med steg-for-steg-veiledning i forsknings- og kvalitetsprosjekter, som du finner i kapittel 2 og i vedlegg.

Både revisjonen av denne veilederen og flytskjema med steg-for-steg-veiledning er utarbeidet i samarbeid med Sikt – Kunnskapssektorens tjenesteleverandør, som på oppdrag fra Kunnskapsdepartementet leverer fellestjenester til kunnskapssektoren, blant annet innen personvern og informasjonssikkerhet.

I arbeidet med utviklingen av flytskjema med steg-for-steg-veiledningen, er det samlet inn verdifulle innspill fra en arbeidsgruppe bestående av en sammensatt gruppe med kompetanse og god kjennskap til helse- og omsorgssektoren, blant annet innen forskning og forskningsstøtte, samt helse- og personvernlovgivningen. Det er videre samlet inn gode innspill fra Datatilsynet, Helsedirektoratet, Helsedataservice, Statens legemiddelverk, REK/NEM og SKDE – Nasjonalt servicemiljø for medisinske kvalitetsregistre. Alle disse innspillene har også blitt brukt i arbeidet med revisjonen av veilederen.

## 1.5 Leseveiledning

I denne veilederen henvender vi oss til deg som skal starte opp et forsknings- eller kvalitetsprosjekt innen helse- og omsorgssektoren.

Ved å følge stegene i forskningsveilederen får du oversikt over hva du må tenke på når det gjelder personvern og informasjonssikkerhet i prosjektet. Veilederen følger stegene i forskningsprosessen, slik at den skal være enkel å bruke.

Veilederen er ganske omfattende, men du kan bruke den som et oppslagsverk. Det kan være lurt å bruke innholdsfortegnelsen aktivt for å finne frem til det du trenger informasjon om. Du kan også bruke Ctrl+F for å søke i dokumentet. Videre er det gjennomgående vist til annet veiledningsmateriale der dette er relevant.

Du kan også bruke flytskjemaet i kapittel 2 sammen med «Steg-for-steg veiledningen til flytskjemaet» i vedlegg 2, som en sjekklister eller leseveiledning.

## 2. Flytskjema for planlegging av prosjekt

Din institusjon har ansvaret for å sikre og påvise at personvern- og helselovgivningen er fulgt i prosjektet. Vær oppmerksom på at institusjoner kan ha ulike rutiner og systemer for å dokumentere at deres forskning og kvalitetssikring er lovlig, og at du må følge retningslinjer ved din institusjon. Mange institusjoner kan f.eks. ha rutine for innmelding av prosjekter og forskningsstøtte du kan rådføre deg med, og/eller bruker personverntjenester som Sikt. Uansett rutiner ved din institusjon, vil forskningsveilederen fungere som støtte og veiledning.

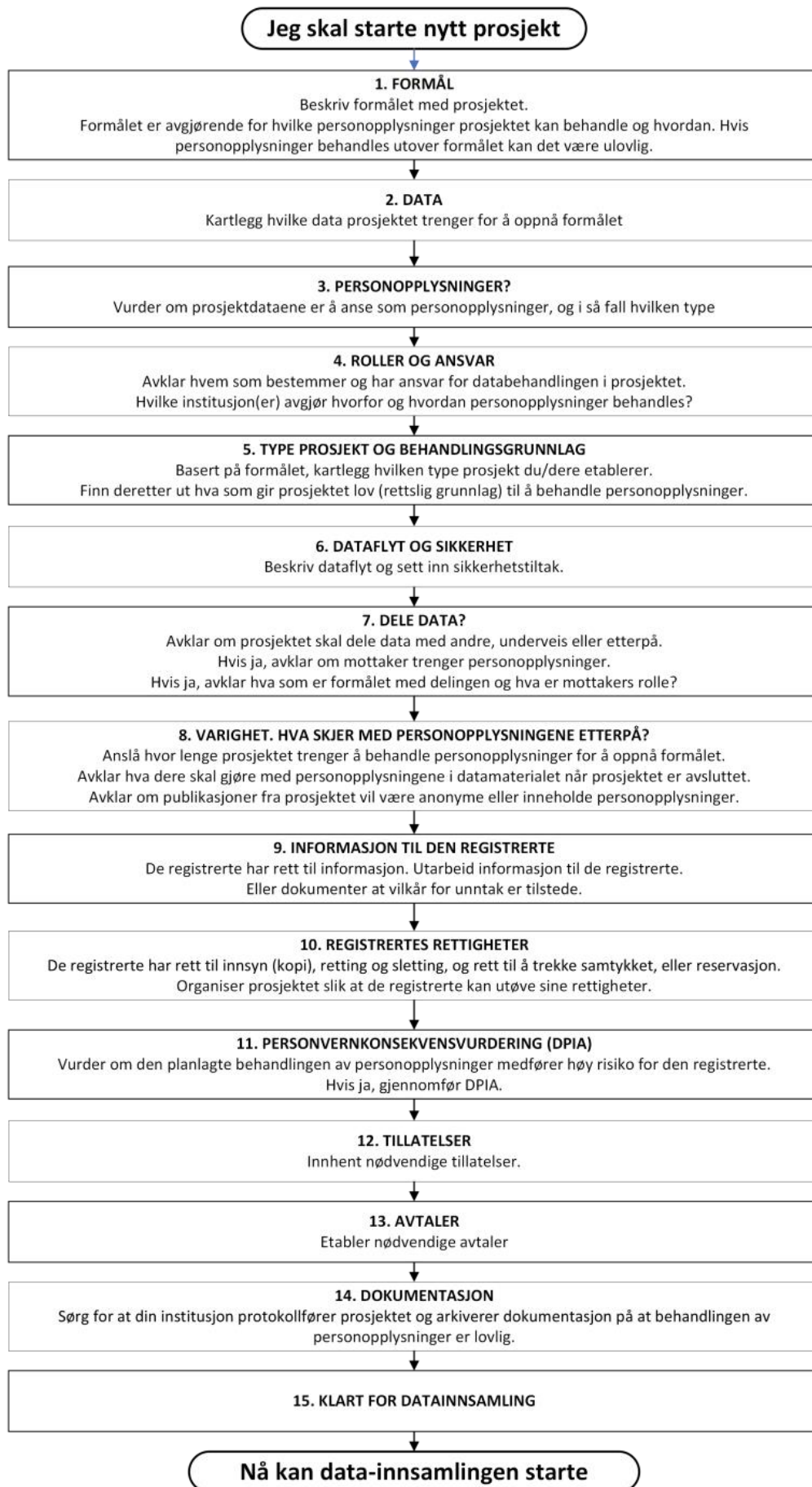
Når du bruker forskningsveilederen i prosjektet ditt, anbefaler vi at du er grundig i beskrivelse og vurdering i hvert punkt. Dette for å unngå følgefeil i de neste stegene, og risiko for ulovlig behandling av personopplysninger. Husk at du må gå igjennom alle stegene før du starter behandlingen av personopplysninger.

Hvis du skulle oppdage avvik i planleggingsfasen, f.eks. hvis du har startet behandling av personopplysninger og hoppet over et av stegene, er det viktig at du sier ifra til institusjonen din så raskt som mulig. Dette fordi institusjonen – for noen typer avvik – har en 72 timers frist på å melde fra til Datatilsynet.

Før du går i gang med datainnsamling må prosjektet ha på plass nødvendige tillatelser og avtaler, samt personvernkonsekvensvurdering (DPIA) hvis dette er et krav. Det kan være lurt å starte disse prosessene så tidlig som mulig. Disse tre stegene er likevel plassert til slutt i veilederen, fordi det er viktig at du først har god oversikt over ulike forhold ved prosjektet. Vår anbefaling er at du leser igjennom hele veilederen og skisserer stegene i oppsatt rekkefølge for ditt prosjekt. Alternativt kan du bruke veilederen parallelt med at du utarbeider søknader, går i dialog med samarbeidspartnere og evt. begynner på DPIA. Det viktigste er at du fullfører alle stegene før søknader sendes, avtaler inngås og DPIA sendes til godkjenning.

Veilederen følger hovedsakelig stegene i dette flytskjemaet.





## 3. Formål

Når du planlegger et nytt prosjekt, anbefaler vi at du starter med å beskrive formålet. Formålet er avgjørende, både for hvilke personopplysninger prosjektet kan behandle og på hvilken måte. Hvordan du beskriver formålet vil dermed være førende for alle vurderingene du skal gjøre videre før du starter datainnsamlingen, og vil legge premissene for hele gjennomføringen av prosjektet. Før oppstart er det viktig å være klar over at manglende samsvar mellom formålet og hvordan personopplysninger behandles kan være ulovlig, og at det kan være både vanskelig og tidkrevende å endre eller utvide formål senere i prosjektet. Sistnevnte gjelder særlig hvis det er vanskelig å komme i kontakt med prosjektdeltakerne igjen etter at data er samlet inn. Da har man få muligheter for å informere deltagerne, og evt. innhente samtykke, til endringene.

Begynn derfor med å tenke godt igjennom – og formulere – hvorfor prosjektet skal gjennomføres. Det vil variere fra prosjekt til prosjekt hvilke rammer man har å forholde seg til. I prosjekter som utføres på oppdrag, vil gjerne oppdragsgiver legge noen føringer som formålsbeskrivelsen må være innenfor. I prosjekter som starter opp på eget initiativ, står man kanskje noe "friere" i å definere formålet.

Uansett hvilke rammer prosjektet har, anbefaler vi at du er grundig med formålsbeskrivelsen. Den trenger ikke nødvendigvis være lang, men den må være konkret og presis. Den må definere en klar problemstilling (eller flere), og gjerne oppsummere de mest sentrale spørsmålene du vil undersøke i prosjektet. Det er nemlig et krav i personvernregelverket at formålet må være "*klart definert, nøyaktig, fullstendig og rimelig*". Med "fullstendig" menes at alle formål for behandlingen av personopplysninger må være beskrevet og at hvert formål må være tydelig definert. Med "rimelig" menes i denne sammenheng at formålet må være forståelig og ligge innenfor det man vil forvente av en institusjon som driver forskning og kvalitetssikring.

Formålet må også være så *spesifikt* som mulig. Innenfor forskning og kvalitetssikring er det ikke alltid mulig å identifisere formålet fullt ut ved oppstart av datainnsamling. Det kan i noen tilfeller være vanskelig, kanskje u hensiktsmessig, å planlegge alle problemstillinger og spørsmål ned til minste detalj. Det gjelder særlig i større studier og forsknings-/kvalitetsregistre der data samles inn for å gi grunnlag til flere delprosjekter med ulike problemstillinger. Personvernregelverket tar høyde for dette, og åpner for at formålet da kan beskrives noe bredere og mer overordnet. Formålsbeskrivelsen må likevel være så presis og konkret som mulig. Hvor konkret den må være, avhenger av prosjektets (eller registerets) karakter. De helt overordnede begrepene "forskning" og "kvalitetssikring" vil uansett være for vide som formålsbeskrivelse, da de ikke sier noe om hvilke typer problemstillinger som skal undersøkes. Formålet må altså avgrenses noe, gjerne tematisk til et forskningsområde. Eksempler på slike brede, men likevel avgrensede formål kan være kreftforskning, kvalitetssikring av helsehjelp ved hjerte-/karsykdom, forskning på befolkningshelse el.

Merk også at formålsbeskrivelsen skal fokusere på den faglige problemstillingen og spørsmålene som prosjektet skal besvare. Det er som regel unødvendig og lite hensiktsmessig å ta inn beskrivelser av hvilke data prosjektet skal samle inn og forklaringer av fremgangsmåte og metode, ettersom disse sidene ved prosjektet uansett skal beskrives i de neste stegene. Det kan selvsagt være unntak der det er nødvendig å forklare om metode i selve formålsbeskrivelsen, for eksempel hvis formålet er å teste ut en bestemt metode.

## 4. Data

Etter at du har beskrevet formålet, anbefaler vi at du kartlegger hvilke data prosjektet vil trenge for å oppnå formålet. Tenk godt over og beskriv hvilket datamateriale du planlegger å samle inn. Beskrivelsen må si noe om utvalget (eller utvalgene), datakildene, og om innhold og omfang på datamaterialet.

Om utvalget beskriver du hvilke kategorier av personer prosjektet skal samle opplysninger om. Her kan det være lurt å kort liste opp utvalgskriteriene, og forklare hvordan du vil gå fram for å rekruttere eller trekke utvalget. Hvis det er flere utvalg, husk å beskrive alle.

Når du har definert utvalget/utvalgene, er det viktig å ta stilling til om noen av de du vil innhente opplysninger om er å anse som sårbare personer. Med "sårbare" mener vi i denne sammenhengen personer som kan ha vansker med å ivareta rettighetene sine. Det kan skyldes ulike forhold, som sykdom, livssituasjon, eller at de står i en skjev maktrelasjon til deg eller institusjonen som er ansvarlig for forskningen/kvalitetssikringen, eller den institusjonen de rekrutteres gjennom. Barn, pasienter, asylsøkere og ansatte er eksempler på sårbare grupper, men også mange andre personer eller grupper kan være sårbare. Du må foreta en konkret vurdering av om utvalget i prosjektet omfatter slike. Husk at graden av sårbarhet kan avhenge av kontekst. For eksempel kan en person være sårbar som ansatt overfor arbeidsgiveren, men ikke på fritiden overfor andre. Husk også at sårbarhet ikke bare kan skyldes permanente forhold (som medfødt kognitiv funksjonsnedsettelse), men også forbigående forhold (som akutt sykdom eller arbeidsløshet). Sårbarhet er altså ikke noe som kun gjelder enkelte deler av befolkningen. Alle mennesker kan befinne seg i situasjoner som gjør dem sårbare når det kommer til spørsmål om deltagelse i forskning og kvalitetssikring og behandling av personopplysninger. Det avgjørende for om personene du forsker på er sårbare, er altså om de av en eller annen grunn kan ha vansker med å ivareta egne rettigheter. Med "ivaretagelse av egne rettigheter" mener vi her at personene kan ha vansker med å forstå hva prosjektet innebærer og konsekvensene av deltagelse; at de kan oppleve det vanskelig å si nei til deltagelse, oppleve et press om å delta, eller tro at de må delta i forskningen/kvalitetssikringen for å kunne motta helsehjelp; eller at de i etterkant av deltagelse kan vegre seg mot å ta kontakt for å be om mer informasjon, innsyn, retting og sletting, f.eks. fordi de står i et avhengighetsforhold og ikke vil ødelegge for prosjektet.

Når det gjelder datakilder, beskriver du hvor og hvordan du skal innhente data til prosjektet. Et viktig hovedskille, som gjerne vil påvirke vurderingene du skal gjøre senere, er om du samler inn data direkte fra forskningsdeltakeren ("den registrerte"), eller om du samler inn data om dem fra andre kilder. Dette må derfor fremgå tydelig av beskrivelsen. Det må også fremgå hvilke metoder du bruker til datainnsamlingen. Hvis prosjektet skal ha direkte kontakt med deltakerne: skal du da samle inn data ved intervju, spørreskjema, observasjon, medisinske eller andre tester, biologiske prøver, eller på annen måte? Hvis prosjektet samler inn data om personer fra andre kilder: skal du da innhente opplysningene fra pasientjournal, helseregistre eller andre registre, SSB, en institusjon, et annet forskningsprosjekt, medisinsk utstyr, eller på annen måte? Det er også viktig å beskrive om du skal kombinere metoder, slik at du samler data om de samme personene gjennom flere datakilder og kobler dataene på individnivå. I så fall må du beskrive konkret hvordan du går frem for å samle dataene,

hvordan du skal foreta koblingen, og hvilket datamateriale som vil inngå om de registrerte i prosjektet (se kapittel 8 om dataflyt og sikkerhet).

Du må også si noe om innhold og omfang av dataene i prosjektet. I beskrivelsen av innhold, tar du utgangspunkt i formålet og datakilden, og forklarer hvilke konkrete opplysninger som trengs for å svare på problemstillingen(e) i prosjektet. I beskrivelsen kan du ta inn – eller vedlegge – det som er aktuelt av intervjuguide, spørreskjema, observasjonsguide, variabelliste og/eller beskrivelse av hvilke data som registreres gjennom medisinske forsøk, biologiske prøver, måleinstrumenter, teknologisk utstyr etc. Viktige momenter for å beskrive datamaterialets omfang vil være å anslå omtrent hvor mange personer det skal samles inn data om, antall og detaljgrad på variabler, og hvor ofte opplysninger skal innhentes (frekvens). Det kan også være hensiktsmessig å skissere det geografiske omfanget, f.eks. om data samles inn om et representativt utvalg av Norges befolkning, om alle ved en arbeidsplass, eller et tilfeldig utvalg fra en kommune.

Hvis prosjektet skal knytte opplysningene til enkeltpersoner (se neste avsnitt), er det noen ting du må være oppmerksom på, som f.eks. prinsippet om dataminimering. Prosjektet kan bare samle inn opplysninger som er adekvate og relevante for formålet. Det er altså ikke tillatt å innhente overskuddsinformasjon "i tilfelle det skulle vise seg å bli nyttig". Du må se datainnsamlingen i lys av formålsbeskrivelsen. For å få med de dataene du trenger, er det viktig at du har beskrevet formålet presist og dekkende.

Vær også oppmerksom på at hvis du henter data fra andre kilder (ikke direkte fra den registrerte), må den institusjonen som gir deg dataene ha lov til å utlevere dem. Institusjonen må ha et rettslig grunnlag for behandlingen (utleveringen) av personopplysningene, og utleveringen må følge regler om taushetsplikt – dvs. samtykke fra den registrerte, dispensasjon eller annet unntak fra taushetsplikten.

Hvis prosjektet ditt skal bruke eller utvikle innovativ teknologi, eller hente data fra tekniske løsninger, medisinsk utstyr el., anbefaler vi at du rådfører deg med ressurser ved din institusjon for å avklare om – og på hvilken måte – prosjektet er teknisk og juridisk mulig å gjennomføre. Du kan for eksempel sjekke retningslinjene ved din institusjon og/eller rådføre deg med IT, jurister, medisinskteknisk personell etc., avhengig av hva prosjektet går ut på.

For mer om dataminimering se [Normens faktaark om personvernprinsippene, kapittel 1.3.](#)

## 5. Personopplysninger

### 5.1 Skal du behandle personopplysninger?

Etter at du har beskrevet hvilke data prosjektet skal bruke, må du vurdere om disse dataene er å anse som personopplysninger, og i så fall hvilken type personopplysninger.

Vi understreker dette like godt først som sist: vurderingen av om prosjektet skal behandle personopplysninger er helt essensiell. Dette fordi alle vurderinger du skal gjøre senere avhenger av at du har vurdert dette spørsmålet riktig. Behandling av personopplysninger er lovregulert, og må følge personvern- og helselovgivningen, mens behandling av anonyme

data ikke må det. En feilvurdering kan dermed innebære at prosjektet behandler personopplysninger uten å vite om det, og uten å gjøre nødvendige (lovpålagte) tiltak, slik at behandlingen er ulovlig. Brudd på personvernregelverket kan føre til store bøter for institusjonen din, og omdømmetap for prosjektet og forskningen. Derfor er det svært viktig at du gjør en grundig vurdering av om prosjektet skal behandle personopplysninger. Hvis du er i tvil i dette viktige spørsmålet, bør du rådføre deg med personvernressurser ved din institusjon.

### **Personopplysninger**

Personopplysninger vil det være hvis dataene i prosjektet på noen måte vil være mulig å knytte til en enkeltperson. Du må ta i betraktning alle data som skal brukes i prosjektet fra start til slutt, uavhengig av format. Vær oppmerksom på at det finnes mange ulike måter data kan knyttes til person på. Det kan være via:

- navn, fødselsnummer, adresse, telefonnummer, epost, samtykkeerklæring osv.
- bakgrunnsinformasjon som tid, sted, institusjon, alder, kjønn, stilling, diagnose osv.
- kode som viser til en koblingsnøkkel hos deg eller andre (f.eks. liste med prosjekt-ID og navn, eller pasientnummer og fødselsnummer)
- bilde, video, lydopptak
- IP-adresse, nettidifikator
- lokasjonsdata, bevegelses-/adferdsmønstre
- biometri (f.eks. iris, fingeravtrykk, ansikt, ganglag)
- humant biologisk materiale eller genetiske analyser (av arvestoff)

Som det fremgår av listen over, vil prosjektet behandle personopplysninger hvis dataene på en eller annen måte kan knyttes til enkeltpersoner. Vær oppmerksom på at data vil være å anse som personopplysninger selv om det eneste som knytter dem til enkeltpersoner er en kode som viser til en koblingsnøkkel (dvs. en liste der kode viser til identifiserbare opplysninger om person som f.eks. navn, pasientnummer, IP-adresse, bakgrunnsinformasjon el.). Dette gjelder selv om dataene ikke inneholder navn eller andre opplysninger som kan identifisere personene. Koden som viser tilbake til koblingsnøkkelen gjør at dataene defineres som personopplysninger. Dette gjelder også i tilfeller der prosjektet ikke selv har tilgang til koblingsnøkkelen, men den lagres hos SSB, FHI eller andre institusjoner. Vær også oppmerksom på at bakgrunnsvariabler (få eller mange) kan gjøre det mulig å spore opplysningene tilbake til enkeltpersoner. Flere variabler sett i sammenheng kan altså bakveisidentifisere de registrerte. Det gjelder selv om du eventuelt ikke har tilgang til direkte identifiserbare opplysninger eller koblingsnøkkel.

Når du har gjort en grundig vurdering av om prosjektet skal behandle personopplysninger, kan du gå videre. Hvis prosjektet skal behandle personopplysninger, er neste steg å vurdere hvilken type personopplysninger det er snakk om. Er det kun såkalt "alminnelige personopplysninger"? Eller er det "særlige kategorier personopplysninger" eller "personopplysninger om straffedommer eller lovovertrædelser" som skal brukes i prosjektet? Du må også vurdere om personopplysningene som skal behandles i prosjektet er taushetsbelagte. Grunnen til at du må gjøre disse vurderingene, er at det knytter seg egne regler til bruk av slike typer personopplysninger. Dine vurderinger her vil dermed påvirke hvilke vurderinger du må gjøre senere.

### **Alminnelige personopplysninger vs. Særlige kategorier personopplysninger**

"Alminnelige personopplysninger" er opplysninger om enkeltpersoner som ikke faller inn under de to neste kategoriene.



“Særlige kategorier personopplysninger” er data om rasemessig/etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning, fagforeningsmedlemskap, genetikk, biometri, helseforhold og/eller seksuelle forhold/orientering.

“Personopplysninger om straffedommer/lovovertrедelser” er definert som en egen kategori personopplysninger, og skal i henhold til norsk lov behandles på tilsvarende måte som særlige kategorier. Det er foreløpig begrenset med veiledning om hva dette begrepet inneholder, men en rimelig tolkning er at det omfatter opplysninger om lovovertrедelser helt fra det straffeprosessuelle mistankestadiet til endelig straffedom foreligger. Vi kan dermed gå ut fra at begrepet dekker de samme typer opplysninger som tidligere personvernlovgivning, nemlig at en person er – eller har vært - mistenkt, siktet, tiltalt eller dømt for en straffbar handling.<sup>1</sup>

De to sistnevnte typene av personopplysninger er gitt et særskilt vern i personvernregelverket. Det er fordi behandlingen av slike personopplysninger kan innebære høyere risiko for de registrerte enn behandling av alminnelige personopplysninger. Hvis opplysninger om enkeltpersoner for eksempel kommer på avveie eller brukes på en uventet eller inngripende måte, vil det ofte ha større konsekvenser for de registrerte hvis opplysningene er av en slik kategori, enn hvis det er alminnelige personopplysninger.

Det kan av og til være vanskelig å vurdere om opplysningene prosjektet skal samle inn er å anse som “særlige kategorier” eller “opplysninger om straffedommer/lovovertrедelser”. Da er det lurt å rådføre seg med personvernressurser ved din institusjon for å få hjelp. Rett vurdering er viktig fordi det gjelder egne regler for behandling av slike typer opplysninger. Kategoriseringen du gjør av opplysningene vil altså påvirke vurderingene du skal gjøre senere. Hvis opplysningene i prosjektet vil være i grenseland, kan det noen ganger være en løsning å ta høyde for at de er å anse som slike typer opplysninger og at prosjektet behandler dem deretter. Men det kan gi noen begrensninger, så det er ikke meningen at man skal definere alt som særlige kategorier for sikkerhets skyld. Det beste er å forsøke å kategorisere personopplysningene rett, og begrunne hvorfor man anser opplysningene som enten alminnelige, særlige eller opplysninger om straffedommer/lovovertrедelser.

Vi skal ikke gå igjennom alle de ulike typene særlige kategorier personopplysninger her. Men det er viktig å nevne at begrepet “helseopplysninger” eller “opplysninger om helseforhold” skal tolkes vidt. Det omfatter enhver opplysning som avdekker noe om en persons tidligere, nåværende eller fremtidige fysiske eller psykiske helsetilstand. Det kan være opplysninger om sykdom, funksjonshemming, sykdomsrisiko, sykehistorie, helsehjelp/behandling, fysiologisk/biomedisinsk tilstand, genetikk, biologiske prøver, tester/undersøkelser av kroppsdeler-/substans mm. Og det gjelder uavhengig av hvor opplysningene kommer fra, f.eks. pasientjournal, helsepersonell, medisinsk utstyr, den registrerte selv eller andre. Vær oppmerksom på at helse ikke trenger å stå i relasjon til sykdom, og at begrepet ikke bare betegner tilstander, men også årsaker og konsekvenser av tilstander.

### **Taushetsbelagte opplysninger**

Når du har vurdert kategori personopplysninger, må du også vurdere om opplysningene som skal behandles til prosjektformålet er underlagt taushetsplikt. Taushetsbelagte personopplysninger er data om personer fra kilder som har lovpålagt eller avtalefestet taushetsplikt om opplysningene. I vurderingen tar du utgangspunkt i datakildene dine. Skal prosjektet hente opplysninger fra en virksomhet eller person som, gjennom lov eller avtale,

---

<sup>1</sup> Skullerud m.fl., Personvernforordningen, kommentarutgave, side 115

har forbud mot å røpe de aktuelle opplysningene? Husk at du må ta i betraktning alle data som behandles i forbindelse med prosjektet, ikke bare data prosjektet innhenter for analyse, men også data som brukes (av prosjektet selv eller annen instans) for å rekruttere/trekke utvalget. Hvilke opplysninger som er taushetsbelagte, avhenger av bestemmelse(n) i den aktuelle loven/avtalen som fastsetter taushetsplikten.

Hvis det er uklart hvilke opplysninger prosjektet skal behandle (i analyser, rekruttering etc.), og om opplysningene er “særlige kategorier personopplysninger”, “personopplysninger om straffedommer/lovovertrедelser” og/eller taushetsbelagte, er det viktig at du får avklart det så tidlig som mulig i prosjektet/forskningsprosessen.

Hvis slike typer opplysninger skal brukes i prosjektet, må du vurdere om det er nødvendig for formålet. Hvis ja, bør du dokumentere en begrunnelse for behovet, og du må senere vurdere hvordan prosjektet skal behandle disse opplysningene for at det skal være lovlig. Hvis det ikke er nødvendig for formålet, kan prosjektet ikke behandle slike opplysninger, og du bør gjøre tiltak for å unngå det (f.eks. revidere intervjuguide/spørreskjema, eller be informanter utelate/slutte slike opplysninger før prosjektet får tilgang).

Hvis du er helt sikker på at prosjektet ikke skal behandle personopplysninger, trenger du ikke gå videre i denne veilederen. Ved siden av forskningsetikk og immateriell rett (som ikke er omtalt i veilederen her), er det eneste du da må tenke på om prosjektet trenger forhåndsgodkjenning fra REK. Hvis prosjektet har et formål som kan falle inn under det å “fremskaffe ny kunnskap om helse og sykdom”, kan det være å anse som helseforskning, selv om prosjektet kun skal behandle anonyme opplysninger. Det kan f.eks. være tester/forsøk som innebærer noe helserisiko der du innhenter samtykke, men ikke knytter data til forsøksperson. Prosjekter som omfattes av helseforskningsloven er søknadspliktige til REK. Hvis du er i tvil, rådfør deg med ressurser ved din institusjon og send gjerne en fremleggelsesvurdering til REK.

## 5.2 Anonyme opplysninger

### 5.2.1 Om anonyme opplysninger

I mange prosjekter brukes anonymisering som et tiltak for å redusere eller fjerne personvernrisikoen ved analyser, forskning, statistikk og publisering av datasett.

Helse- og personvernlovgivningen kommer kun til bruk når det er tale om personopplysninger, og gjelder ikke etter at opplysningene er anonymisert. Dette innebærer at dataansvarlig institusjon – etter anonymiseringen – ikke lenger er bundet av helse- og personvernlovgivningen, og derfor ikke må vurdere behandlingens lovlighet, eller om behandlingen er i tråd med de øvrige prinsippene i personvernforordningen. Videre vil f. eks ikke helsepersonellovens regler om taushetsplikt gjelde for anonyme opplysninger.

Det er imidlertid viktig å merke seg at behandlingen frem til opplysningene er å anse som anonyme må skje i tråd med formålet og behandlingsgrunnlaget opplysningene opprinnelig ble samlet inn for, slik det for eksempel er beskrevet i et informasjon- og samtykkeskriv, eller vedtak om dispensasjon fra taushetsplikten i et forskningsprosjekt. Selve anonymiseringsprosessen er derfor å regne som behandling av personopplysninger. Dette

betyr at dataansvarlig må tydelig definere hva som er formålet med anonymiseringen og vurdere om det foreligger et behandlingsgrunnlag etter personvernforordningen.<sup>2</sup>

Videre må ikke anonymisering forveksles med det å pseudonymisere opplysninger. Til forskjell fra anonymisering, er pseudonymisering en behandling av personopplysninger. Pseudonyme personopplysningene kan kun knyttes til en bestemt registrert gjennom bruk av tilleggsopplysninger, som er lagret atskilt og er omfattet av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til den registrerte.<sup>3</sup> Det mest praktiske eksempelet på pseudonyme opplysninger er personopplysninger der alle direkte og indirekte identifiserbare kjennetegn er fjernet, og de gjenstående opplysningene kun kan knyttes til den registrerte ved hjelp av en unik kode og kodenøkkel. Med andre ord kan den registrerte re-identifiseres selv om opplysningene er pseudonymisert.

## 5.2.2 Anonymiseringsprosessen og de vanligste risikoene

Vurderingen av hva som er anonyme opplysninger kan være en krevende øvelse. I personvernforordningens fortale står det at personopplysninger regnes som anonymiserte når de håndteres eller bearbeides slik at de ikke lenger kan knyttes til en identifisert eller identifiserbar fysisk person.<sup>4</sup> Anonymisering skal være en irreversibel prosess slik at det ikke er mulig å re-identifisere den registrerte.<sup>5</sup>

For å finne ut om opplysninger kan anonymiseres, må dataansvarlig først vurdere om de aktuelle opplysningene kan knyttes til den registrerte, og om det er sannsynlig at den registrerte kan re-identifiseres. Det bør tas hensyn til alle midler som det med rimelighet kan tenkes at dataansvarlig eller andre kan ta i bruk for å identifisere den registrerte direkte eller indirekte. For å fastslå om midler med rimelighet kan tenkes å bli tatt bruk for å identifisere den fysiske personen bør det tas hensyn til alle objektive faktorer, f.eks. kostnadene og tiden som er nødvendig for å foreta identifikasjonen, idet det tas hensyn til teknologien som er tilgjengelig på behandlingstidspunktet, samt den teknologiske utviklingen.<sup>6</sup>

Selv om personvernforordningens fortale gir en viss veiledning, er det ingen standard metode for hvordan helse- og personopplysninger kan anonymiseres. Det blir derfor opp til dataansvarlig institusjon å vurdere hva som skal til for at opplysninger skal anses som anonyme. Blant annet må det tas hensyn til antall opplysninger, hvilke opplysninger det er tale om og hvilke opplysninger som kan være tilgjengelig for offentligheten eller andre aktører.

Datatilsynet trekker frem tre sentrale risikoer som kan oppstå ved anonymisering av helse- og personopplysninger, og som bør brukes i vurderingen av hvor godt dataansvarlig har sikret seg mot re-identifisering<sup>7</sup>:

- Er det mulig å skille ut en enkeltperson i datasettet etter at anonymiseringen er gjennomført?
- Er det mulig å koble flere datasett sammen og til den samme personen?

<sup>2</sup> Les mer om behandlingsgrunnlag i [Faktaark 56 – Formål og behandlingsgrunnlag](#) og kapittel 2.5 om prosjekttype og behandlingsgrunnlag i denne veilederen

<sup>3</sup> Personvernforordningen art. 4 nr. 5

<sup>4</sup> Personvernforordningens fortalepunkt 26

<sup>5</sup> Datatilsynets veileder «Anonymisering av personopplysningene» (2015) side 6

<sup>6</sup> Personvernforordningens fortalepunkt 26

<sup>7</sup> Datatilsynets veileder «Anonymisering av personopplysningene» (2015) side 6



- Er det mulig å utlede informasjon som kan knyttes til en enkeltperson fra datasettet?

I en vurdering av om en anonymiseringsprosess er tilfredsstillende, bør dataansvarlig vurdere risikoen for re-identifisering av opplysningene, både før og etter at anonymiseringen er gjennomført. Videre er det viktig å være oppmerksom på at omstendighetene rundt opplysningene kan endre seg i tråd med den teknologiske utviklingen og at nye tilleggsopplysninger blir tilgjengelig. Prosjektet bør derfor ha gode rutiner for å evaluere risiko knyttet til faren for re-identifisering.

Dersom det ikke ble gjort en grundig nok vurdering av om opplysningene kan anonymiseres, og det ikke er mulig å anonymisere, foreligger en risiko for at det rettslige grunnlaget for behandlingen av personopplysninger i prosjektet, ikke dekker at opplysningene lagres videre. Dette kan medføre at prosjektet må få på plass nytt behandlingsgrunnlag. Det kan også være nødvendig med tiltak som å gi de registrerte ny informasjon, eventuelt å innhente nytt samtykke fra de registrerte. En konsekvens kan også være at opplysningene må slettes.

Som prosjektleder bør du rådføre deg med institusjonen din hvis du er usikker på om dataene du skal bruke i prosjektet er anonyme, eller hvilke tiltak du skal gjøre for å anonymisere dem etterpå.

## 6. Roller og ansvar

### 6.1 Hvorfor er det viktig å avklare roller og ansvar i et prosjekt?

Når du setter i gang med et prosjekt må roller og ansvar avklares. Det er særlig viktig å ha klarhet i hvem som bestemmer og har ansvaret for behandlingen av personopplysninger i prosjektet. Å kartlegge roller og ansvar er blant annet viktig for å finne ut hva din institusjon må iverksette av tiltak for å ivareta personvernet til de registrerte i prosjektet, og hva som må være på plass av dokumentasjon, f. eks hvilke typer avtaler som skal inngås med eventuelle samarbeidspartnere. Ansvar og roller skal dokumenteres før datainnsamlingen i et prosjekt begynner.

Dersom du er usikker på rollene og ansvaret i ditt prosjekt, anbefaler vi at du tar kontakt med personvernressurser ved din institusjon i god tid før oppstart av datainnsamlingen i prosjektet.

Vi anbefaler også å lese Datatilsynets veileder om roller og ansvar, som gir gode forklaringer og eksempler: [Behandlingsansvarlig og databehandler | Datatilsynet](#)

### 6.2 Dataansvarlig institusjon

Etter personvernforordningen er en dataansvarlig institusjon forpliktet til å ivareta personvernet og informasjonssikkerheten knyttet til alle behandlinger av personopplysninger som skjer i institusjonen.

Dataansvarlig er definert som 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 midler som skal benyttes»<sup>8</sup>. Med «midler» menes her hvordan vi behandler personopplysninger, f. eks hvordan de skal analyseres og lagres. Hvordan et prosjekt finansieres vil imidlertid ikke alene påvirke dataansvaret. Vær oppmerksom på at det er institusjonen, og ikke den enkelte prosjektleder, som bestemmer over behandlingen av personopplysninger i prosjektet og hvilken rolle institusjonen skal ha.

Dersom din institusjon bestemmer formålet og midler alene ved behandlingen av personopplysninger, eventuelt har samarbeidspartnere som har liten eller ingen innflytelse på behandlingen av personopplysninger i et prosjekt, vil din institusjon være dataansvarlig.

I helseforskning vil som oftest rollen som dataansvarlig og forskningsansvarlig være sammenfallende, se definisjon av forskningsansvarlig i vedlegg 1. Det finnes imidlertid tilfeller der dette nødvendigvis ikke er samme institusjon. En institusjon/virksomhet kan altså være dataansvarlig uten å være forskningsansvarlig. Et eksempel kan være legemiddelstudier der et helseforetak er forskningsansvarlig og dataansvarlig frem til utlevering av personopplysninger til sponsor, som også vil være dataansvarlig.

Hvilke plikter som er pålagt dataansvarlig institusjon, f.eks. om den registrertes rettigheter, krav til behandlingsgrunnlag mv., er regulert i helse- og personvernlovgivningen. Mange institusjoner har imidlertid også interne rutiner som beskriver hvordan disse pliktene skal etterleves i praksis, som er tilpasset den enkelte institusjon. Vi anbefaler at derfor du setter deg inn i hva som gjelder ved din institusjon.

### **6.3 Når flere institusjoner har felles dataansvar**

Din institusjon kan være dataansvarlig alene, eller ha felles dataansvar sammen med andre institusjoner. Da vil din institusjon bestemme formål og midler ved behandling av personopplysninger (helt eller delvis) sammen med en eller flere andre institusjoner. Dette kan f.eks. være tilfellet i multisenterstudier. For å finne ut av om det foreligger et felles dataansvar, kan det være nødvendig å ta en felles gjennomgang av hvilke aktiviteter knyttet til personvern den enkelte institusjon skal ha ansvar for å gjennomføre i prosjektet, og dokumentere dette sammen. Et verktøy som kan brukes til denne øvelsen er flytskjemaet med steg-for-steg-veiledningen som hører til denne veilederen.

Videre må ansvarsforholdene i et prosjekt tydelig kommuniseres utad. Det er f. eks viktig at informasjonen som de registrerte mottar i et prosjekt klart kommuniserer hvem som er dataansvarlig institusjon(er), slik at de registrerte vet hvor de kan rette henvendelser om sitt personvern. I prosjekter der det er flere forsknings- og/eller dataansvarlige institusjoner må disse organisere seg på en måte som gjør at de på en god måte kan ivareta henvendelser fra den registrerte.

### **6.4 Databehandler**

En databehandler er «en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige»<sup>9</sup>. En databehandler vil med andre ord ha liten eller ingen innflytelse

---

<sup>8</sup> Personvernforordningen art. 4 nr. 7

<sup>9</sup> Personvernforordningen art. 4 nr. 8

på formålet med behandlingen av personopplysningene eller midlene som skal brukes. Databehandleren behandler opplysningene på instruks fra dataansvarlig institusjon.

Hvordan databehandler skal behandle de aktuelle personopplysningene skal reguleres i en databehandleravtale. Se kapittel 15.3 om avtaler og Normens faktaark 10 om [bruk av databehandler](#).

Et eksempel på databehandlere kan være laboratorier som gjennomfører analyser på humant biologisk materiale som frembringer personopplysninger for et forskningsprosjekt. Andre eksempler er Tjeneste for sensitive data (TSD), SAFE og HUNT som et prosjekt kan bruke for å samle inn og lagre data.

I prosjekter med flere dataansvarlige er det viktig å kartlegge om det skal brukes databehandler i den felles gjennomgangen av aktiviteter i prosjektet knyttet til personvern.

## 6.5 Prosjektleders ansvar

De fleste typer prosjekter vil ha en utpekt prosjektleder, som har ansvaret for planleggingen og den daglige driften. Prosjektleder er gjerne den som i praksis skal følge opp, slik at prosjektet ivaretar lovpålagte krav til personvern og informasjonssikkerhet. Det er imidlertid viktig å understreke at institusjonen sitter med ansvaret. Som prosjektleder kan du derfor forvente å få råd og veiledning fra din institusjon, og det er viktig at du gjennomfører prosjektet og behandlingen av personopplysninger i tråd med interne rutiner og i samråd med institusjonen din.

Det er kun helseforskningsloven som konkret regulerer hvilke forpliktelser og oppgaver en prosjektleder har i et helseforskningsprosjekt<sup>10</sup>.

Alle forskere og forskningsprosjekter i Norge er imidlertid også bundet av lov om organisering av forskningsetisk arbeid. Det er utarbeidet en rekke forskningsetiske retningslinjer, både generelle og innen ulike fagområder.<sup>11</sup> Din institusjon vil også som regel ha egne rutiner der prosjektleders ansvar er nærmere beskrevet. I tillegg kan denne veilederen og flytskjema være verktøy prosjektleder kan bruke som et hjelpemiddel for å ivareta sitt ansvar.

# 7. Type prosjekt og behandlingsgrunnlag

## 7.1 Hvordan henger type prosjekt og behandlingsgrunnlag sammen?

Når du skal definere prosjekttype, tar du utgangspunkt i formålet med prosjektet ditt. Se på hvordan du har beskrevet formålet med prosjektet i kapittel 3, og forsøk deretter å plassere prosjektet innenfor en av kategoriene i oversikten under.

---

<sup>10</sup> Helseforskningsloven § 6 og forskrift om organisering av helseforskning § 5

<sup>11</sup> Se f. eks [Generelle forskningsetiske retningslinjer | Forskningsetikk](#)

Det å finne riktig prosjekttype er ikke alltid så lett i praksis. Mange prosjekter vil ha formål som kan ligge i “gråsonen” mellom ulike prosjekttyper. Samtidig er det svært viktig at du får plassert prosjektet ditt i rett kategori, fordi det vil påvirke både hvilke rettslige grunnlag du kan bruke i behandlingen av personopplysninger, og hvilke tillatelser du må innhente i prosjektet.

Vi anbefaler derfor at du ser nøye på definisjonene under, og at du rådfører deg med institusjonen din hvis du er i tvil. Her følger en kort definisjon av de vanligste prosjekttypene for forskning og kvalitetssikring innenfor helse- og kunnskapssektoren. Under forklarer vi mer om de vanligste “gråsonene”, og gir noen tips til hvordan du lettere kan finne rett prosjekttype for ditt prosjekt.

## 7.2 Type prosjekt

### 7.2.1 Definisjon av type prosjekt

#### **Medisinsk og helsefaglig forskning (Helseforskning)**

Helseforskning er virksomhet som utføres med vitenskapelig metodikk på mennesker, helseopplysninger eller humant biologisk materiale, for å fremskaffe ny kunnskap om helse og sykdom.

#### **Annen forskning på særlige kategorier personopplysninger**

“Annen forskning på særlige kategorier personopplysninger” er definert som en egen prosjekttype her, for å skille slik forskning fra helseforskning. “Annen forskning” er også virksomhet som utføres med vitenskapelig metodikk, men til forskjell fra helseforskning er ikke formålet å fremskaffe kunnskap om sykdom og helse, men f.eks. helsetjenesteforskning. Forskning på særlige kategorier personopplysninger krever andre behandlingsgrunnlag enn forskning på alminnelige personopplysninger, derfor skilles det mellom disse (se kapittel 5.1 over, om ulike typer personopplysninger).

#### **All forskning på alminnelige personopplysninger**

Helseforskning eller annen forskning der det behandles alminnelige personopplysninger (se kapittel 5.1 over, om ulike typer personopplysninger).

#### **All forskning på personopplysninger om straffedommer og lovovertrедelser**

Helseforskning eller annen forskning der det behandles personopplysninger om straffedommer og lovovertrедelser (se kapittel 5.1 over, om ulike typer personopplysninger).

#### **Kvalitetssikring på tvers av virksomheter**

Prosjekter, undersøkelser, evalueringer ol. som har som formål å kontrollere at diagnostikk og behandling faktisk gir de intenderte resultater. Disse prosjektene bruker helseopplysninger fra ulike virksomheters behandlingsrettede helseregistre eller andre helseregistre, eventuelt også data direkte fra de registrerte (f.eks. intervju, spørreskjema).

#### **Intern kvalitetssikring**

Prosjekter, undersøkelser, evalueringer ol. som har som formål å kontrollere at diagnostikk og behandling faktisk gir de intenderte resultater internt i virksomheten. Disse prosjektene bruker kun helseopplysninger fra virksomhetens interne behandlingsrettede helseregistre, eventuelt fra virksomheter man deler felles behandlingsrettede helseregistre med. I noen tilfeller innhentes også data fra de registrerte selv.

### **Etablering av medisinske kvalitetsregistre**

Formålet er å løpende dokumentere resultater fra helsehjelp for en avgrenset pasientgruppe med utgangspunkt i individuelle behandlingsforløp i et medisinske kvalitetsregistre, som gjennom statistikker, analyser og forskning danner grunnlag for:

- kvalitetsforbedring av helse- og omsorgstjenesten og/eller
- planlegging, styring og beredskap i helse- og omsorgstjenesten og i helse- og omsorgsforvaltningen.

### **Etablering av befolkningsbaserte helseundersøkelser**

Oppstart av en ny undersøkelse der det samles inn helseopplysninger og eventuelt humant biologisk materiale, basert på deltakernes samtykke, for å gi kunnskap om helseforholdene i en hel befolkning, befolkningsgruppe eller representativt utvalg av befolkningen,

### **Videreføring av befolkningsbaserte helseundersøkelser**

Viderebehandling av personopplysninger i en befolkningsbasert helseundersøkelse (se over) som ble etablert før sommeren 2018. Dette er definert som egen prosjekttype fordi det rettslige grunnlaget for behandling av personopplysninger i disse undersøkelsene skiller seg noe fra behandlingsgrunnlaget for etablering av nye befolkningsbaserte helseundersøkelser.

## **7.2.2 Noen vanlige gråsoner**

### **Hvordan skille mellom helseforskning og annen forskning?**

Helseforskning har til formål å fremskaffe ny kunnskap om helse og sykdom. Forskning som ikke har dette formålet, defineres ikke som helseforskning og reguleres ikke av helseforskningsloven. Det avgjørende er altså formålet med forskningen, ikke om det forskes på helseopplysninger eller om forskningen skjer innenfor helse- og omsorgstjenesten. Husk at begrepene “helse” og “sykdom” skal tolkes vidt (se kapittel 5.1).

På noen forskningsområder kan det være særlig utfordrende å skille mellom helseforskning og annen forskning. Det gjelder for eksempel:

- Arbeidslivsforskning og idrettsforskning. Her er det ekstra viktig å vurdere prosjektets problemstilling: Er formålet med prosjektet å gi “ny kunnskap om sykdom og helse”? Ved tvil, kan prosjektet likevel falle innenfor helseforskningsloven hvis risikoen for forskningsdeltakerne vurderes som betydelig.
- Prosjekter om kunstig intelligens og maskinlæring. Disse må også vurderes opp mot formålet. Det avgjørende er om selve treningen av algoritmen og utviklingsprosessen kan gi ny kunnskap om helse og sykdom.
- Innen grunnforskning kan enkelte prosjekter være helseforskning, hvis de involverer mennesker, helseopplysninger eller humant biologisk materiale, og vil frembringe ny kunnskap om helse og sykdom.

Hvis du er i tvil om prosjektet er “helseforskning” eller “annen forskning”, er det viktig å få avklart dette på et tidlig tidspunkt. Vi anbefaler da at du sender en fremleggelsesvurdering til REK. Du kan også lese mer om skillet mellom helseforskning og annen forskning i NEM sin veileder “[Helseforskningslovens saklige virkeområde](#)”.

### **Hvordan skille mellom (helse)forskning og kvalitetssikring?**

Det kan være vanskelig å skille forskning og kvalitetssikring. Begge prosjekttyper bruker som regel vitenskapelig metodikk for å analysere helseopplysninger. Både helseforskning og

kvalitetssikring har gjerne et overordnet mål om å bidra til å gi befolkningen bedre helsehjelp. Det som skiller disse to er det mer det konkrete formålet.

Kvalitetssikring innebærer å undersøke/evaluere om diagnostikk, behandling og annen helsehjelp faktisk gir forventede resultater og om kravene til kvalitet er oppfylt. I kvalitetssikring utvikler man ikke ny kunnskap om helse og sykdom, men vurderer om den helsehjelpen man vanligvis gir eller har gitt, resulterer i forventet utfall for pasientene og holder forventet kvalitet. Hvis prosjektet skal fremskaffe kunnskap om andre forhold enn dette, vil det trolig ikke kategoriseres som "kvalitetssikring", men heller falle inn under kategorien "forskning" (helseforskning eller annen forskning, se over).

Man kan bruke tre spørsmål, utviklet av Europarådet, som en hjelp i vurderingen. Hvis svaret er ja på de to første spørsmålene her, og nei på det siste, er prosjektet sannsynligvis kvalitetssikring:

- 1) Er prosjektets formål å forbedre kvaliteten på pasientbehandlingen på lokalt plan?
- 2) Går prosjektet ut på å prøve praksis mot etablerte standarder?
- 3) Innebærer prosjektet at noe gjøres med pasientene som ellers ikke ville blitt gjort som ledd i klinisk praksis og kvalitetssikring?

Hvis du er usikker på type prosjekt, anbefaler vi at du rådfører deg med din institusjon i god tid før datainnsamling. Er du usikker på om prosjektet er helseforskning, kan du sende fremleggelsesvurdering til REK og få svar ila. kort tid. Som nevnt over har NEM publisert en veileder om Helseforskningslovens saklige virkeområde. Denne forklarer nærmere om hvordan helseforskning kan avgrenses mot hhv. annen forskning, kvalitetssikring og helseregistre. Hvis du skal etablere medisinsk kvalitetsregister anbefaler vi å søke veiledning hos Nasjonalt servicemiljø for medisinske kvalitetsregistre.

### **Hvordan skille mellom "intern kvalitetssikring" og "kvalitetssikring på tvers"?**

Intern kvalitetssikring og "kvalitetssikring på tvers" har begge som formål å undersøke eller evaluere om diagnostikk, behandling og annen helsehjelp faktisk gir forventede resultater og om kravene til kvalitet er oppfylt (jf. avsnittet over). Det som skiller de to, er at "intern kvalitetssikring" kun foregår ved egen institusjon, mens "kvalitetssikring på tvers" involverer flere institusjoner.

Formålet med intern kvalitetssikring er å evaluere helsehjelpen som ytes ved egen institusjon. Virksomheten som yter helsehjelpen må selv stå som dataansvarlig for prosjektet, og prosjektet kan kun benytte data hentet fra pasientjournal og andre behandlingsrettede registre ved egen institusjon. I tilfeller der virksomheter har formalisert journalsamarbeid (felles pasientjournalssystem), kan de aktuelle virksomhetene drive intern kvalitetssikring av helsehjelpen de yter i fellesskap, og bruke helseopplysninger hentet fra deres felles behandlingsrettede registre. Slik kvalitetssikring vil fortsatt sortere under prosjekttypen "intern kvalitetssikring".

All annen kvalitetssikring vil være å anse som "kvalitetssikring på tvers av virksomheter". Det kan f.eks. være kvalitetsprosjekter der formålet er å evaluere helsehjelpen som ytes ved flere institusjoner (som ikke har formalisert journalsamarbeid), der man bruker data fra ulike pasientjournalssystemer og andre behandlingsrettede helseregistre. Vær oppmerksom på at også kvalitetprosjekter som bruker data fra sentrale helseregistre vil være å anse som "kvalitetssikring på tvers".



## 7.3 Tabell: prosjekttype og behandlingsgrunnlag

I [Tabell type prosjekt og behandlingsgrunnlag](#) finner du oversikt over de mest aktuelle behandlingsgrunnlagene for de ulike prosjekttypene hentet fra personvernforordningen, personopplysningsloven og helselovgivningen. Merk at dette ikke er en uttømmende oversikt, og det kan være andre behandlingsgrunnlag, blant annet EU/EØS-regelverk, som kan være relevante for ditt prosjekt.

## 7.4 Hva er et behandlingsgrunnlag?

Kartleggingen av prosjekttype du har gjennomført over er nødvendig for å finne ut hvilke lover prosjektet ditt må følge, og hvilke tillatelser du må innhente.

All behandling av personopplysninger reguleres av EUs personvernforordning og den norske personopplysningsloven. For noen formål (type prosjekt) vil helselover gjelde i tillegg. Hver behandling av personopplysninger må ha behandlingsgrunnlag i personvernforordningen artikkel 6, og oppfylle vilkår i aktuelle lover og forskrifter, for å være lovlig. I tillegg må behandling av særlige kategorier personopplysninger oppfylle et av unntakene i artikkel 9.

For hvert behandlingsgrunnlag i art. 6 og for hvert unntak i art. 9 er det kriterier som må være oppfylt for at det skal kunne brukes når du behandler personopplysninger.

Det er viktig å være klar over at behandlingsgrunnlagene i personvernforordningen er likestilte. Hvis en behandling av personopplysninger oppfylder vilkårene i flere ulike behandlingsgrunnlag, kan man velge. Det er altså ikke slik at ett grunnlag (f.eks. samtykke) har forrang og bør velges fremfor et annet (f.eks. allmennhetens interesse). Det innebærer imidlertid ikke at alle behandlingsgrunnlagene kan brukes i alle typer prosjekter. Det sentrale når du skal bestemme behandlingsgrunnlag, er hvilke vilkår prosjektet er i stand til å oppfylle.

Noen av behandlingsgrunnlagene i personvernforordningen er "selvstendige", i den forstand at det er tilstrekkelig å oppfylle vilkårene i det aktuelle grunnlaget for at behandlingen skal være lovlig. Samtykke er eksempel på et slikt grunnlag. Andre behandlingsgrunnlag krever derimot et supplerende grunnlag i norsk rett. Eksempler på slike behandlingsgrunnlag er "allmennhetens interesse" og "rettslig forpliktelse". Når man bruker disse, må man oppfylle kravene både i det aktuelle behandlingsgrunnlaget i forordningen, og oppfylle vilkårene som er gitt i lovhjemmelen i norsk rett. Lovhjemmelen fra norsk rett er det som kalles supplerende rettsgrunnlag.

Under gis det en oversikt over de ulike behandlingsgrunnlagene som er vanlig å bruke i forskning- og kvalitetssikringsprosjekter. Vi gir først en oversikt over behandlingsgrunnlagene i personvernforordningen og deretter en oversikt over supplerende rettsgrunnlag i norsk lov. Vi peker også på hvilke typer prosjekter du kan bruke de ulike behandlingsgrunnlagene.

I kapittel 7.3 finner du en tabell der både prosjekttype og behandlingsgrunnlag er oppsummert. Der vil du også se hvordan behandlingsgrunnlagene i personvernforordningen og supplerende rettsgrunnlag henger sammen.

## 7.5 De mest aktuelle behandlingsgrunnlagene etter personvernforordningen

### 7.5.1 Den registrertes samtykke til behandling av personopplysninger

Behandling av personopplysninger kan baseres på samtykke fra den registrerte. Samtykke er et selvstendig behandlingsgrunnlag som ikke krever supplerende grunnlag i norsk rett, det er tilstrekkelig å oppfylle vilkårene i personvernforordningen. Dette behandlingsgrunnlaget har vært vanlig å bruke i ulike former for forsknings- og kvalitetsprosjekter. Det er imidlertid viktig å være klar over at det ikke alltid er mulig å innfri alle kravene som stilles til et samtykke. Hvis det er vanskelig å oppfylle kravene til samtykke i ditt prosjekt, må du finne et annet behandlingsgrunnlag. I noen tilfeller kan det også være slik at andre behandlingsgrunnlag er bedre egnet for å ivareta formålet i forsknings- og kvalitetsprosjekter. Samtykke er derfor ikke et behandlingsgrunnlag som passer i alle prosjekter.

For at et samtykke skal være gyldig, må det være frivillig, spesifikt, informert, og utvetydig. Det siste innebærer at samtykke må være aktivt. Det er ikke å anse som et samtykke hvis man gir informasjon med reservasjonsrett (tidligere kalt passivt samtykke). Samtykket må også kunne dokumenteres og skal enkelt kunne trekkes tilbake av den registrerte. Ved behandling av personopplysninger i særlige kategori og/eller om straffedommer og lovovertridelser, er det i tillegg et krav at samtykke skal være uttrykkelig. Under forklares hvert av vilkårene.

#### **Frivillig**

Et samtykke skal være frivillig. Det innebærer at den registrerte av egen fri vilje samtykker til behandlingen av personopplysninger. Den registrerte skal ikke ha noen fordeler eller ulemper, eller oppleve noe press ved å gi fra seg opplysningene til prosjektet.

#### **Spesifikt**

Et samtykke skal også være spesifikt. Det må være klart og tydelig hva den registrerte samtykker til, mht. hvorfor og hvordan personopplysningene skal behandles.

#### **Informert**

I forkant av at det innhentes samtykke fra den registrerte skal prosjektet gi god informasjon om behandlingen av personopplysninger. Informasjonen skal sette den registrerte i stand til å forstå hva behandlingen innebærer, slik at vedkommende selv kan vurdere risikoen. For at samtykke skal være informert, må den registrerte ha fått informasjon:

- Hvem som er dataansvarlig institusjon
- Hva som er formålet med prosjektet
- Hvilke personopplysninger som skal behandles
- Den registrertes rett til når som helst å trekke tilbake sitt samtykke
- Hvis aktuelt: Overføring til tredjeland og hvilken risiko det innebærer
- Informeres om de registrertes rettigheter, se veilederens kapittel 12

Informasjonen som gis skal være kortfattet, åpen og lett tilgjengelig, i et klart og enkelt språk. Poenget er at den registrerte skal forstå informasjonen prosjektet gir, slik at de får et godt beslutningsgrunnlag.



### **Utvetydig viljesytring**

Samtykket skal være en "utvetydig viljesytring". Det betyr at den registrerte gir samtykke gjennom en aktiv handling som ikke kan misforstås, f. eks ved å møte opp, eller gi signatur skriftlig eller elektronisk signatur. Det skal være helt klart at den registrerte gir tillatelse til behandling av sine personopplysninger. Ved behandling av særlige kategorier personopplysninger er kravet skjerpet, ved at samtykket skal være uttrykkelig og gjelde for ett eller flere spesifikke formål. Samtykket skal da være gitt på en ekstra tydelig måte, slik at det ikke er tvil om at samtykket eksplisitt gjelder for det/de aktuelle formålene.

### **Dokumenterbart**

Det er ingen formkrav til samtykke. Samtykke kan gis muntlig, skriftlig eller på annen måte. Men du må kunne dokumentere at samtykke foreligger. I praksis vil det derfor foreligge et krav om å registrere at samtykke er avgitt, f.eks. ved at den registrerte undertegner en samtykkeerklæring, gir et elektronisk samtykke ved å logge seg inn og klikke på en avkryssingsboks, eller gir muntlig samtykke på et lyd- eller videoopptak.

### **Det skal være enkelt å trekke tilbake samtykket**

Et samtykke skal være like enkelt å trekke tilbake som det har vært å gi. Prosjektet må derfor være organisert slik at det er mulig for de registrerte å ta kontakt og få slettet opplysningene sine. Med andre ord må prosjektet sørge for å være tilgjengelig for den registrerte. F. eks tydelig kommunisere hva kontaktinformasjonen til prosjektleder eller annen prosjektmedarbeider er. En forutsetning for at prosjektet kan sikre at den registrerte får trukket seg, er at opplysningene behandles slik at de registrerte kan gjenfinnes i datamaterialet, og at man sikkert kan vite at dataene gjelder vedkommende. F. eks. ved bruk av kodenøkkel.

Som nevnt innledningsvis, kan du bare bruke samtykke som behandlingsgrunnlag dersom prosjektet ditt oppfyller alle kravene over. I noen prosjekter kan det være både mulig og ønskelig å gjøre tiltak for at behandlingen av personopplysninger skal kunne baseres på samtykke. Det kan f.eks. gjelde i mindre forsknings- eller kvalitetssikringsprosjekter der den registrerte bidrar aktivt i datainnsamlingen gjennom intervju, spørreskjema, tester, deltagende observasjon eller på annen måte. Samtykke kan i noen tilfeller også være aktuelt ved datainnsamling fra pasientjournal og andre behandlingsrettede registre, eller fra yrkesgrupper som har taushetsplikt, der man ber den registrerte tillate at taushetsbelagte personopplysninger brukes i forskning eller kvalitetssikring. I retningslinjer utgitt i forbindelse med Corona-pandemien trekker European Data Protection Board (EDPB) frem at samtykke kan benyttes som behandlingsgrunnlag i undersøkelser i ikke-intervensjonsstudier på en gitt populasjon, hvor det forskes på symptomer og utviklingen av en sykdom.<sup>12</sup>

I andre prosjekter, derimot, vil samtykke være uegnet som behandlingsgrunnlag. Det vil gjelde i alle tilfeller der det er umulig å innfri samtykkekravene, og andre behandlingsgrunnlag er aktuelle. Det kan også være tilfeller der andre behandlingsgrunnlag vil være bedre egnet.

Samtykke er f.eks. ikke egnet i tilfeller der det foreligger et skjevt maktforhold mellom den registrerte og forsknings- og/eller dataansvarlig institusjon. Det vil gjelde en del prosjekter innen helseforskning, herunder legemiddelstudier og andre kliniske studier. Den registrerte kan være sårbar på grunn av dårlig helsetilstand, og kan i noen tilfeller se på deltakelse i et

---

<sup>12</sup> EDPB: Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak: [edpb\\_guidelines\\_202003\\_healthdatascientificresearchcovid19\\_en.pdf \(europa.eu\)](https://edpb.europa.eu/our-work-and-activities/our-policies/eu-data-protection-boards-guidelines/03-2020-guidelines-03-2020-healthdatascientificresearchcovid19_en.pdf), avsnitt 20

forskningsprosjekt med så store forhåpninger at deltakelsen ikke fremstår som et reelt valg. Dette utfordrer kravet til at samtykket skal være frivillig avgitt.

Samtykke vil heller ikke være egnet behandlingsgrunnlag i tilfeller der det er vanskelig for den registrerte å forstå hva behandlingen av personopplysninger innebærer. For eksempel kan det i mange større forskningsprosjekter og i legemiddelstudier være lagt opp til en omfattende og komplisert behandling av personopplysninger, slik at det er vanskelig å gi den registrerte informasjon som de har forutsetninger for å sette seg inn i og forstå. Dette kan også være tilfelle ved etablering av medisinske kvalitetsregistre og befolkningsbaserte helseundersøkelser. Når det er vanskelig å påse og dokumentere at samtykket er tilstrekkelig informert, kan samtykke ikke brukes som behandlingsgrunnlag. De registrerte har rett til informasjon, uavhengig av dette, men prosjektet må finne et annet behandlingsgrunnlag som er mer egnet enn samtykke.

Det er viktig å være klar over at et samtykke kan ha ulike funksjoner. Som vist over, kan samtykke være et behandlingsgrunnlag, Men samtykke fra den registrerte kan også ha andre funksjoner:

- Når prosjektet bruker et annet behandlingsgrunnlag (som "allmennhetens interesse"), kan samtykke være et tiltak for å ivareta den registrertes rettigheter og friheter, fordi det både vil sikre medbestemmelse, åpenhet og forutsigbarhet for de som deltar i prosjektet.
- Når prosjektet skal behandle taushetsbelagte opplysninger, kan den registrerte gi samtykke som opphever taushetsplikten, slik at det ikke er nødvendig å søke om dispensasjon fra taushetsplikten<sup>13</sup>.
- Samtykke kan være et "ja til deltagelse" i et helseforskningsprosjekt<sup>14</sup>.
- Samtykke kan også være et "etisk ja til deltagelse" i annen forskning og kvalitetssikring der den registrerte aktivt deltar, f.eks. i intervju, spørreskjema eller eksperimenter.

### **Samtykke når de registrerte er barn**

Hvis barn skal delta i prosjektet, må du vurdere hvem som skal samtykke for barnet. Hovedregelen er at foreldre eller andre med foreldreansvar må gi samtykke frem til barnet er 18 år. I helseforskning og helseregistre er hovedregelen at ungdom kan samtykke selv fra 16 år.

For annen forskning enn helseforskning, faller man tilbake på hovedregelen om at foreldre med foreldreansvar samtykker på vegne av barnet frem til barnet er 18 år. Det er viktig å påpeke i den forbindelse at barn har en gradvis medvirknings- og selvråderett, hjemlet i barnelova § 31 og 33. Medvirkningsretten innebærer at barnet skal ha informasjon tilpasset sin alder og få muligheten til å si sin mening, i tråd med alder og modenhet. Det må også vurderes hvor inngripende forskningen anses å være for barnet. Hva som anses som det beste for (det enkelte) barnet, skal alltid være et grunnleggende hensyn, og som vil være avgjørende for om barn i det hele tatt skal delta i forskningsprosjekt eller ikke. De ovennevnte momentene må vurderes før foreldrene beslutter å gi et samtykke, eller ikke, til forskningen.

Dersom foreldre eller andre med foreldreansvar har samtykket på vegne av et barn til deltakelse i forskning eller kvalitetssikring, skal barnet når det blir 16 år få informasjon om

---

<sup>13</sup> Helsepersonelloven § 22

<sup>14</sup> Helseforskningsloven § 13

behandlingen av personopplysninger i prosjektet/registeret, og retten til å trekke samtykke tilbake eller motsette seg behandling.

**Samtykke når de registrerte er voksne uten samtykkekompetanse**

Samtykke kan ikke brukes som behandlingsgrunnlag i prosjekter der de registrerte mangler samtykkekompetanse. Dette kan f. eks være tilfelle i prosjekter som gjelder psykiatri og rus. Hvis det foreligger tvil om de registrerte har samtykkekompetanse eller ikke, må prosjektet foreta grundige vurderinger, noen ganger i samråd med helsepersonell eller pårørende som kjenner den registrerte. Vurderingene av samtykkekompetanse er ofte komplekse, og behandlingen av personopplysninger kan utgjøre en høy risiko for den registrertes rettigheter og friheter. Hvis det er aktuelt å forske på personer med redusert eller manglende samtykkekompetanse i ditt prosjekt, anbefaler vi derfor at du rådfører deg med din institusjon om hvordan prosjektet kan gjennomføres i tråd med helse- og personvernlovgivningen.

## **7.5.2 Nødvendig for å utføre en oppgave i allmennhetens interesse**

Behandling av personopplysninger for å utføre en oppgave i “allmennhetens interesse”, jf. personvernforordningen art. 6 nr. 1 e), er et behandlingsgrunnlag som er vanlig i forskning og kvalitetssikring. Det må kunne dokumenteres at behandlingen av personopplysninger er nødvendig for å utføre en oppgave av allmenn interesse. Her er det helt sentralt at du kan begrunne hvorvidt prosjektets formål har nytteverdi for samfunnet, og at det er nødvendig for dette formålet å behandle de aktuelle personopplysningene. I tillegg må du dokumentere at prosjektet følger vilkårene i et supplerende rettsgrunnlag i norsk lov (se kapittel 7.8)

## **7.5.3 Nødvendig for å oppfylle en rettslig forpliktelse**

Behandling av personopplysninger er lov når det er nødvendig for å “oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige”, jf. personvernforordningen art. 6 nr. 1 c). Dette behandlingsgrunnlaget kan være aktuelt å vise til i kvalitetssikring som gjennomføres ved institusjoner som yter helsehjelp. Du må da dokumentere at prosjektet har et formål som din institusjon har en lovpålagt plikt til å oppfylle, og at det er nødvendig å behandle de aktuelle personopplysningene for å oppfylle dette formålet. Et krav er at behandlingen har supplerende rettsgrunnlag i norsk lov, og at prosjektet oppfylder kravene som er gitt i dette rettsgrunnlaget. Du må derfor kunne vise konkret til den norske lovhjemmelen som sier at det er en rettslig forpliktelse for din institusjon å behandle personopplysninger til det aktuelle formålet, f.eks. krav i spesialisthelsetjenesteloven eller helse- og omsorgstjenesteloven som pålegger helseforetak å kvalitetssikre sitt behandlingstilbud.

## **7.6 De mest aktuelle unntakene fra forbudet mot behandling av personopplysninger i særlig kategori**

### **7.6.1 Nødvendig for arkivformål, forskning og statistikk**

Personvernforordningen art. 9 nr. 2 j) åpner for at personopplysninger kan behandles når det er nødvendig for “arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål”. Også her må du dokumentere en begrunnelse for at prosjektets formål har nytteverdi for samfunnet, og at det er nødvendig for dette formålet å behandle de særlige kategoriene personopplysninger. Du må også dokumentere at prosjektet oppfylder vilkårene i personvernforordningen art. 89 nr. 1 og et supplerende rettsgrunnlag i norsk lov (se kapittel 7.8). Det innebærer for det første at behandlingen av personopplysninger i prosjektet må være forholdsmessig – det må være et rimelig forhold mellom formålet og personvernrisikoen for de registrerte. For det andre må du dokumentere at prosjektet setter inn egnede tiltak som gir et tilstrekkelig vern av de registrertes rettigheter og friheter. Eksempler på slike tiltak kan være dataminimering og pseudonymisering. Andre eksempler kan være at prosjektet innhenter samtykke fra den registrerte selv om det ikke er behandlingsgrunnlaget. Og videre at prosjektet følger regler som følger av helselovgivningen for øvrig, som f. eks krav til taushetsplikt etter helsepersonelloven eller kravene i helseforskningsloven.

## **7.6.2 Nødvendig for forebyggende medisin, yting og/eller forvaltning av helsetjenester mm.**

Personvernforordningen art. 9 nr. 2 h) åpner for at særlige kategorier personopplysninger kan behandles når det er nødvendig "i forbindelse med forebyggende medisin eller arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet, i forbindelse med medisinsk diagnostikk, yting av helse- eller sosialtjenester, behandling eller forvaltning av helse- eller sosialtjenester og –systemer».

Dette behandlingsgrunnlaget kan derfor brukes i kvalitetssikring. Det gjelder både for prosjektypene "intern kvalitetssikring" og "kvalitetssikring på tvers". Du må kunne dokumentere at prosjektets formål faller inn under formålet som er beskrevet i personvernforordningen, og at det er nødvendig å behandle de aktuelle personopplysningene til dette formålet. I tillegg må prosjektet oppfylle vilkårene i et supplerende rettsgrunnlag i norsk lov.

I kvalitetssikringsprosjekter der Helsedirektoratet har fattet vedtak om dispensasjon fra taushetsplikten, er det praksis at dette fungerer som et behandlingsgrunnlag sammen med art. 9 nr. 2 g og i, se omtale om disse behandlingsgrunnlagene under.

## **7.6.3 Nødvendig av hensyn til viktige allmenne interesser**

Personvernforordningen art. 9 nr. 2 g) åpner for at særlige kategorier personopplysninger kan behandles hvis det er nødvendig av hensyn til «viktige allmenne interesser». På samme måte som over må du da kunne dokumentere en begrunnelse for at prosjektets formål har nytteverdi for samfunnet, og at det er nødvendig for dette formålet å behandle de særlige kategoriene personopplysninger. Du må også dokumentere at prosjektet oppfyller vilkårene i et supplerende rettsgrunnlag i norsk lov, som viser at behandlingen er forholdsmessig (nytte vs. risiko) og at dere setter inn egnede tiltak for å verne den registrertes rettigheter og friheter. Dette behandlingsgrunnlaget kan være aktuelt å bruke f.eks. i kvalitetssikringsprosjekter.

## **7.6.4 Nødvendig av allmenne folkehelsehensyn**

Personvernforordningen art. 9 nr. 2 i) åpner for at særlige kategorier personopplysninger kan behandles når det er nødvendig "av allmenne folkehelsehensyn, f.eks. vern mot alvorlige grenseoverskridende helsetrusler eller for å sikre høye kvalitets- og sikkerhetsstandarder for helsetjenester og legemidler eller medisinsk utstyr."

For å bruke dette behandlingsgrunnlaget må formålet med prosjektet falle innunder begrepet "allmenne folkehelsehensyn", slik det er beskrevet i loven, og du må dokumentere at det er nødvendig for formålet å behandle de særlige kategoriene personopplysninger. Du må også dokumentere at prosjektet oppfyller vilkårene i et supplerende rettsgrunnlag i norsk lov, og at prosjektet setter inn egnede tiltak, som f. eks taushetsplikt, for å verne den registrertes rettigheter og friheter. Dette behandlingsgrunnlaget kan være aktuelt å bruke i forsknings- og kvalitetssikringsprosjekter i samsvar med formålet nevnt over.

## **7.6.5 Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte selv har offentliggjort**

Behandling av særlige kategorier personopplysninger er også lovlig dersom «behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort», jf. personvernforordningen art. 9 nr. 2 e). Dette behandlingsgrunnlaget kan f.eks. være aktuelt ved forskning på personopplysninger hentet fra sosiale medier. Det er da tilstrekkelig å oppfylle kravene som personvernforordningen gir, fordi dette behandlingsgrunnlaget ikke krever supplerende grunnlag i norsk rett. Viktige forutsetninger er at opplysningene faktisk er publisert av den det gjelder, og at vedkommende er i rimelig stand til å forstå konsekvensene av publiseringen. Det kan f.eks. ikke vises til dette behandlingsgrunnlaget hvis personopplysninger er publisert av et barn eller en person med demens. Prosjektet og din institusjon har ansvar for å sikre og påvise at vilkårene er oppfylt. Ved forskning med internettbaserte kilder kan det i en del tilfeller være rimelig å anta at opplysningene er lagt ut av den registrerte selv, og at den registrerte forstår hva det innebærer. Men hvis det er vanskelig å dokumentere dette, vil det være «tryggere» å undersøke og dokumentere at dette faktisk er riktig, eller vise til et annet behandlingsgrunnlag.

## **7.7 Unntak fra forbudet mot å behandle personopplysninger om straffedommer og lovovertrедelser**

Etter personvernforordningens art. 10 kan personopplysninger om straffedommer og lovovertrедelser bare behandles av offentlige myndigheter, med mindre nasjonal rett har egne lover som åpner for annen behandling av slike opplysninger. I Norge åpner personopplysningsloven § 11 for at slike opplysninger på visse vilkår kan behandles av andre institusjoner, blant annet til forskning (se under). Men omfattende registre over straffedommer kan uansett bare føres under en offentlig myndighets kontroll. Se definisjon av begrepet “personopplysninger om straffedommer og lovovertrедelser” i kapittel 5.1.

Det er foreløpig begrenset med veiledning om hva begrepet “straffedommer og lovovertrедelser” inneholder. En rimelig tolkning er at det omfatter opplysninger om lovovertrедelser helt fra det straffeprosessuelle mistankestadiet til endelig straffedom foreligger. Vi kan dermed gå ut fra at begrepet dekker de samme typer opplysninger som tidligere personvernlovgivning, nemlig at en person er – eller har vært - mistenkt, siktet, tiltalt eller dømt.

## **7.8 Supplerende rettsgrunnlag**

### **7.8.1 Personopplysningsloven § 8 – behandlingen av personopplysninger er nødvendig for arkivformål, forskning og statistikk**

Personopplysningsloven § 8 tillater å behandle personopplysninger til forskningsformål med rettslig grunnlag i allmennhetens interesse hvis det er nødvendig for arkiv/forskning/statistikkformål og behandlingen er omfattet av “nødvendige garantier for å ivareta de registrertes rettigheter og friheter”. I tillegg må du ha lovlig tilgang til opplysningene, som for eksempel unntak fra taushetsplikt dersom opplysningene er taushetsbelagt.

Denne bestemmelsen brukes som supplerende rettsgrunnlag til personvernforordningen art. 6 nr. 1 e), for eksempel i forskningsprosjekter som behandler personopplysninger med



grunnlag i allmennhetens interesse. Det gjelder forskning på alle typer opplysninger. Hvis prosjektet behandler særlige kategorier personopplysninger, må det i tillegg foreligge unntak fra forbudet i art. 9. Men også behandling av slike typer opplysninger må ha grunnlag i personvernforordningen art. 6, og når dette grunnlaget er art. 6 nr. 1 e), må man vise til personopplysningsloven § 8 i tillegg.

Når du bruker dette rettsgrunnlaget, må du dokumentere en begrunnelse for at prosjektets formål faller inn under begrepet "arkiv/forskning/statistikk" og er i allmennhetens interesse, og at behandlingen av de aktuelle personopplysningene er nødvendig for å oppnå prosjektformålet. Du må også dokumentere at prosjektet setter inn «nødvendige garantier». Med nødvendige garantier menes særskilte tiltak som har til hensikt å verne om den registrertes rettigheter og friheter. Disse garantiene skal særlig sikre at prinsippet om dataminimering overholdes. Du må altså passe nøye på at prosjektet ikke behandler flere eller andre typer personopplysninger enn det som er helt nødvendig for å oppnå prosjektformålet.

For å finne hvilke nødvendige garantier prosjektet kan sette inn, vil en fremgangsmåte kunne være å vurdere den planlagte behandlingen opp mot de generelle reglene i personvernforordningen, for å se på om prinsippene og rettighetene kan ivaretas enda bedre. Her kan det f. eks vurderes om det er mulig med tydeligere formålsbegrensning, mer dataminimering, bedre sikring av opplysningene, begrenset varighet, eller å gi bedre informasjon om behandlingen og rettighetene til de registrerte. Ta gjerne kontakt med personvernressurser ved din institusjon for å få hjelp til å finne passende tiltak.

## **7.8.2 Personopplysningsloven § 9 – særlige kategorier personopplysninger er nødvendig for arkivformål, forskning og statistikk**

Personopplysningsloven § 9 tillater å behandle særlige kategorier personopplysninger når det er nødvendig for arkiv/forskning/statistikkformål (personvernforordningen art. 9 nr. 2 j) hvis alle disse kriteriene er oppfylt:

- Behandlingen er nødvendig for arkiv/forskning/statistikkformål
- Samfunnsinteressen av behandlingen overstiger klart ulempene for den enkelte
- Prosjektet har rådført seg med personvernombud eller tilsvarende, og ombudet har vurdert at behandlingen vil oppfylle kravene i personvernlovgivningen.

Denne bestemmelsen brukes som supplerende rettsgrunnlag til personvernforordningen art. 9 nr. 2 j), blant annet i forskning på særlige kategorier personopplysninger der det ikke er behov for dispensasjon fra taushetsplikten etter helselovgivningen. I tillegg må du ha lovlig tilgang til opplysningene, som for eksempel unntak fra taushetsplikt dersom opplysningene er taushetsbelagt.

Når du bruker dette rettsgrunnlaget, må du - på samme måte som over - dokumentere en begrunnelse for at prosjektets formål faller inn under begrepet "arkiv/forskning/statistikk" og er i allmennhetens interesse. Du må også argumentere for at samfunnets interesse i at prosjektet gjennomføres klart overstiger ulempene for den enkelte som det behandles personopplysninger om. Videre må du begrunne at behandlingen av de aktuelle personopplysningene er nødvendig for å oppnå prosjektformålet. Du må også sørge for – og dokumentere – at prosjektet setter inn «nødvendige garantier». Du kan da vise til

nødvendige garantier som forklart over. Gode tiltak vil også være å følge de mer spesifikke reglene i helselovgivningen, herunder ivareta taushetsplikt, regler om samtykkekompetanse mv.

### **7.8.3 Personopplysningsloven § 11 – unntak fra forbudet mot å behandle personopplysninger om straffedommer og lovovertrедelser**

Personvernforordningen gir, som nevnt over, et generelt forbud mot at opplysninger om straffedommer og lovovertrедelser behandles av andre enn offentlige myndigheter, med mindre nasjonal lov åpner for annen behandling. Personopplysningsloven § 11 tillater at institusjoner - både offentlige myndigheter og andre – kan behandle opplysninger om straffedommer og lovovertrедelser til andre formål enn offentlig myndighetsutøvelse, på ett av følgende grunnlag:

- Uttrykkelig samtykke fra den registrerte
- Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte selv har gjort offentlig kjent
- Behandlingen er nødvendig for arkiv/forskning/statistikk-formål. Vilkår er da at samfunnsinteressen av behandlingen klart overstiger klart ulempene for den enkelte, og at prosjektet har rådført seg med personvernombud eller tilsvarende som har vurdert at behandlingen vil oppfylle kravene i personvernlovgivningen.

Denne bestemmelsen brukes som supplerende rettsgrunnlag til personvernforordningen art. 10, i forskningsprosjekter som behandler personopplysninger om straffedommer og lovovertrедelser, nærmere bestemt at en person er siktet, mistenkt, tiltalt eller dømt for en straffbar handling. Personopplysningsloven § 11 tillater bare at slike opplysninger behandles hvis ett av de tre punktene over gjør seg gjeldende. Opplysningene kan da behandles på samme måte som særlige kategorier personopplysninger iht. de aktuelle unntakene i personvernforordningen art. 9 nr. 2. Når du bruker dette rettsgrunnlaget, må du derfor dokumentere en begrunnelse for at opplysningene om straffedommer og lovovertrедelser behandles med grunnlag – enten i den registrertes uttrykkelige samtykke, eller at det gjelder personopplysninger som det er åpenbart at den registrerte selv har offentliggjort, eller at det er nødvendig for arkiv/forskning/statistikkformål og at vilkårene er oppfylt.

### **7.8.4 Helseregisterloven § 19b – vedtak fra Helsedataservice om tilgjengeliggjøring av helseopplysninger fra lovbestemte helseregistre**

Helseregisterloven § 19 b) åpner for at helseopplysninger fra lovbestemte helseregistre på visse vilkår kan behandles, ved at de sammenstilles og tilgjengeliggjøres uten hinder av taushetsplikt. Dersom Helsedataservice har innvilget søknad om tilgjengeliggjøring av helseopplysninger fra et eller flere lovbestemte helseregistre, som f. eks Legemiddelregisteret eller Dødsårsaksregisteret, kan prosjektet som mottaker av disse opplysningene bruke vedtaket etter helseregisterloven § 19b som et supplerende rettsgrunnlag, dvs. behandlingsgrunnlag i prosjektet. Vilkår for tilgjengeliggjøring er at de registrertes integritet og konfidensialitet er ivaretatt, og at behandlingen av personopplysninger er av vesentlig interesse for samfunnet.



I en søknad er det derfor viktig at du dokumenterer at lovens vilkår er oppfylt. I veilederens kapittel 14.2 er det inntatt tips til søknadsprosessen.

### **7.8.5 Helsepersonelloven § 29 og helseregisterloven § 19e – vedtak om dispensasjon fra taushetsplikten**

Utgangspunktet er at det skal innhentes samtykke fra den registrerte når helseopplysninger skal behandles. I mange tilfeller er det imidlertid ikke mulig eller vanskelig å innhente samtykke, f. eks. i prosjekter der det skal bruke store mengder registerdata, dersom de registrerte er avdøde eller prosjektet skal gjennomgå pasientjournaler for å finne aktuelle prosjektdeltakere. Derfor er det i helselovgivningen åpnet for at det kan fattes vedtak om dispensasjon fra taushetsplikten på nærmere vilkår.

- For opplysninger fra pasientjournal og andre behandlingsrettede helseregistre kan du søke om dispensasjon fra taushetsplikten etter helsepersonelloven § 29.
- For opplysninger fra helseregistre kan du søke om dispensasjon fra taushetsplikten etter helseregisterloven § 19e).

I veilederens kapittel 14.1 og 14.2 er det gitt en oversikt over hvilke instanser du skal sende søknader om dispensasjon til. I tillegg er det gitt tips til søknadsprosessen.

Hvis du får innvilget dispensasjon, vil dette vedtaket utgjøre både unntak fra taushetsplikten for virksomheten som skal utlevere opplysninger til prosjektet, og det rettslige behandlingsgrunnlaget for behandlingen av personopplysninger i prosjektet. Vær oppmerksom på at dispensasjonen kan inneholde vilkår som du må følge.

### **7.8.6 Pasientjournalloven § 6 og helsepersonelloven § 26 – intern kvalitetssikring**

Pasientjournalloven § 6 og helsepersonelloven § 26 gir adgang til å behandle helseopplysninger til formålet intern kvalitetssikring.

Adgangen til å behandle personopplysninger etter disse bestemmelsene er avgrenset til å gi opplysninger til institusjonens ledelse "når dette er nødvendig for å kunne gi helsehjelp, for administrasjon, eller for internkontroll og kvalitetssikring av tjenesten". Bestemmelsene kan med andre ord utelukkende brukes for å hjemle behandling av personopplysninger for formål om intern kvalitetssikring. De gir ikke adgang til å gjøre oppslag i pasientjournal for andre formål som f.eks. forskningsprosjekter, verken helseforskning eller annen forskning. De gir heller ikke adgang til å behandle personopplysninger i kvalitetsprosjekter der dere samarbeider med eller bruker data fra eksterne institusjoner.

En viktig forutsetning for å bruke helsepersonelloven § 26 og pasientjournalloven § 6 som supplerende behandlingsgrunnlag er at din institusjon yter helsehjelp, og derfor har en lovpålagt plikt til å kvalitetssikre denne helsehjelpen. En annen viktig forutsetning er at prosjektet kun behandler personopplysninger om pasienter som inngår i virksomhetens pasientjournalssystem, eventuelt fra institusjoner som din institusjon har et formalisert journalsamarbeid med. En tredje forutsetning er at behandlingen av personopplysninger i prosjektet er forankret hos ledelsen ved din institusjon. For å sikre og dokumentere at disse vilkårene er oppfylt, anbefaler vi at prosjektet beskriver den planlagte behandlingen av personopplysninger og får godkjenning til dette fra ledelsen.

For interne kvalitetssikringsprosjekter som bruker dette behandlingsgrunnlaget, er det ikke nødvendig å innhente samtykke fra pasientene. Det er heller ikke nødvendig å informere dem om prosjektet, med mindre helsepersonellet som kjenner pasienten “har grunn til å tro at pasienten ville ha motsatt seg behandlingen av personopplysninger dersom vedkommende ble informert”. Prosjektet må altså gjøre en konkret vurdering av om pasienten har rett på informasjon eller ikke, om at personopplysninger behandles i kvalitetssikringsprosjektet. Dere bør dokumentere vurderingen. I enkelte tilfeller er det naturlig å informere og be om samtykke. Det vil særlig gjelde i prosjekter der pasientene selv skal bidra med tilleggsopplysninger som ikke samles inn for å yte helsehjelp, men kun innhentes for kvalitetssikringsformålet. Samtykket vil da fungere som et tiltak for å ivareta de registrertes rettigheter og friheter, men trenger ikke utgjøre det rettslige grunnlaget for behandlingen av personopplysninger.

### **7.8.7 Forskrift om medisinske kvalitetsregistre**

Forskrift om medisinske kvalitetsregistre åpner for at personopplysninger kan behandles når formålet er å etablere et register der man løpende dokumenterer resultater fra helsehjelp for en avgrenset pasientgruppe med utgangspunkt i individuelle behandlingsforløp.

Forskriften inneholder en rekke vilkår, og du må sikre og dokumentere at alle disse er oppfylt. Det er forskriften i sin helhet som gir det supplerende rettsgrunnlaget. Hovedregelen etter forskriften er at samtykke skal innhentes fra den registrerte. Som et alternativ er det adgang til, på nærmere vilkår, at den registrerte kan reservere seg mot deltakelse fremfor å avgi samtykke. Den registrertes samtykke eller reservasjonsadgang fungerer da som et tiltak for å ivareta de registrertes rettigheter og friheter.

Siden forskriften er etablert med hjemmel i helseregisterloven, må du også forsikre deg om – og dokumentere – at behandlingen av personopplysninger er i samsvar med reglene i helseregisterloven. Helseregisterloven gir blant annet regler om tilgjengeliggjøring av helseopplysninger, som prosjektet må følge hver gang personidentifiserbare opplysninger skal utleveres til ulike forsknings- og kvalitetssikringsprosjekter som ønsker å bruke data fra registeret.

Etablering av medisinske kvalitetsregistre innebærer som regel høy personvernrisiko fordi det skal behandles et stort omfang særlige kategorier personopplysninger om ulike pasientgrupper. Det vil dermed være krav om å foreta en grundig vurdering av personvernkonsekvenser (DPIA) før oppstart (se kapittel 13).

Hvis du planlegger etablering av et medisinsk kvalitetsregister, anbefaler vi derfor at du så tidlig som mulig i prosessen ber om bistand fra personvernressurser ved din institusjon. Du kan også søke veiledning hos [Nasjonalt servicemiljø for medisinske kvalitetsregistre](#).

### **7.8.8 Forskrift om befolkningsbaserte helseundersøkelser**

Forskrift om befolkningsbaserte helseundersøkelser åpner for at personopplysninger kan behandles når formålet er å samle inn helseopplysninger og evt. humant biologisk materiale i et register etter samtykke fra deltagerne, for å legge til rette for at helseopplysninger fra undersøkelsen kan benyttes til analyser og forskning som kan gi kunnskap om helsen i befolkningen eller en befolkningsgruppe.

Også denne forskriften inneholder en rekke vilkår. Når du bruker dette rettsgrunnlaget, må du sikre og dokumentere at alle disse vilkårene er oppfylt. Siden forskriften er etablert med hjemmel i helseregisterloven, må du i tillegg forsikre deg om – og dokumentere – at

behandlingen av personopplysninger er i samsvar med reglene i helseregisterloven. Som nevnt i kapittel 7.8.7, gir helseregisterloven blant annet regler om tilgjengeliggjøring av helseopplysninger. Befolkningsbaserte helseundersøkelser må følge disse reglene hver gang personopplysninger skal tilgjengeliggjøres for ulike forsknings- og kvalitetssikringsprosjekter som ønsker å bruke data fra registeret.

Etablering av befolkningsbaserte helseundersøkelser innebærer som regel høy personvernrisiko fordi det skal behandles et stort omfang særlige kategorier personopplysninger, ofte om sårbare personer. Det vil dermed være krav om å foreta en grundig vurdering av personvernkonsekvenser før oppstart (se kapittel 13 under). Hvis du planlegger å etablere en befolkningsbasert helseundersøkelse, anbefaler vi derfor at du så tidlig som mulig i prosessen ber om bistand fra personvernressurser ved din institusjon.

Forskriften åpner også for at befolkningsbaserte helseundersøkelser som ble etablert før forskriften kom i 2018 kan videreføres på visse vilkår. Slike undersøkelser hadde tidligere konsesjon fra Datatilsynet og behandlingsgrunnlag i samtykke. Da personvernforordningen ble innført i 2018, ble kravene til samtykke skjerpet. Samtykke kunne dermed ikke lenger brukes som behandlingsgrunnlag i helseundersøkelsene. Forskriften ble etablert for å gi hjemmel til å videreføre behandlingen av personopplysninger i disse undersøkelsene, for å hindre at verdifulle data gikk tapt.

Hvis du er prosjektleder for en befolkningsbasert helseundersøkelse som ble etablert før 2018, anbefaler vi at du i samråd med din institusjon gjennomfører en personvernkonsekvensvurdering (se kapittel 13), der dere vurderer den pågående behandlingen av personopplysninger i undersøkelsen opp mot vilkårene i forskriften. Hvis det er vanskelig å følge vilkårene i forskriften, bør dere be om veiledning fra Datatilsynet.

## **7.8.9 REK-godkjenning etter helseforskningsloven gir ikke behandlingsgrunnlag**

Medisinsk og helsefaglige forskningsprosjekter skal være forhåndsgodkjent av den regionale etiske komite for medisinsk og helsefaglig forskningsetikk. Vær oppmerksom på at denne forskningsetiske forhåndsgodkjenningen fra REK ikke gir rettslig grunnlag for å behandle personopplysninger. Dette er en vanlig misforståelse ved oppstart av nye helseforskningsprosjekter, og ved personvern vurderinger av pågående helseforskningsprosjekter.

I perioden 2010-2018 utgjorde REK-godkjenningen både nødvendig og tilstrekkelig grunnlag for å behandle personopplysninger i helseforskningsprosjekter. Ved innføringen av personvernforordningen i 2018 ble det avklart at REK-godkjenningen ikke videreføres som et behandlingsgrunnlag.

Helseforskningsprosjekter må derfor følge de generelle reglene for behandling av personopplysninger, og dokumentere behandlingsgrunnlag i personvernforordningen art. 6 og unntak fra forbudet i art. 9. Tilsvarende regler gjaldt før helseforskningsloven kom i 2010, etter den tidligere personopplysningsloven.

Det stilles fortsatt krav til forskningsetisk godkjenning fra REK i helseforskningsprosjekter.<sup>15</sup> Men godkjenningen har en annen funksjon. Den gir som nevnt ikke lenger et

---

<sup>15</sup> Helseforskningsloven § 9

behandlingsgrunnlag, men utgjør et viktig tiltak ("nødvendig garanti") for å ivareta de registrertes rettigheter og friheter i et prosjekt.

Når dette er sagt, er det i realiteten små endringer i reglene for hvordan man behandler personopplysninger i helseforskning etter at personvernforordningen ble innført.

## 8. Dataflyt og sikkerhet

For å få en oversikt over dataflyten i prosjektet bør du lage en konkret plan for hvordan prosjektet skal samle inn, analysere, koble, lagre, dele og sikre personopplysninger. For mange kan det være nyttig å illustrere dataflyten i et flytskjema.

Vi anbefaler at du tar med følgende momenter i beskrivelsen av dataflyten i prosjektet:

- alle datakilder
- alle enheter og kanaler dataene skal innom
- om/hvordan data om enkeltpersoner fra ulike datakilder kobles
- om personopplysninger lagres sammen med eller adskilt fra datasettet
- hvor eventuell koblingsnøkkel lagres
- hvem som får tilgang til personopplysninger (institusjon og rolle). Prosjektleder må sørge for at det finnes en løpende oversikt over hvilke navngitte personer som til enhver tid har tilgang til hvilke personopplysninger og hvorfor slik tilgang er nødvendig. Husk å oppdatere tilganger ved endringer i prosjektgruppen.
- hvilke opplysninger de ulike mottakerne skal ha tilgang til og til hvilket tidspunkt
- hvorfor de får tilgang
- om publikasjoner vil inneholde anonyme eller personidentifiserende data
- hvordan prosjektet avslutter behandlingen av personopplysninger (sletting, anonymisering eller viderebehandling)

Videre bør du beskrive og vurdere følgende sikkerhetstiltak:

- vurderes for hver enhet og kanal som dataene flyter gjennom
- kan være tekniske og/eller organisatoriske
- skal være egnet til å sikre dataene mot uautorisert deling, endring og sletting
- må være bedre jo høyere personvernrisikoen er, se veilederens kapittel 13 om personvernkonsekvensvurdering (DPIA)

Beskrivelsen av dataflyt og vurderingen av sikkerhetstiltak må være god og riktig. Det kan være hensiktsmessig og i noen tilfeller nødvendig, å be om bistand fra IT-ressurser ved din institusjon for å sikre dette, særlig når dataflyten er kompleks og/eller kan innebære høy risiko. Du bør også rådføre deg med din institusjon dersom prosjektet skal bruke nytt utstyr, løsning eller leverandør som ikke allerede er vurdert av institusjonen. Vi anbefaler at du gjør dette i god tid før datainnsamling.

Se også [Normens faktaark 25 om lagringstid og sletting](#) og [Normens veileder om risiko](#).

Ved oppstart av et prosjekt er det gjerne mange prosesser som pågår samtidig som du skaffer deg oversikt over dataflyten, f. eks utarbeidelse av søknader, informasjon- og samtykkeskriv mv. Du må da huske på at det skal være samsvar mellom dataflyten i

prosjektet og den informasjonen du gir til den registrerte og REK, Helsedataservice, Helsedirektoratet, SLV mv.

## 9. Dele data?

### 9.1 Hva vil det si å dele data?

Før oppstart av prosjektet, må du avklare om prosjektet skal dele data med andre, underveis eller etterpå. Med deling av data mener vi her alle former for deling. Du kan se for deg at du som prosjektleder samler inn dataene til prosjektet. For hver person du deler disse dataene med for prosjektformålet eller andre formål, internt eller eksternt, må du vite hvilke mottakere du deler med, hva deres rolle er, og hva som er formålet med delingen.

### 9.2 Hvilke mottakere skal data deles med, for hvilke formål?

Vi anbefaler at du først kartlegger hvilke personer og institusjoner som trenger tilgang til data for å få gjennomført prosjektet, i lys av prosjektformålet som du har beskrevet (i kapittel 3).

Her kan du stille deg følgende spørsmål:

- Hvem trenger tilgang til data for at prosjektet skal kunne gjennomføres?
- Hvem av dem trenger tilgang til personopplysninger? Og hvem kan utføre sine oppgaver ved hjelp av anonyme opplysninger?

Deretter må du vurdere om det er aktuelt å dele data for andre formål, enten underveis i prosjektperioden, eller etterpå. Her vil disse spørsmålene være nyttige:

- Skal du eller andre som har tilgang til prosjektets data (for å gjennomføre prosjektet), bruke prosjektdataene til andre formål?
- Skal personer/institusjoner som ikke jobber i prosjektet få utlevert data fra prosjektet?
- Hvilke andre formål skal prosjektdataene brukes til?
- Hvilke mottakere skal bruke prosjektdataene til hvilke formål?
- Er det nødvendig at de aktuelle mottakerne får data med personopplysninger, eller får de oppfylt sine formål hvis du kun deler anonyme data?

### 9.3 Dele personopplysninger eller anonyme opplysninger?

For hver mottaker må du, som vist over, ta stilling til om mottakeren trenger dataene med eller uten personopplysninger. Du kan bare dele personopplysninger hvis det er nødvendig. Hvis mottakeren kan løse sine oppgaver (i prosjektet eller til andre formål) ved hjelp av anonyme data, skal du bare dele anonyme data fra prosjektet med denne mottakeren.

Når du skal ta stilling til om data som skal deles vil inneholde personopplysninger eller ikke, er det viktig å gjøre en grundig vurdering. Det er lett å trå feil og utlevere personidentifiserbare data som man tror er anonyme. Hvis du deler personopplysninger fra prosjektet uten å være klar over det, får du ikke tatt de nødvendige forholdsreglene for å forsikre deg om – og dokumentere – at delingen er lovlig (se avsnittene under). Som prosjektleder må du være klar over at en slik uautorisert deling av personopplysninger er

ulovlig. Det vil blant annet innebære brudd på personopplysningsikkerheten som kan være varlingspliktig til Datatilsynet. Vi anbefaler derfor at du ser nøye på definisjonene av personopplysninger vs. anonyme opplysninger i kapittel 5.1 og 5.2, når du vurderer hvilke mottakere som skal ha tilgang til personopplysninger. Vi anbefaler også at du rådfører deg med din institusjon hvis du er usikker på om dataene du skal dele vil inneholde personopplysninger eller ikke.

## 9.4 Når du skal dele personopplysninger for prosjektformålet

Hvis du har kommet frem til at det er nødvendig å dele personopplysninger med andre for å få gjennomført prosjektet (dvs. oppfylle prosjektformålet), er det flere forhold du må sikre og dokumentere.

For det første må du kartlegge rollene til de ulike personene som bidrar i prosjektet. Du må ha oversikt over hvem som skal få tilgang til personopplysninger, og hvilke opplysninger hver av dem trenger for å utføre sine oppgaver. Enkelt sagt kan du ikke dele alt med alle, bare fordi de har en tilknytning til prosjektet. Tilgangen må differensieres ut fra hvilke oppgaver de har i prosjektet.

Vi kan nevne noen eksempler for å illustrere dette. En medarbeider som skal oppsummere forskningsfunnene trenger kanskje bare tilgang til anonyme analyseresultater for å utføre sin oppgave. Medarbeidere som skal analysere data, derimot, vil kanskje trenge hele datasettet, med alle bakgrunnsvariabler og prosjekt-ID for hver forskningsdeltager (indirekte personopplysninger), men de trenger gjerne ikke navn på deltagerne. Tilgang til navnene og koblingsnøkkelen trenger kanskje bare du som prosjektleder, evt. også en administrativt ansatt i ditt fravær. Disse eksemplene er ikke uttømmende, og det finnes mange ulike måter å organisere tilgangene på. Men de viser at det kan variere fra person til person i prosjektet hvilke prosjektdata de trenger tilgang til. Prosjektet må ha en dokumentert oversikt over hvilke prosjektmedarbeidere som har tilgang og hvorfor.

For det andre må du ha oversikt over om prosjektdata med personopplysninger skal deles kun med prosjektmedarbeidere som er ansatt internt ved din institusjon, eller om slike data også skal deles med ansatte ved andre institusjoner. Det kan for eksempel være nødvendig å dele personopplysninger med eksterne prosjektmedarbeidere, samarbeidspartnere og/eller leverandører for å få gjennomført prosjektet.

Vær oppmerksom på at når du som prosjektleder deler personopplysninger med ansatte ved en annen institusjon for å oppfylle prosjektformålet, gjør du dette på vegne av din institusjon. Ved slike samarbeid må det foreligge en skriftlig avtale mellom de to institusjonene (se kapittel 15.1 til 15.4). For at dere skal inngå rett type avtale, må du og din institusjon vite hvilken rolle mottakerinstitusjonen har. Se definisjonene i kapittel 6 om roller og ansvar, og finn ut hvilken rolle hver av de eksterne mottakerne har i ditt prosjekt. Den andre institusjonen vil ha rolle enten som databehandler eller som fellesansvarlig, avhengig av hvem som bestemmer formålet (hvorfor) og midlene (hvordan) for behandlingen av personopplysningene i prosjektet. Hvis prosjektet ditt benytter leverandører som kun får tilgang til personopplysninger uten å bruke dem til egne formål, definerer du disse mottakerne som databehandlere (f.eks. nettskjema, videosamtale, analyseinfrastruktur, lagringstjenester, skytjenester). Hvis institusjonene du deler med derimot samarbeider, slik at dere – helt eller delvis – bestemmer formål og midler i fellesskap, er de felles dataansvarlige sammen med din institusjon.



For det tredje må du finne ut om personopplysninger fra prosjektet skal deles med internasjonale institusjoner eller institusjoner som er etablert i land utenfor EU/EØS. Det kan f.eks. være tilfelle hvis prosjektet benytter leverandører av skytjenester, eller samarbeider med utenlandske forskere som skal bistå med analyser av data. Hvis personopplysninger deles utenfor EU/EØS, må dere ha eget rettslig grunnlag for denne overføringen.

Når du deler personopplysninger fra prosjektet som forklart over, er det viktig at du følger interne retningslinjer ved din institusjon. Institusjonen har gjerne rutiner både for å dokumentere prosjektmedarbeideres tilganger, for samarbeid med databehandlere og fellesansvarlige, og for overføringer til tredjeland. Institusjonen din har gjerne også lagringsguider, der du får vite hvilke IT-utstyr/-tjenester du kan bruke for å behandle typer opplysninger, og hvilke leverandører din institusjon allerede har databehandleravtale med (slik at du ikke trenger egen avtale for ditt prosjekt).

Hvis du er usikker, eller du ikke finner retningslinjer som gir svar på hvordan og med hvem du kan dele personopplysninger i ditt prosjekt, rådfør deg med personvernressurser ved din institusjon.

## 9.5 Når du eller andre skal bruke personopplysninger fra prosjektet til andre formål

Hvis du eller andre skal bruke personopplysninger fra prosjektet til andre formål, er det også flere forhold du og din institusjon må sikre og dokumentere.

Vær oppmerksom på at det kan være vanskelig å vurdere om slike delinger er lovlige, og at konsekvensene av feilvurderinger kan være alvorlige, både for prosjektet ditt, institusjonen din, og for de registrerte som prosjektet behandler personopplysninger om. Hvis det er aktuelt å dele personopplysninger fra prosjektet for andre formål, bør du derfor rådføre deg med din institusjon for bistand. Da forankrer du vurderingen av at viderebehandlingen er lovlig. Din institusjon har gjerne retningslinjer for slik deling som vil veilede deg. Her følger noen generelle råd:

Det kan være hensiktsmessig å kartlegge hvem mottakerne er først:

- Er det du selv eller medarbeidere i prosjektet som skal bruke personopplysninger fra prosjektet til andre formål? Eller skal personopplysninger fra prosjektet utleveres til personer/institusjoner som ikke selv deltar i prosjektet?
- Skal dataene deles kun med ansatte ved din institusjon? Eller skal data utleveres til andre institusjoner?
- Skal samarbeidsinstitusjoner (databehandler eller fellesansvarlig) i prosjektet selv bruke dataene de har tilgang til i prosjektet for egne formål som ligger utenfor prosjektformålet?
- Skal personopplysninger utleveres til internasjonale institusjoner eller institusjoner som er etablert i land utenfor EU/EØS?

Når dere har kartlagt hvilke mottakere som vil bruke personopplysninger fra prosjektet til egne formål, bør dere be om dokumentasjon fra hver mottaker, blant annet om:

- Hvilke formål har mottaker? Hva skal personopplysningene brukes til?
- Hvilke opplysninger trenger mottaker for sitt/sine formål?
- Hvilket rettslig grunnlag har mottaker for å behandle personopplysningene til sitt/sine formål?

Når dere har mottatt denne dokumentasjonen fra aktuelle mottakere, må dere finne ut om det er lov til å dele personopplysningene fra prosjektet til det nye formålet.

Det er viktig å være klar over at når personopplysninger deles for nye formål, skjer det i praksis to behandlinger av personopplysninger: selve delingen, og den videre bruken. Den som deler må vurdere at deres behandling (delingen) er lovlig. Og den som mottar må vurdere at deres behandling (den videre bruken) er lovlig.

Hvis dere deler data fra prosjektet, vil altså mottakeren vil være dataansvarlig for den videre behandlingen av personopplysninger. Hovedoppgaven for dere er å vurdere om selve utleveringen er lovlig. Dette må dere vurdere i lys av de juridiske rammene som gjelder for prosjektet. Her må dere se på de lovbestemmelsene, avtalene og tillatelsene som gjelder for behandlingen av personopplysninger i prosjektet, og vurdere om disse åpner for deling til andre formål, i så fall på hvilke vilkår. Dere må særlig vurdere hva som kan gi rettslig grunnlag for behandlingen (delingen) i personvernregelverket, og hvordan delingen kan skje i samsvar med reglene om taushetsplikt. Dere må også sørge for at delingen følger personvernprinsippene (som formålsbegrensning, dataminimering, sikkerhet), og at de registrertes rettigheter ivaretas (f.eks. at de informeres om delingen, med mindre det finnes lovlig unntak).

Ettersom hver deling til nye formål er å anse som en egen behandling av personopplysninger, vil det være hensiktsmessig å følge flytskjemaet vedlagt forskningsveilederen fra start for å finne ut hvilke forhold dere må kartlegge og vurdere før delingen. Det gjelder enten det er du selv eller andre ved din institusjon – eller det er eksterne ved andre institusjoner – som skal bruke opplysningene videre til andre formål.

## 10. Varighet – Hva skjer med personopplysningene etter prosjektslutt?

### 10.1 Hvor lenge er det nødvendig å behandle personopplysninger i prosjektet?

En sentral del av å planlegge prosjektet er å vurdere hvor lenge det er nødvendig å behandle personopplysninger for å oppnå prosjektets formål. Personopplysninger skal ikke lagres lenger enn det som er nødvendig for formålet.<sup>16</sup> Når du planlegger sluttdato er det imidlertid blant annet lurt å ta høyde for at det kan skje uplanlagte hendelser og forsinkelser, og at det kan ta tid å innhente tillatelser, få på plass avtaler, rekruttere projektdeltakere, få tilgang til data og publisere. Det kan også oppstå uplanlagte endringer i prosjektet som kan kreve nye

---

<sup>16</sup> Prinsippet om lagringsbegrensning, jf. personvernforordningen art. 5 nr. 1 bokstav b.



vurderinger knyttet til personvern, innhenting av tillatelser og ny informasjon til den registrerte.

Videre må du ta stilling til hvordan personopplysningene i datamaterialet skal håndteres når prosjektet avsluttes, herunder om de skal slettes, anonymiseres eller viderebehandles. I tillegg må du ta stilling til hvordan du skal gjennomføre publisering.

Mange prosjekter er omfattende ved at det behandles store mengder med personopplysninger og at de pågår over lang tid. I et prosjekts livsløp kan det være utskiftninger av prosjektleder og prosjektmedarbeidere. Dette vil kunne medføre økt risiko for at f. eks prosjektet ikke overholder de lovpålagte kravene om lagringstid og sletting til riktig tidspunkt. Videre kan det tekniske løsninger som brukes til både lagring og analyser videreutvikles, som muliggjør at enkeltpersoner kan identifiseres i datasett som tidligere er ansett som anonyme. Dette krever at både institusjoner og prosjekter har gode rutiner for hvordan personopplysninger skal håndteres ved prosjektslutt.

## 10.2 Hvordan skal du håndtere personopplysningene etter prosjektslutt?

### 10.2.1 Sletting

Som nevnt over er utgangspunktet at personopplysninger ikke skal lagres lenger enn det som er nødvendig for å oppnå formålet med prosjektet, og derfor skal slettes ved prosjektslutt. Før du legger en plan for hvordan personopplysningene skal slettes, må du undersøke om prosjektet omfattes av lovfestede krav og/eller retningslinjer om arkiveringsplikt. Eksempler på dette er REK sin adgang til å fastsette vilkår om at prosjektet skal oppbevaring av dokumentasjon 5 år etter prosjektslutt i helseforskning av hensyn til etterkontroll.<sup>17</sup> Det er imidlertid viktig å merke seg at data kun skal lagres av hensyn til etterkontroll, og ikke brukes av prosjektleder eller andre i perioden mellom prosjektslutt- og slettedato. Videre er andre eksempler krav til oppbevaring av dokumentasjon på 25 år i legemiddelstudier<sup>18</sup> og retningslinjene Good Clinical Practice (GCP). Merk her at GCP ikke er i strid med prinsippet om lagringsbegrensning i personvernforordningen.

Se også Normens [faktaark 25 om lagringstid og sletting](#).

### 10.2.2 Anonymisering

Hvordan personopplysninger anonymiseres er beskrevet under veilederens kapittel 5.2.2. Kort oppsummert innebærer dette at personopplysninger i et datasett må slettes eller omskrives slik at det ikke lenger er mulig å gjenkjenne enkeltpersoner, verken direkte eller indirekte. Anonymisering kan være en krevende prosess, og det f. eks ikke alltid tilstrekkelig å slette kodenøkkel, du må også vurdere om datasettet i seg selv er egnet til å identifisere enkeltpersoner. Dersom du er usikker på hvordan du skal anonymisere personopplysninger, eller om du har fått det til anbefaler vi at du rådfører seg med personvernressurser i din institusjon.

---

<sup>17</sup> Helseforskningsloven § 38

<sup>18</sup> EUs forordning for kliniske studier (Clinical Trials Regulation, no. 536/2014) artikkel 58

### 10.2.3 Viderebehandling

På visse vilkår kan det også være adgang til å viderebehandle personopplysninger for forskningsformål. Her er det blant annet sentralt å avklare hva formålet med viderebehandlingen er, hvilken informasjon som er gitt til den registrerte og/eller hvilket rettslig grunnlag den opprinnelige behandlingen av personopplysningene var basert på, samt hvem som er dataansvarlig. Dette er det lurt å vurdere allerede i planleggingen av prosjektet, og det anbefales at du rådfører deg med personvernressurser i din institusjon. Det vil også være nyttig å se til veilederens kapittel 3 om formål.

Det er også mulig å lagre opplysningene videre for gjenbruk i forskning på visse vilkår, her er det blant annet sentralt å avklare hvilke formål det er ønskelig å viderebehandle opplysningene for og hvem som er dataansvarlig. Hvis det er aktuelt, er det best å planlegge dette ved prosjektstart. Rådfør deg med ressurser i din institusjon.

Et annet spørsmål det bør tas stilling til i forbindelse med prosjektslutt er publisering. Dette står det mer om i veilederens kapittel 10.3.

## 10.3 Publisering

Med publisering mener vi her offentliggjøring, utgivelse eller kunngjøring. Det er vanlig å publisere fagartikler i forbindelse med både forsknings- og kvalitetsprosjekter.

Et forskningsprosjekt er i utgangspunktet forpliktet til å publisere, uavhengig av resultat. Plikten til å publisere resultater bygger på den akademiske frihet, samfunnsnyttene og rettighetene til forsker og forskningsansvarlig institusjon. Blant annet er forskning en akademisk ytring som har et særlig vern.<sup>19</sup> Ny kunnskap som frembringes gjennom forskning har betydning for samfunnet skal både deles og være tilgjengelig for etterprøvnbarhet. Hensynet til den registrerte tilsier imidlertid at resultater fra forskning ikke kan publiseres fritt. Ved publisering av resultater eller annen informasjon fra prosjektet må du vurdere om de opplysningene som kommer frem i publikasjonen er personopplysninger eller om de er anonyme, se også veilederens kapittel 5.2.2 om anonymisering. I tillegg vil både type og mengde data, samt hvilken form de skal publiseres i, som tabeller og figurer, også være relevante momenter som bør tas med i vurderingen.

Dersom du skal publisere anonyme opplysninger bør det lages en plan og dokumenteres hvilke tiltak prosjektet må gjøre for å sikre at opplysningene faktisk er anonyme.

Det kan være tilfeller der det er vanskelig å publisere opplysninger anonymt, f. eks i helseforskning som gjelder sjeldne sykdommer eller kasuistikker. Da må du avklare om prosjektet har et rettslig grunnlag for å behandle personopplysninger for formål om publisering. Dette vil som hovedregel være den registrertes samtykke. Det er derfor viktig at det oppgis at det er aktuelt å publisere resultater, så langt det lar seg gjøre hvilke data som skal publiseres, og om det er risiko for at den registrerte kan bli identifisert i publikasjonen, i informasjon- og samtykkeskrivet. Tilgjengeliggjøring av data for redaktører og fagfeller før publisering i vitenskapelige tidsskrift krever ikke spesifikt samtykke.<sup>20</sup>

I avsnittene over er forskning særlig omtalt, men de samme vurderingene vil ha overføringsverdi til publisering i forbindelse med andre type prosjekter.

---

<sup>19</sup> Personopplysningsloven § 3

<sup>20</sup> Helse- og omsorgsdepartementet: Rundskriv om informasjonshåndtering i spesialisthelsetjenesten

# 11. Informasjon til den registrerte

## 11.1 Prosjektet er forpliktet til å gi den registrerte informasjon

Når du behandler personopplysninger i et prosjekt, er hovedregelen at de registrerte har rett på informasjon om dette. Personvernlovgivningen stiller krav både til form, innhold og tidspunkt. Du må derfor legge en plan for hvordan prosjektet kan gi deltakerne god og forståelig informasjon til rett tid.

Etter å ha gjennomført stegene hittil i veilederen, har du skaffet god nok oversikt over hva prosjektet og behandlingen av personopplysninger vil innebære til at du kan starte arbeidet med å lage utkast til informasjon. Men vi anbefaler at du venter med å sende ut informasjonen til du har fullført flytskjema, og har alle nødvendige tillatelser og avtaler på plass, samt DPIA hvis det er påkrevd, ettersom disse kan gi vilkår om hvilken informasjon prosjektet må gi og hvordan.

Hvis det er umulig, svært vanskelig eller utilrådelig å gi informasjon til den registrerte, eller slik informasjon sannsynligvis vil ødelegge for prosjektformålet, finnes det enkelte unntak i loven som åpner for at prosjektet ikke trenger å informere dem. Men terskelen er relativt høy for å ikke informere de registrerte, og eventuelle unntak fra hovedregelen om informasjon må begrunnes og dokumenteres godt.

## 11.2 Når skal prosjektet gi informasjon?

Når prosjektet skal gi informasjon er det flere ting å huske på.

Det første er form. Informasjonen kan gis skriftlig eller muntlig. Men du må kunne dokumentere at de registrerte har fått informasjon, og hvilken informasjon som er gitt. Derfor vil det i de fleste tilfeller være fordelaktig å gi informasjonen skriftlig. Uavhengig av om prosjektet gir skriftlig eller muntlig informasjon, er det et absolutt krav at informasjonen er lett forståelig for den registrerte. Informasjonen bør være kortfattet og må formidles på et språk som den registrerte forstår. Det kan være nødvendig å legge inn en ekstra innsats for klarspråk og språklige tilpasninger, for å forsikre seg om at informasjonen blir forstått. Det kan også være et godt tiltak å gå igjennom informasjonen muntlig sammen med den registrerte (f.eks. før intervju), selv om informasjonen er gitt skriftlig på forhånd. Det er også viktig at informasjonen gis via kanaler der den faktisk når frem til dem som skal motta den. Informasjonen må gis individuelt til hver deltaker. Det er *ikke* tilstrekkelig å gi kollektiv informasjon for å oppfylle den registrertes rett til informasjon (les mer under unntak).

Det andre er innhold. Regelverket stiller krav til hva du må informere om. Den registrerte har rett til informasjon om:

- Hvem som er forsknings- og dataansvarlig institusjon (kontaktopplysninger- og personer i alle deltakende institusjoner)
- Hvorfor personopplysningene skal behandles (formål), hvor lenge, og på hvilket lovgrunnlag opplysningene behandles,
- Hvem som vil få tilgang til personopplysningene (mottakere),

- Hvilke datakilder opplysningene hentes fra
- Hvilke rettigheter den registrerte har: innsyn/kopi, retting, sletting, protest/trekke samtykke, og at den registrerte kan klage på behandlingen til Datatilsynet
- Kontaktopplysninger til personvernombudet ved din institusjon
- Lovlig grunnlag for å overføre personopplysningene ut av EU/EØS (hvis aktuelt)
- Planer om utlevering/viderebehandling av opplysningene til andre formål (hvis aktuelt)

Det tredje er tidspunktet. Hvis prosjektet skal samle data direkte fra de registrerte, må du gi informasjonen før datainnsamlingen starter. Dette vil for eksempel være tilfelle ved datainnsamling gjennom intervju, spørreskjema, deltakende observasjon, medisinske/andre tester, biologiske prøver og andre former for datainnsamling der prosjektet får personopplysningene direkte fra den det gjelder. De registrerte er da aktive deltakere i prosjektet, og må på forhånd ha fått vite hva deltakelsen innebærer og hvordan personopplysningene deres vil bli behandlet. Hvis prosjektet ikke samler data direkte fra de registrerte, men innhenter opplysninger om dem fra andre datakilder, må du informere de registrerte senest en måned etter at datainnsamlingen har startet, eller (hvis aktuelt) senest når opplysningene skal utleveres til andre, eller prosjektet skal kontakte de registrerte. Sistnevnte kan f.eks. være aktuelt når prosjektet behandler personopplysninger for å trekke og/eller rekruttere et utvalg som blir spurt om å delta i intervju. I informasjonen som blir gitt til utvalget må det da beskrives hvordan personopplysninger ble behandlet ifm. rekruttering.

Det finnes flere ressurser å støtte seg på, når du skal utarbeide informasjon til de registrerte. Sikt personverntjenester har utarbeidet maler for informasjonsskriv i forskning: [Informasjon til deltakarane i forskningsprosjekt \(sikt.no\)](#). REK har utarbeidet maler for informasjonsskriv i helseforskning: [Hjem - Insights \(rekportalen.no\)](#). Se også [Normens veileder om de registrertes rettigheter](#).

## 11.3 Unntak fra retten til informasjon

Som nevnt åpner loven for at prosjekter i enkelte situasjoner kan behandle personopplysninger uten å gi individuell informasjon til de registrerte. Her er de aktuelle unntakene for forskning og kvalitetssikring:

- Den registrerte har allerede fått informasjonen
- Det er umulig eller krever uforholdsmessig stor innsats å informere
- Informasjon vil sannsynligvis ødelegge for formålet (forskning/kvalitetssikring)
- Dataansvarlig er lovpålagt å behandle personopplysningene
- Det er utilrådelig å informere, av hensyn til den registrertes helse eller forhold til nærpå personer

Hver av disse unntakene er nærmere forklart i lovhjemler, der det også er forklart hvilke vilkår som må være oppfylt for at unntaket skal kunne anvendes. Hvis det er aktuelt å gjøre unntak fra retten til informasjon i ditt prosjekt, må du passe på å dokumentere hvilken lovhjemmel for unntak som er aktuell, og at vilkårene i denne lovhjemmelen er oppfylt. Det er svært viktig at prosjektet har en gyldig begrunnelse for å gjøre unntak – ved at den faktiske situasjonen i prosjektet stemmer overens med vilkårene i loven, og at dette er godt nok dokumentert. Vi anbefaler derfor at du rådfører deg med din institusjon for å få dette på plass.

Det mest brukte unntaket i fra informasjon i forskning/kvalitetssikring er at det er umulig eller uforholdsmessig vanskelig å informere. Dette gjelder typisk i prosjekter som samler inn data fra andre kilder enn den registrerte, og der utvalget er stort og/eller prosjektet ikke har tilgang til kontaktinformasjon. Hvis prosjektet samler data fra de registrerte og/eller utvalget er lite og man har kontaktinformasjon, er det vanskelig å argumentere for at dette unntaket fra informasjon kan brukes.

Et annen begrunnelse for unntak fra informasjon som kan være aktuell, er at informasjon til de registrerte sannsynligvis vil ødelegge for formålet. Dette kan f.eks. være aktuelt i eksperimenter der det kan påvirke deltakernes adferd hvis de på forhånd får vite hva som skal utforskes, slik at det ødelegger datavaliditeten. En løsning kan da være å informere deltagerne om de fleste forhold på forhånd (inkludert det overordnede forskningstemaet og at det er et eksperiment der de ikke kan få vite alt på forhånd), og supplere med informasjon om det nøyaktige formålet etter datainnsamlingen. Dette unntaket kan også være aktuelt dersom prosjektet er avhengig av et representativt utvalg og det vil ødelegge mye for formålet hvis registrerte trekker seg.

Vær oppmerksom på at det er påkrevd å gi kollektiv informasjon hvis prosjektet ikke kan gi individuell informasjon fordi det er umulig, uforholdsmessig vanskelig, og/eller kan ødelegge forskningsformålet. Prosjektet må kunne dokumentere unntak fra individuell informasjon, ettersom kollektiv informasjon ikke er tilstrekkelig for å oppfylle de registrertes rett til informasjon. Kollektiv informasjon gis som et tiltak for å bøte på ulempene de registrerte har ved å ikke få informasjonen individuelt. Kravet om kollektiv informasjon innebærer at prosjektet må utarbeide informasjon om hvordan prosjektet behandler personopplysninger, og forsøke å nå ut med denne informasjonen slik at den når ut til flest mulig av de registrerte. Det er gjerne anbefalt å publisere informasjonen på hjemmesidene til institusjonen som er ansvarlig for prosjektet, men dette er ofte ikke tilstrekkelig. Prosjektet må også legge ut informasjonen i kanaler/nettsider *som det er sannsynlig* at de registrerte leser. Det kan f.eks. være nettsidene til interesseorganisasjonen de er en del av, oppslag på skolen eller arbeidsplassen der utvalget er rekruttert, eller liknende. Informasjonen må utformes på samme måte som beskrevet over med hensyn til form og innhold. Den skal være forståelig for de som mottar den, og den må gi en dekkende beskrivelse av behandlingen av personopplysninger i tråd med punktlisten over.

Vær oppmerksom på at unntaket "utilrådelig" skal brukes med forsiktighet. Terskelen for å ikke informere den registrerte av slike grunner er høy. Det er f.eks. ikke tilstrekkelig at den registrerte er syk eller kan bli opprørt av informasjon om prosjektet. Hvis du mener dette unntaket er aktuelt i prosjektet, anbefaler vi at du rådfører deg med personvernressurser ved din institusjon.

## 12. Den registrertes rettigheter

Når prosjektet behandler personopplysninger, har de registrerte flere personvernrettigheter.

Ved siden av retten til informasjon (omtalt over), vil de ha rett til innsyn, retting og sletting av egne personopplysninger. De har også rett til dataportabilitet (når samtykke utgjør rettslig grunnlag for behandlingen), eller rett til å protestere mot behandlingen (når behandlingen har annet rettslig grunnlag). Alle registrerte har i tillegg rett til å kreve begrensning av

behandlingen, og rett til vern mot automatiserte avgjørelser (sistnevnte er lite aktuell i forskning/kvalitetssikring). Du kan lese mer om rettighetene i Normens [veileder for rettigheter ved behandling av helse og personopplysninger](#).

Prosjektet må tilrettelegge for at den registrerte kan utøve disse rettighetene.

Retten til informasjon er omtalt i et eget kapittel (11) over, fordi du før oppstart av prosjektet må gjøre en konkret forhåndsvurdering av hvordan prosjektet kan innfri denne rettigheten, eventuelt om unntak gjør seg gjeldende. En slik generell forhåndsvurdering kan du vanskelig gjøre for de øvrige personvernrettighetene. Den konkrete vurderingen av om rettighetene skal innfris eller om unntak gjelder, må du – i samråd med institusjonen din – gjøre hvis en registrert tar kontakt og ønsker å utøve rettighetene.

Det du må gjøre før oppstart av prosjektet, er å organisere prosjektet slik at de registrerte kan utøve rettighetene sine.

For det første er det viktig at du kjenner til følgende:

- Rettighetene gjelder så lenge de registrerte kan identifiseres i datamaterialet.
- Hovedregelen er at rettighetene gjelder. Loven åpner for unntak fra rettighetene i enkelte situasjoner, men avslag må ikke gis uten begrunnelse og lovhjemmel.
- Innsyn må kun gis til den som personopplysningene gjelder, ikke til andre. I noen tilfeller kan det være vanskelig å vurdere hvem som har rett til innsyn i hvilke opplysninger. Det vil f.eks. gjelde prosjekter som behandler personopplysninger om deltager/tredjeperson, og prosjekter der barn deltar og foreldre forvalter personvernrettighetene på deres vegne.
- Feilvurdering av rettigheter kan føre til ulovlig behandling. Rådfør deg med din institusjon, særlig før du gir innsyn eller avslag.
- Institusjonen din har plikt til å vurdere om rettighetene skal/kan innfris, og svare den registrerte innen en måned.
- Du bør før oppstart av prosjektet ha gjort deg kjent med hva hver rettighet innebærer. Vi anbefaler derfor at du leser om rettighetene i Normens faktaark.
- Du bør også ha kartlagt hvilke rettigheter som i utgangspunktet gjelder i ditt prosjekt (avhengig av behandlingsgrunnlag), og i hvilke situasjoner unntak fra rettighetene kan gjøre seg gjeldende. Denne kartleggingen er i noen tilfeller nødvendig for å kunne gi rett informasjon til de registrerte, bl.a. om hvem som har innsynsrett (jf. eksemplene over).

For det andre må prosjektet ha på plass en infrastruktur som gjør at det mulig for de registrerte å ta kontakt og få behandlet sin henvendelse på rett måte:

- Når du informerer om prosjektet (individuell eller kollektivt), må den registrerte få kontaktinformasjon til prosjektansvarlige og personvernombud, slik at de vet hvor de kan henvende seg for å utøve rettighetene.
- Data bør lagres slik at prosjektet lett kan gjenfinne opplysningene om den registrerte (f.eks. via en koblingsnøkkel som prosjektet har – eller kan få – tilgang til). Vær likevel oppmerksom på at prosjektet ikke skal lagre flere personopplysninger enn nødvendig for formålet, bare for å kunne innfri rettighetene.
- Du og andre kontaktpersoner (ved egen eller samarbeidende institusjoner) må vite hva dere skal gjøre hvis registrerte henvender seg, slik at de får rett svar innen tidsfristen.



- Institusjonen din må ha kompetanse om reglene som gjelder for de registrertes rettigheter, slik at dere gjør riktige vurderinger og oppfyller rettighetene når de gjelder, og unntar fra rettighetene når det er lovlig grunnlag for det.

## 13. Personvernkonskvensvurdering (DPIA)

Før oppstart av prosjektet må du – i samråd med institusjonen din – vurdere om det er nødvendig å utføre en personvernkonskvensvurdering (DPIA). DPIA er et verktøy for å kartlegge og håndtere risikoer knyttet til behandling av personopplysninger. Målet er å redusere risikoen til et akseptabelt nivå, slik at behandlingen av personopplysninger kan gjennomføres, samtidig som prosjektet ivaretar rettighetene og frihetene til de personene dere forsker på.

DPIA er ikke nødvendig i alle prosjekter som behandler personopplysninger. Det er påkrevd før oppstart av en behandling av personopplysninger som “sannsynligvis gir høy risiko for de registrertes rettigheter og friheter”. Du må altså vurdere om dette gjelder i ditt prosjekt. Ved å følge stegene hittil i veilederen, har du kartlagt forhold ved prosjektet ditt som gjør deg i stand til å foreta denne vurderingen.

Hva som regnes som “høy risiko” er definert i personvernforordningen art. 35. Her står det blant annet at DPIA er nødvendig før særlige kategorier eller strafferettslige personopplysninger behandles i stor skala, og før systematisk overvåking i stor skala av et offentlig tilgjengelig område. EUs personvernråd (EDPB) og Datatilsynet har utgitt egne veiledere om gir utfyllende forklaringer på hvordan man går frem for å vurdere hva som er høy risiko.

I sin veileder lister EDPB opp ni kriterier for hva som gir høy risiko, og forklarer at jo flere av kriteriene som gjelder for behandlingen av personopplysninger, desto mer sannsynlig er det at DPIA er påkrevd.

Etter EDPB-kriteriene skal DPIA vurderes hvis prosjektet:

- behandler sensitive personopplysninger (særlige kategorier, straffedommer/lovovertrædelser, eller svært personlig karakter)
- behandler personopplysninger i stor skala (mht. utvalgsstørrelse, mengde opplysninger, varighet, frekvens)
- behandler personopplysninger om sårbare registrerte
- sammenstiller datasett (f.eks. datakilder med ulike formål/dataansvarlige) som overstiger den registrertes rimelige forventninger
- innebærer at de registrerte hindres i å utøve sine rettigheter
- innebærer innovativ bruk av ny teknologi eller organisatorisk løsning
- innebærer evaluering (profilering/kartlegging av personopplysninger for å analysere eller forutsi personers adferd, helseforhold, preferanser, interesser, evner, behov el.)
- innebærer systematisk monitorering (ulike former for observasjon/sporing av personer, bl.a. på internett/offentlig område, f.eks. kameraovervåking, observasjon av

internettaktivitet, lokasjonssporing og helseovervåking ved hjelp av sensorer og applikasjoner)

I tillegg til disse kriteriene, har Datatilsynet utarbeidet en liste over behandlinger av personopplysninger som krever DPIA. Vi har laget en kortversjon av Datatilsynets liste som følger under. Datatilsynets veiledning og listen i sin helhet finner du her: [Veiledning om DPIA | Datatilsynet](#)

Oppsummert, må dere ifølge Datatilsynet gjennomføre DPIA hvis prosjektet faller inn under ett eller flere av disse punktene:

1) Personopplysninger behandles slik, i følge med ett annet EDPB-kriterium (jf. over):

- samles inn via tredjepart
- i stor skala gjennom «tingenes internett» / velferdsteknologi
- biometriske opplysninger for å identifisere enkeltpersoner
- med innovativ teknologi
- genetiske opplysninger
- lokasjonsdata
- uten samtykke til forskningsformål

**eller**

2) Personopplysninger behandles:

- for systematisk monitorering av ansatte
- for å evaluere læring, mestring og trivsel i skoler eller barnehager
- ved å systematisk monitorere effektivitet, ferdigheter, kunnskap, mental helse og utvikling
- for å tilby tjeneste/utvikle produkter for kommersiell bruk som involverer evaluering av svært personlige opplysninger (forutsi jobbprestasjoner, økonomi, helse, pålitelighet, adferd, personlige preferanser/interesser, lokasjon eller bevegelsesmønster)
- i form av systematisk monitorering på offentlige områder i stor skala (inkl. kameraovervåking)
- i form av kameraovervåking i skoler/barnehager i åpningstid
- i stor skala for algoritmetrening og inkluderer særlige kategorier/svært personlige opplysninger

Hvis prosjektet ditt oppfylder et eller flere av EDPB-kriteriene over, og/eller faller inn under et av punktene på Datatilsynets liste, må prosjektet trolig ha DPIA. Vi anbefaler da at du rådfører deg med din institusjon eller personvernombud for å finne ut om DPIA er nødvendig. Det samme gjelder hvis du er usikker på om prosjektet oppfylder kriteriene. Sjekk også hvilke retningslinjer som gjelder for vurdering av DPIA ved din institusjon.

Hvis prosjektet trenger DPIA, følger du prosedyrene ved din institusjon. DPIA er vanligvis ikke noe du skal sitte med alene. Som regel utfører du DPIA i samarbeid med personvern- og IT-ressurser ved din institusjon. Det finnes flere gode veiledere om hvordan man konkret går frem for å gjennomføre DPIA:

- Datatilsynet har en egen veileder om dette: [Veiledning om DPIA | Datatilsynet](#)
- Direktoratet for e-helse har utgitt [Mal og veiledning for utfylling av personvernkonsekvensvurdering \(DPIA\) - ehelse.](#)

- Hvis du skal melde prosjekt til Sikt, utarbeider Sikt en DPIA for prosjektet i samarbeid med deg, basert på Sikt sin DPIA-mal.

Kort fortalt er DPIA er en prosess, der dere beskriver den planlagte behandlingen og vurderer om den er lovlig og forholdsmessig. Deretter kartlegger dere risikoer, og foreslår risikoreduserende tiltak. Personvernombudet skal rådføres, før resultatet av DPIA fremlegges i et dokument for ledelsen ved din institusjon. Ledelsen skal så vurdere om DPIA er godt nok utført, og om risikoen er akseptabel, slik at prosjektet kan starte. Hvis ledelsen kommer til at risikoen ikke er akseptabel, kan ledelsen bestemme at DPIA må revideres, eller at behandlingen må forhåndsdrøftes med Datatilsynet, eventuelt ikke igangsettes.

Husk at det kan være nyttig å undersøke om det er gjennomført DPIA i lignende prosjekter som har brukt samme metodikk og behandling av personopplysninger, og som inneholdervurderinger du kan gjenbruke. Det er imidlertid viktig at vurderingene i DPIA tilpasses ditt prosjekt.

I prosjekter der flere institusjoner deltar, f.eks. multisenterstudier, er det viktig at dere vurderer om DPIA bør gjennomføres i samarbeid med de andre institusjonene. Først må dere identifisere hvilke av institusjonene som er dataansvarlig for behandlingen av personopplysninger som utgjør høy risiko. Hvis flere institusjoner i fellesskap er ansvarlige for behandlingen, er det som regel ingenting i veien for at en av partene påtar seg å utarbeide utkast til DPIA, så fremt alle er enige om det. Men DPIA bør forankres (med eventuelle lokale tilpasninger) hos alle dataansvarlige, ved at ledelsen signerer.

Hvis personvernkonsekvensene fortsatt er for høye etter at DPIA er utført, og institusjonen(e) vil gjennomføre behandlingen av personopplysninger, er det påkrevd å forhåndsdrøfte behandlingen med Datatilsynet før oppstart. Datatilsynet kan da gi råd og/eller sette vilkår for behandlingen.

## 14. Tillatelser

### 14.1 Oversikt over tillatelser

Basert på kartleggingen du har gjort i prosjektet, særlig knyttet til personopplysninger, prosjekttype og behandlingsgrunnlag, må du undersøke om prosjektet trenger å innhente godkjenning fra en eller flere instanser. Under er det laget en oversikt over de ulike tillatelsene.

Tillatelsene under gjelder for alle typer prosjekt, med mindre annet er spesifisert. I noen tilfeller må du sende søknader til flere instanser. Merk da at alt du søker til REK om, sendes i samme søknad, f. eks (vedtak om forhåndsgodkjenning for helseforskning, dispensasjon fra taushetsplikt og forskningsbiobank). Hvis du er usikker på hvilke godkjenninger og tillatelser prosjektet trenger, kontakt din institusjon i god tid før datainnsamling.

Helseforskning:

Vedtak om forhåndsgodkjenning fra REK

Klinisk utprøving av legemidler og medisinsk utstyr og ytelsesstudier av in-vitro diagnostisk utstyr:

Vedtak om godkjenning fra Statens legemiddelverk (SLV), inkludert godkjenning fra REK KULMU

#### Bruk av humant biologisk materiale

- I helseforskning, annen forskning, kvalitetssikring på tvers av virksomheter og medisinske kvalitetsregister: Vedtak om godkjenning fra REK
- I intern kvalitetssikring og befolkningsbaserte helseundersøkelser (opprettelse av biobank): Melding må sendes til biobankregisteret ved FHI

#### Helseopplysninger fra pasientjournal eller andre behandlingsrettede registre der det ikke innhentes samtykke fra den registrerte:

- Til helseforskning eller annen forskning: Vedtak om dispensasjon fra taushetsplikten fra REK
- Til kvalitetssikring på tvers av virksomheter: Dispensasjon fra taushetsplikten fra Helsedirektoratet.

Med "samtykke" menes samtykke fra den enkelte registrerte i forkant av behandlingen av personopplysninger. Hvis det er nødvendig å gjøre oppslag i pasientjournal for å rekruttere deltakere til et prosjekt, må prosjektet få et vedtak om dispensasjon fra taushetsplikten for dette, selv om den registrerte i etterkant samtykker til deltakelse (f. eks intervju).

#### Helseopplysninger fra helseregistre omfattet av Forskrift om nasjonal løsning for tilgjengeliggjøring av helsedata:

- Vedtak fra om tilgjengeliggjøring av helseopplysninger fra Helsedataservice
- Vedtak om dispensasjon fra taushetsplikten for helseopplysninger fra helseregistre, eventuelt som skal sammenstilles med helseopplysninger fra pasientjournal eller andre behandlingsrettede registre. Her vil det også være Helsedataservice som fatter vedtaket.

Helsedataservice kan fatte vedtak om tilgjengeliggjøring og dispensasjon fra taushetsplikten for følgende helseregistre: Dødsårsaksregisteret, Kreftregisteret, Medisinsk fødselsregister, Meldingssystem for smittsomme sykdommer (MSIS), System for vaksinasjonskontroll (SYSVAK), Norsk pasientregister (NPR), Nasjonalt register over hjerte- og karlidelser, System for bivirkningsrapportering, Kommunalt pasient- og brukerregister (KPR), Legemiddelregisteret og Helsearkivregisteret.

#### Helseopplysninger fra registre som ikke er omfattet av forskriften over:

- Vedtak fra registerforvalter om tilgjengeliggjøring
- Til forskning og annen forskning: Dispensasjon fra taushetsplikten fra REK
- Til kvalitetssikring på tvers av virksomheter: Dispensasjon fra taushetsplikten fra Helsedirektoratet

#### Andre taushetsbelagte personopplysninger der det ikke innhentes samtykke:

Vedtak fra aktuelt fagdepartement eller direktorat (f. eks NAV, Bufdir, UDI og SSB mv.)

#### Helseopplysninger til intern kvalitetssikring:

For intern kvalitetssikring gir helsepersonelloven § 26 og pasientjournalloven § 6 unntak fra taushetsplikten. Du trenger derfor ikke vedtak om dispensasjon. Det er likevel viktig å dokumentere at gjennomføringen av prosjektet og behandlingen av personopplysninger er

forankret hos institusjonens ledelse. Vi anbefaler at du følger interne rutiner ved din institusjon mht. dette.

#### Særlig om datainnsamling ved observasjon i helse- og omsorgstjenesten:

I noen prosjekter er det ønskelig å samle inn ved observasjon i helse- og omsorgstjenesten. Dette kan f. eks være et helsetjenesteforskningsprosjekt der formålet er å se på hvordan helsepersonell kommuniserer og fatter avgjørelser på en spesifikk avdeling ved et sykehus. For slike tilfeller er det ingen adgang til å fatte dispensasjon fra taushetsplikten i helsepersonelloven § 29, noe som innebærer at det må innhentes samtykke fra den registrerte (pasienten) eller pårørende. Merk at det ikke vil være tilstrekkelig å innhente samtykke fra den registrerte i etterkant av en observasjon.

## 14.2 Noen tips til søknadsprosessen

Det lønner seg å begynne arbeidet med å utarbeide og sende søknader så tidlig som mulig, og i god tid før datainnsamlingen. Dersom du må sende flere søknader vil det være en fordel å sende søknadene samtidig, dette gjør du når du sender søknad til Helsedataservice om tilgjengeliggjøring av helseopplysninger i f. eks helseforskning. Du bør være nøye med å svare ut de spørsmålene søknadsskjemaet stiller og beskrive prosjektet på samme måte i samtlige søknader, se veilederens kapittel 3 om formål.

Når du utarbeider søknader bør du være så konkret som mulig, det er f. eks viktig å kommunisere både hvilken kilde og hvilke data du ber om å få tilgjengeliggjort, se kapittel 4 og 5 om data og personopplysninger. Det er f. eks ikke tilstrekkelig å oppgi at du ønsker tilgang til Kreftregisteret i forbindelse med en søknad om dispensasjon fra taushetsplikten i kvalitetssikring på tvers av virksomheter, du må konkret vise til hvilke opplysninger du trenger. Det er også viktig å løfte blikket og få frem samfunnsnyttens prosjektet ditt gir.

Videre er det viktig å være grundig når du skal begrunne hvorfor det ikke kan innhentes samtykke når du sender søknad om dispensasjon fra taushetsplikten. Det kan også forekomme at det er ulike grupper registrerte det skal samles inn data fra. Noen grupper er det mulig å innhente samtykke fra, mens andre vil det være mer vanskelig. Det er da viktig å differensiere mellom disse gruppene når du gir begrunnelsen for hvorfor samtykke ikke skal innhentes. Videre er det viktig å få frem både fordeler og ulemper med prosjektet, og ikke minst reflektere over om det er sider ved prosjektet som kan bidra til at tilliten til helsetjenesten svekkes.

# 15. Etabler nødvendige avtaler

## 15.1 Hvilke avtaler trenger du?

På bakgrunn av kartleggingen du har gjort av roller og ansvar i prosjektet, sammen med deling av data (veilederens kapittel 6 og 9) må du vurdere om det er nødvendig å få på plass avtaler knyttet til behandling av personopplysninger. Mange institusjoner vil ha rutiner for hvilke avtalemaler som skal brukes og rutiner for kvalitetskontroll i forkant av signering. Vi anbefaler at du tar kontakt med personvernressurser for å undersøke hva som gjelder ved

din institusjon. Husk at avtalene må inngås før den aktuelle behandlingen av personopplysninger settes i gang.

## 15.2 Avtale om felles dataansvar

Dersom det er et samarbeidsprosjekt der din institusjon er dataansvarlig sammen med en eller flere institusjoner må det inngås en avtale om felles dataansvar. Her er det viktig å være oppmerksom på at en samarbeidsavtale mellom institusjonene nødvendigvis ikke omfatter partenes plikter knyttet til behandling av personopplysninger. F. eks vil det i samarbeid være slik at det foreligger en samarbeidsavtale der andre forhold som finansiering, organisering og rettigheter knyttet til resultater og forfatterskap er regulert. Ved siden av vil det da være en avtale om felles dataansvar som beskriver partenes ansvar og roller knyttet til behandlingen av personopplysninger i prosjektet.

## 15.3 Databehandleravtale

Når det tas i bruk leverandører av f. eks laboratorietjenester, lagringstjenester ol., der leverandøren vil behandle personopplysninger på vegne av prosjektet, må det inngås en databehandleravtale. Denne avtalen vil sette rammen for behandlingen av personopplysninger. Merk også at det kan være tilfeller der din institusjon kan behandle personopplysninger på instruks fra andre og derfor vil ha rollen som databehandler, også da er det nødvendig å inngå en databehandleravtale.

Ved noen institusjoner er det inngått databehandleravtaler som også vil dekke behandling av personopplysninger i prosjekter ved institusjonen. Da vil det ikke være nødvendig å inngå en databehandleravtale for det konkrete prosjektet. Dersom du skal bruke databehandler kan det være nyttig å undersøke i forkant om det allerede foreligger en slik avtale eller om det er nødvendig å inngå en prosjektspesifikk databehandleravtale.

Du finner mer informasjon om databehandlere og databehandleravtaler i Normens faktaark 10. Direktoratet for e-helse har utgitt mal for standard databehandleravtale med veileder: [Standard databehandleravtale med veileder – ehelse](#)

## 15.4 Andre avtaler som kan være relevante

Det kan oppstå situasjoner der du f. eks får forespørsel om å utlevere personopplysninger fra ditt prosjekt til et annet. Dette kan typisk være tilfelle der to eller flere prosjekter forsker på det samme fagområdet, og kan ha nytte av hverandres data uten at det foreligger noe ytterligere samarbeid. Det kan også være at en institusjon har tilgang til humant biologisk materiale et forskningsprosjekt ved en annen institusjon trenger. I en slik situasjon der du utleverer personopplysninger uten å bestemme verken formål eller midler ved behandlingen, er det ikke noe felles dataansvar. Det er likevel viktig å inngå en avtale om utlevering av data, som beskriver de nærmere vilkårene for utleveringen og behandlingen av personopplysninger i det andre prosjektet. Før du vurderer å overføre personopplysninger bør du lese veilederens kapittel 9 om å dele data.

Videre er det som nevnt over ikke uvanlig å både motta og utlevere humant biologisk materiale. Materialet analyseres og frembringer personopplysninger, og krever derfor at det inngås en avtale om felles dataansvar eller databehandleravtale. I tillegg bør det også inngås en avtale som regulerer utleveringen av selve materialet, hvor det f. eks fremgår hva som utleveres og hvordan materialet er merket, rammer for bruk og analyser, oppbevaring, om det skal returneres eller destrueres etter at analyser er gjennomført mv.



## 16. Dokumentasjon

Dataansvarlig er forpliktet til å føre protokoll over behandlingsaktiviteter etter personvernforordningen.<sup>21</sup> Dette innebærer at din institusjon trenger følgende informasjon om hvordan prosjektet behandler personopplysninger:

- hvem som er dataansvarlig (og om det er flere dataansvarlige)
- formålet/ene (hvorfor personopplysningene behandles)
- kategorier registrerte og typer personopplysninger,
- hvilke mottakere som får tilgang (hvis utenfor EU/EØS - oppgi land og garantier)
- tidspunkt/kriterier for når dere skal slette personopplysningene
- og sikkerhetstiltak ved behandlingen

Når du setter i gang et prosjekt må du derfor sørge for at prosjekt blir protokollført, og at du arkiverer dokumentasjon på at behandlingen av personopplysninger er lovlig. Din institusjon kan ha egne rutiner på hvordan behandlingsaktiviteter blir protokollført og hvordan dette skal dokumenteres, f. eks i form av elektroniske meldeskjemaer. Det anbefales at du undersøker hva som gjelder ved din institusjon.

## 17. Klart for datainnsamling

Når du nå har fullført alle stegene i forskningsveilederen, nærmer det seg klart for datainnsamling. Før du går i gang, må du passe på at alle nødvendige tillatelser er innhentet, og at alle nødvendige avtaler er inngått. Du må også sjekke at DPIA er godkjent, dersom dette er et krav.

I tillegg er det viktig at du sørger for at retningslinjene ved din institusjon erfor alle stegene. kan du starte prosjektet og datainnsamlingen. Vær oppmerksom på at hvis prosjektet endres underveis (mht. punktene over), må du foreta ny vurdering av relevante punkter, se veilederens kapittel 18.

## 18. Endringer og vurderinger underveis i prosjektet

Gjennom hele prosjektet skal du alltid følge prosjektbeskrivelsen, tillatelser og de vurderingene du gjorde knyttet til personvern. Det vil likevel alltid kunne oppstå endringer i

---

<sup>21</sup> Personvernforordningen art. 30

prosjektet som avviker fra planleggingen du gjorde før oppstart. Det kan være overraskende funn og utfordringer knyttet til dataene, det kan være behov for mer og nye data, og det kan skje endringer i ressurser og organisering. Konsekvensene av dette er at det kan bli nødvendig å gjøre endringer i prosjektet.

Når du skal vurdere om det er behov for å gjøre endringer, er det viktig å huske at alle tillatelser, innsamlede samtykker og personvern vurderinger bygger på den opprinnelige prosjektbeskrivelsen. Et prosjekt vil etter hvert ofte ha flere versjoner av prosjektbeskrivelser, og det er derfor viktig å dokumentere hva som til enhver tid er gjeldende versjon, og hvilke grep som har blitt gjennomført som følge av endringene. Noen typiske eksempler på endringer som kan påvirke behandlingen av personopplysninger er:

- Utsettelse av prosjektslutt som medfører forlengelse av behandling av personopplysninger
- Nye og utgående prosjektmedarbeidere
- Nye datainnsamlinger, f. eks ny type personopplysninger
- Inklusjon av nye prosjektdeltakere (registrerte)
- Inklusjon av ny dataansvarlig institusjon
- Endringer i hvordan prosjektdeltakere rekrutteres
- Endringer i tekniske løsninger som benyttes (f. eks eCRF-løsning)

I helseforskning vil også endringer både av faglig og organisatorisk karakter kreve at prosjektet sender endringsmelding til REK.

Videre må du alltid vurdere endringen før den gjennomføres. I helseforskning vil også endringer både av faglig og organisatorisk karakter kreve at prosjektet sender endringsmelding til REK. Endringer kan også medføre at prosjektet må ha en ny vurdering og tillatelse fra SLV, Helsedirektoratet eller Helsedataservice. Merk at det ikke vil være tilstrekkelig å dokumentere at endringsmelding er sendt.

Prosjektet må videre alltid vurdere hvordan endringene i prosjektet påvirker den registrerte, og om behandlingen av deres personopplysninger fortsatt vil være forutsigbar, åpen og rettferdig. F. eks kan det være slik at informasjonen prosjektet har gitt til den registrerte, og det samtykket som er samlet inn, ikke er dekkende for behandlingen av personopplysninger endringen medfører. Dersom dette er tilfellet må prosjektet iverksette tiltak som å gi den registrerte ny informasjon, gi dem mulighet til å reservere seg eller samle inn nytt samtykke.

## Vedlegg 1: Definisjoner

For forklaring på generelle ord og uttrykk benyttet i denne veilederen henvises det til vedlegg «6.2 Definisjoner» i Normen 6.0. Det er imidlertid enkelte ord og uttrykk som er spesifikke for denne veilederen og dermed ikke er definert i Normen 6.0. Definisjonen av disse følger i listen under.

- F -

**Forskningsansvarlig institusjon:** Den forskningsansvarlige er en (fortrinnsvis) juridisk eller (unntaksvis) fysisk person med et overordnet ansvar for å tilrettelegge for at forskningen skjer på en forsvarlig måte, herunder sørge for at personvern- og informasjonssikkerhetsmessige forhold ivaretas. Den forskningsansvarlige kan delegere

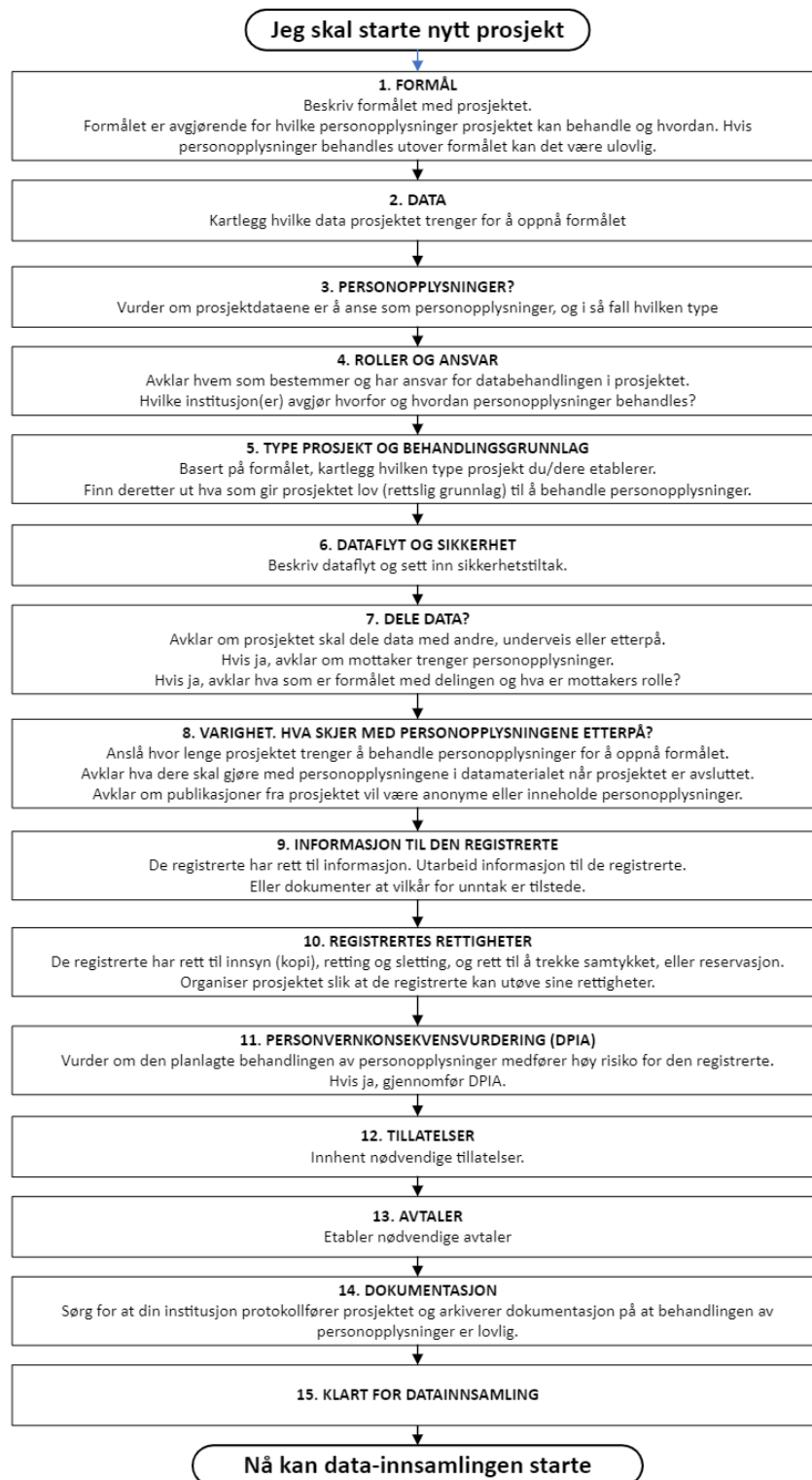
oppgaver til andre, så fremt den det delegeres til har nødvendig kompetanse til å utføre oppgaven. Merk at det kun er oppgaver som kan delegeres, ikke ansvaret.

## Vedlegg 2: Flytskjema og steg-for-steg veiledning til flytskjema

Din institusjon har ansvaret for å sikre og påvise at personvern- og helselovgivningen er fulgt i prosjektet. Ved å følge stegene i flytskjemaet får du oversikt over hva du må tenke på. Vær oppmerksom på at institusjoner kan ha ulike rutiner og systemer for å dokumentere at deres forskning/kvalitetssikring er lovlig, og at du må følge retningslinjer ved din institusjon. Mange institusjoner kan f.eks. ha rutine for innmelding av prosjekter og forskningsstøtte du kan rådføre deg med, og/eller bruker personverntjenester som Sikt. Uansett rutiner ved din institusjon, vil flytskjemaet fungere som støtte og veiledning.

Når du bruker flytskjemaet i prosjektet ditt, anbefaler vi at du er grundig i beskrivelse og vurdering i hvert punkt. Dette for å unngå følgefeil i de neste stegene, og risiko for ulovlig behandling av personopplysninger. Husk at du må gå igjennom alle stegene før du starter behandlingen av personopplysninger. Hvis du skulle oppdage avvik i planleggingsfasen, f.eks. hvis du har startet behandling av personopplysninger og hoppet over et av stegene, er det viktig at du sier ifra til institusjonen din så raskt som mulig. Dette fordi institusjonen - for noen typer avvik - har en 72 timers frist på å melde fra til Datatilsynet.

Før du går i gang med datainnsamling må prosjektet ha på plass nødvendige tillatelser og avtaler og personvernkonskvensvurdering (DPIA) hvis dette er et krav. Det kan være lurt å starte disse prosessene så tidlig som mulig. De er likevel plassert til slutt i malen, fordi det er viktig at du først har god oversikt over ulike forhold ved prosjektet. Vår anbefaling er at du ser over hele malen og skisserer stegene i oppsatt rekkefølge for ditt prosjekt. Alternativt kan du bruke malen parallelt med at du utarbeider søknader, går i dialog med samarbeidspartnere og evt. begynner på DPIA. Det viktigste er at du fullfører alle stegene før søknader sendes, avtaler inngås og DPIA sendes til godkjenning.



## Formål

Beskriv formålet med prosjektet. Vær oppmerksom på at formålet er avgjørende for hvilke personopplysninger prosjektet kan behandle og hvordan. Hvis personopplysninger behandles utover formålet, kan det være ulovlig.

Beskriv og vurder formålet:

- Forklar problemstilling og sentrale forskningsspørsmål du vil undersøke i prosjektet.

Husk:

- Formålet med prosjektet må være klart definert, nøyaktig, fullstendig og rimelig
- Formålet må beskrives så spesifikt som mulig

Tips:

- Vær grundig med formålsbeskrivelsen. Den er førende for alle vurderingene du skal gjøre under. Den er også førende for instanser du må innhente tillatelser fra, som f.eks. REK og SLV.
- Det kan være vanskelig og tidkrevende å endre eller utvide formål på et senere tidspunkt i prosjektet, særlig hvis det er vanskelig å innhente samtykke på nytt fra de som har deltatt i prosjektet (de registrerte).
- Formålet kan beskrives bredere/mer overordnet i større studier og registre der data skal brukes i flere delprosjekter med ulike problemstillinger. Men det må alltid gis en så presis og konkret formålsbeskrivelse som mulig. Hvor konkret den må være, beror på prosjektet eller registerets karakter. Vær oppmerksom på at "forskning" og "kvalitetssikring" uansett er for vidt, formålet må avgrenses tematisk til et forskningsområde.

Se også Normens faktaark [om formål og behandlingsgrunnlag](#).

## Data

Kartlegg hvilke data prosjektet trenger for å oppnå formålet.

Beskriv og vurder datamaterialet du vil samle inn:

- **Utvalgsriterier.** Hvilke kategorier av personer skal prosjektet ha opplysninger om?
- **Sårbare personer?** Kan noen i utvalget ha vansker med å ivareta rettighetene sine, pga. sykdom, livssituasjon, skjev maktrelasjon til deg/institusjon el.? F.eks. barn, pasienter, asylsøkere og ansatte.
- **Datakilder.** Hvor og hvordan innhenter prosjektet opplysninger?
  - fra den registrerte selv: gjennom intervju, spørreskjema, notater, observasjon etc.
  - og/eller fra andre kilder: pasientjournal, helseregister, SSB, institusjon, annet forskningsprosjekt, medisinsk utstyr, etc.
- **Dataomfang og innhold.** Beskriv ca. antall personer, antall og detaljgrad på variabler, hvor ofte opplysninger skal innhentes, og om data fra ulike kilder skal kobles på personnivå. Og beskriv hvilke opplysninger som skal innhentes (via intervjuguide, spørreskjema, observasjonsguide, variabelliste, medisinske forsøk, biologiske prøver, måleinstrumenter, teknologisk utstyr etc.)

Husk:

- **Dataminimering:** prosjektet kan kun samle inn opplysninger som er adekvate og relevante for formålet.

- Hvis du henter data fra andre kilder enn direkte fra den registrerte må:
  - den som utleverer ha rettslig grunnlag (personvernforordningen og norsk lov)
  - og utleveringen må følge regler om taushetsplikt (samtykke fra den registrerte, dispensasjon eller annet unntak fra taushetsplikten)
- Hvis prosjektet skal bruke/utvikle innovativ teknologi, eller hente data fra tekniske løsninger, medisinsk utstyr el. bør du rådføre deg med ressurser ved din institusjon (IT, jurister, medisinskteknisk personell) for å avklare om – og på hvilken måte - prosjektet er teknisk/juridisk mulig å gjennomføre.

For mer om dataminimering se [Normens faktaark om personvernprinsippene, kap 1.3.](#)

## Personopplysninger?

Vurder om prosjektdataene er å anse som personopplysninger, og i så fall hvilken type.

Vurder:

- Tenk på alle data som skal brukes i prosjektet fra start til slutt, uavhengig av format. Og les definisjonene under.
- Skal prosjektet behandle personopplysninger?
- Hvis nei, trenger du ikke gå videre. Merk at du likevel må avklare med REK om prosjektet er søknadspliktig dersom formålet er å fremskaffe ny kunnskap om helse og sykdom (helseforskning), selv om prosjektet kun skal behandle anonyme opplysninger (f.eks. tester/forsøk som innebærer helserisiko der du innhenter samtykke, men ikke knytter data til forsøksperson).
- Hvis ja, vurder om prosjektet skal behandle:
  - særlige kategorier personopplysninger
  - personopplysninger om straffedommer eller lovovertridelser
  - og/eller taushetsbelagte personopplysninger

Viktige definisjoner

- **Personopplysninger** behandles hvis det på noen måte vil være mulig å knytte dataene til en enkeltperson, f.eks. via:
  - navn, fødselsnummer, adresse, telefonnummer, epost, samtykkeerklæring osv.
  - bakgrunnsinformasjon som tid, sted, institusjon, alder, kjønn, stilling, diagnose osv.
  - kode som viser til en koblingsnøkkel hos deg eller andre (f.eks. liste med prosjekt-ID og navn, eller pasientnummer og fødselsnummer)
  - bilde, video, lydopptak
  - IP-adresse, nettidentifikator
  - lokasjonsdata, bevegelses-/adferdsmønstre
  - biometri (f.eks. iris, fingeravtrykk, ansikt, ganglag)
  - humant biologisk materiale eller genetiske analyser (av arvestoff)
- **Særlige kategorier personopplysninger** er data om rasemessig/etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning, fagforeningsmedlemskap, genetikk, biometri, helseforhold og/eller seksuelle forhold/orientering.
- **Personopplysninger om straffedommer/lovovertridelser** er data om at en person er mistenkt, siktet, tiltalt eller dømt for straffbar handling.



- **Taushetsbelagte personopplysninger** er data om personer fra kilder som har lovpålagt eller avtalefestet taushetsplikt om opplysningene.

Husk:

- Begrepet «helseopplysninger» skal tolkes vidt. Det omfatter enhver opplysning som avdekker noe om en persons tidligere, nåværende eller fremtidige fysiske eller psykiske helsetilstand. Det kan være opplysninger om sykdom, funksjonshemning, sykdomsrisiko, sykehistorie, helsehjelp/behandling, fysiologisk/biomedisinsk tilstand, genetik, biologiske prøver, tester/undersøkelser av kroppsdel-/substans mm. Det gjelder uavhengig av hvor opplysningene kommer fra, f.eks. pasientjournal, helsepersonell, medisinsk utstyr, den registrerte selv eller andre.
- Prosjektet behandler personopplysninger selv om data kun kan knyttes til enkeltpersoner gjennom en kode og koblingsnøkkel. Det gjelder også dersom prosjektet ikke selv har tilgang til koblingsnøkkelen, men lagrer den ved andre institusjoner.

Vær også oppmerksom på at flere variabler sett i sammenheng kan være egnet til å bakveisidentifisere de registrerte, selv om du ikke har tilgang til direkte identifiserbare opplysninger eller koblingsnøkkel.

## Roller og ansvar

Avklar hvem som bestemmer og har ansvar for databehandlingen i prosjektet. Hvilke institusjon(er) avgjør hvorfor og hvordan personopplysninger behandles?

Vurder:

- Er din institusjon:
  - **Dataansvarlig alene** – bestemmer formål og midler alene ved behandlingen av personopplysninger (evt. samarbeidspartnere har liten/ingen innflytelse)
  - **Felles dataansvarlig** – bestemmer formål og midler ved behandling av personopplysninger (helt eller delvis) sammen med en eller flere andre institusjoner
  - **Databehandler** – bestemmer ikke/lite over formål og midler, men behandler personopplysninger på instruksjon fra andre

Husk:

- Det er institusjonen, ikke den enkelte forsker, som bestemmer over databehandlingen og hvilken rolle institusjonen har.
- Hvis rollen til din institusjon er uklar, kontakt ressurser ved din institusjon i god tid før oppstart av datainnsamling.
- Roller og ansvar må kartlegges for å finne ut hva din institusjon må sikre/dokumentere, og hvilke avtaler dere må ha med evt. samarbeidspartnere.
- Ved felles behandlingsansvar: ta en felles gjennomgang av flytskjemaet, se hvilke aktiviteter knyttet til personvern den enkelte institusjon skal ha ansvar for å gjennomføre i prosjektet og dokumenter stegene sammen.
- Med «midler» mener vi her hvordan vi behandler personopplysninger, f. eks hvordan de skal analyseres og lagres

Tips:

- Vi anbefaler å lese Datatilsynets veileder om roller og ansvar, som gir gode forklaringer og eksempler, se [Behandlingsansvarlig og databehandler | Datatilsynet](#)

For mer om roller og ansvar, se [Normens veileder om internkontroll](#) og Normens [faktaark om bruk av databehandler](#)

## Type prosjekt og behandlingsgrunnlag

Basert på formålet, kartlegg hvilken type prosjekt du/dere etablerer.

Finn deretter ut hva som gir prosjektet lov (rettslig grunnlag) til å behandle personopplysninger.

Kartlegging av **prosjekttype** er nødvendig for å finne ut **hvilke lover** prosjektet må følge, og **hvilke tillatelser** man må ha før oppstart.

All behandling av personopplysninger reguleres av EUs personvernforordning og den norske personopplysningsloven. For noen formål (type prosjekt) vil helselover gjelde i tillegg. Hver behandling av personopplysninger må ha behandlingsgrunnlag i personvernforordningen artikkel 6 (behandling av personopplysninger i alminnelig kategori) og artikkel 9 (unntak fra forbudet om behandling av personopplysninger i særlig kategori), og oppfylle vilkår i aktuelle lover og forskrifter, for å være lovlig.

I tabellen "[Tabell type prosjekt og behandlingsgrunnlag](#)" er det laget en oversikt over de mest aktuelle behandlingsgrunnlagene for de ulike prosjekttypene hentet fra personvernforordningen, personopplysningsloven og helselovgivningen. Merk at dette ikke er en uttømmende oversikt, og det kan være andre behandlingsgrunnlag, blant annet EU/EØS-regelverk, som kan være relevant for ditt prosjekt.

Vurder:

- Definer først prosjekttype ut fra formålet. Og velg deretter det rettslige grunnlaget som passer for ditt prosjekt.
- Vær oppmerksom på at prosjektet ditt kan ha formål i "gråsonen" mellom ulike prosjekttyper. Les derfor nøye på definisjonene av alle prosjekttypene, slik at du får plassert prosjektet ditt i rett kategori. Er du i tvil, rådfør deg med din institusjon.
- Det kan være vanskelig å skille forskning og kvalitetssikring. Kvalitetssikring innebærer å undersøke/evaluere om diagnostikk, behandling og annen helsehjelp faktisk gir forventede resultater og om kravene til kvalitet er oppfylt. Hvis prosjektet bruker vitenskapelig metodikk for å evaluere, undersøke eller fremskaffe kunnskap om andre forhold, vil det trolig falle inn under kategorien forskning (ikke kvalitetssikring).
- Vær oppmerksom på at prosjektet må følge vilkårene i det rettslige grunnlaget, og lovene som gir det rettslige grunnlaget.
- Du bør beskrive og dokumentere konkret hvordan prosjektet oppfyller vilkårene, og hvorfor du mener det aktuelle rettslige grunnlaget skal brukes.
- Merk at hvis behandlingen av personopplysninger i prosjektet skal ha rettslig grunnlag i samtykke, er det flere vilkår som må være oppfylt. Samtykket må være **spesifikt, frivillig, aktivt og utvetydig**. Samtykket må også kunne **dokumenteres**

og skal **enkelt kunne trekkes tilbake** av den registrerte. Hvis det er vanskelig å oppfylle disse kriteriene, kan ikke samtykke brukes som rettslig grunnlag, og du må vurdere om et annet alternativ til rettslig grunnlag kan benyttes i ditt prosjekt.

Husk:

- Merk at et samtykke fra den registrerte kan ha ulike funksjoner. Samtykke kan:
  - være rettslig grunnlag for behandling av personopplysninger (som vist i tabellen over)
  - være et tiltak som ivaretar den registrertes rettigheter og friheter (når rettslig grunnlag er allmennhetens interesse, jf. tabellen over)
  - oppheve taushetsplikt (for opplysninger prosjektet henter fra datakilder med taushetsplikt)
- Samtykke når de registrerte er barn:
  - Hvis barn skal delta i prosjektet, må du vurdere hvem som skal samtykke for barnet. Hovedregelen er at foreldre eller andre med foreldreansvar må gi samtykke frem til barnet er 18 år. I helseforskning og helseregistre er hovedregelen at ungdom kan samtykke selv fra 16 år.
  - For annen forskning enn helseforskning, faller man tilbake på hovedregelen om at foreldre med foreldreansvar samtykker på vegne av barnet frem til barnet er 18 år. Det er viktig å påpeke i den forbindelse at barn har en gradvis medvirknings- og selvråderett, hjemlet i barnelova § 31 og 33. Medvirkningsretten innebærer at barnet skal ha informasjon tilpasset sin alder og få muligheten til å si sin mening, i tråd med alder og modenhet. Det må også vurderes hvor inngripende forskningen anses å være for barnet. Hva som anses som det beste for (det enkelte) barnet, skal alltid være et grunnleggende hensyn, og som vil være avgjørende for om barn i det hele tatt skal delta i forskningsprosjekt eller ikke. De ovennevnte momentene må vurderes før foreldrene beslutter å avgi et samtykke, eller ikke, til forskningen.
  - Dersom foreldre eller andre med foreldreansvar har samtykket på vegne av et barn til deltakelse i forskning eller kvalitetssikring, skal barnet når det blir 16 år få informasjon om behandlingen av personopplysninger i prosjektet/registeret, og retten til å trekke samtykke tilbake eller motsette seg behandling.
- Hvis voksne uten samtykkekompetanse skal delta, rådfør deg med din institusjon om hvordan prosjektet kan gjennomføres på lovlig måte.
- Hvis prosjektet behandler personopplysninger i flere omganger (f.eks. for flere utvalg, eller først for å rekruttere deltagere, og deretter for intervju), må prosjektet ha rettslig grunnlag for hver aktivitet.
- Ved etablering av medisinske kvalitetsregistre skal du følge kravene som stilles i forskrift om medisinske kvalitetsregistre. Flytskjemaet og forskningsveilederen kan likevel hjelpe deg i vurderingene du må gjennomføre etter forskriften. Hvis du skal etablere medisinsk kvalitetsregister anbefaler vi å søke veiledning hos [Nasjonalt servicemiljø for medisinske kvalitetsregistre](#)

Tips:

- Hvis du er usikker på type prosjekt, rådfør deg med din institusjon i god tid før datainnsamling.
- Hvis du er usikker på om prosjektet er helseforskning, kan du sende fremleggelsesvurdering til REK og få svar ila. kort tid.

- Det kan være vanskelig å skille større helseforskningsprosjekt fra befolkningsbasert helseundersøkelse. Rådfør deg med din institusjon eller REK.
- Se også NEMs veileder [Helseforskningslovens saklige virkeområde](#), som avgrensner helseforskning mot hhv. kvalitetssikring og helseregistre.
- Resultater fra intern kvalitetssikring kan publiseres anonymt (se boks 8).
- Hvis du skal forske på, utvikle produkter eller ta i bruk utstyr som er basert på kunstig intelligens innenfor helse anbefaler vi å ta i bruk veiledningssiden til Koordineringsprosjektet for kunstig intelligens. Her kan det også søkes om kostnadsfri regulatorisk veiledning. Les mer på [Kunstig intelligens i helsetjenesten](#).
- Merk at helsepersonelloven § 29 gir adgang til å søke om dispensasjon fra taushetsplikten i prosjekter der formålet er å utvikle og ta i bruk klinisk beslutningsstøtteverktøy. Søknaden sendes til Helsedirektoratet.

Se også Normens faktaark [om formål og behandlingsgrunnlag](#)

## Dataflyt og sikkerhet

Beskriv dataflyt og sett inn sikkerhetstiltak.

Beskriv og vurder:

- Lag en konkret plan for hvordan prosjektet skal samle inn, analysere, koble, lagre, dele og sikre data. Illustrer gjerne i et flytskjema.
- Få med følgende i beskrivelse av dataflyt:
  - alle datakilder
  - alle enheter og kanaler dataene skal innom
  - om/hvordan data om enkeltpersoner fra ulike datakilder kobles
  - om personopplysninger lagres sammen med eller adskilt fra datasettet
  - hvor eventuell koblingsnøkkel lagres
  - hvem som får tilgang til personopplysninger (institusjon og rolle)
  - hvilke opplysninger de ulike mottakerne skal ha tilgang til og til hvilket tidspunkt
  - hvorfor de får tilgang
  - om publikasjoner vil inneholde anonyme eller personidentifiserende data
  - hvordan prosjektet avslutter behandlingen av personopplysninger (sletting, anonymisering eller viderebehandling).
- Beskriv og vurder sikkerhetstiltakene:
  - vurderes for hver enhet og kanal som dataene flyter gjennom
  - kan være tekniske og/eller organisatoriske
  - skal være egnet til å sikre dataene mot uautorisert deling, endring og sletting
  - må være bedre jo høyere personvernrisikoen er (se boks 11)

Husk:

- Du må følge lagringsguide og retningslinjer for informasjonssikkerhet ved din institusjon.
- Beskrivelsen av dataflyt og vurderingen av sikkerhetstiltak må være god og riktig. Det kan være hensiktsmessig (og i noen tilfeller nødvendig), å be om bistand fra IT-ressurser fra din institusjon for å sikre dette, særlig når dataflyten er kompleks og/eller innebærer høy risiko.
- Rådfør deg med din institusjon hvis du er usikker eller prosjektet bruker nytt utstyr/løsning/leverandør som ikke er godkjent ved din institusjon.
- Prosjektleder må sørge for at det finnes en løpende oversikt over hvilke navngitte personer som til enhver tid har tilgang til hvilke personopplysninger og hvorfor slik tilgang er nødvendig. Husk å oppdatere tilganger ved endringer i prosjektgruppen.
- Du må sørge for at det er samsvar mellom dataflyten i prosjektet og den informasjonen du gir til den registrerte og REK, Helsedataservice, Helsedirektoratet, SLV mv.

Se også [Normens faktaark om lagringstid og sletting](#) og [Normens veileder om risiko](#)

## Dele data?

Avklar om prosjektet skal dele data med andre, underveis eller etterpå.

Hvis ja, avklar om mottaker trenger personopplysninger.

Hvis ja, avklar hva som er formålet med delingen og hva mottakers rolle er?

Vurder:

- Hvilke tilganger som er nødvendig for prosjektformålet:
  - Hvilke personer skal få tilgang til personopplysningene i prosjektet?
  - Hvorfor trenger de tilgang til personopplysninger for å oppfylle formålet/sine oppgaver i prosjektet?
- Hvilken rolle har de som får tilgang (kategori mottaker)?
  - ansatte ved din institusjon (dataansvarlig)
  - ansatte hos fellesansvarlig institusjon
  - ansatte hos databehandler
- Om personopplysninger skal brukes til andre formål enn prosjektet:
  - Skal du eller andre bruke personopplysninger fra prosjektet til andre formål enn prosjektformålet (underveis eller etterpå)?
- Før deling/ny bruk må du i samråd med din institusjon:
  - Sikre rettslig grunnlag for delingen. Hvilke vilkår datadelingen må oppfylle finner du i lover/forskrifter som gjelder ditt prosjekt (boks 5).
  - Ta stilling til hvilken dokumentasjon mottaker må gi til prosjektet, for at din institusjon skal kunne påvise at delingen er lovlig.
- Hvis prosjektet skal dele data systematisk til nye formål:
  - Lag en skriftlig rutine som viser hvilke momenter dere må vurdere og hvilken dokumentasjon dere må ha før hver utlevering.
  - Sjekk at utleveringsrutinen er i samsvar med de lover/forskrifter som gjelder ditt prosjekt.
  - Det er særlig viktig før oppstart av befolkningsbaserte helseundersøkelser og medisinske kvalitetsregistre, der formålet er gjenbruk av data.
- Institusjonen din må føre skriftlig protokoll over alle utleveringer av personopplysninger fra prosjektet. For hver utlevering må dere dokumentere mottakers rettslige grunnlag og momentene i sjekklisten under Protokoll (nederst i flytskjema).

Husk:

- Personer som jobber i prosjektet, kan bare få tilgang til personopplysninger hvis de trenger det for å utføre sine oppgaver.
- Hvis prosjektet benytter leverandører som får tilgang til personopplysninger uten å bruke dem til egne formål (f.eks. nettskjema, videosamtale, analyseinfrastruktur, lagringstjeneste, skytjeneste), definerer du disse mottakerne som databehandlere
- Enhver deling – og enhver ny bruk – av personopplysningene til nytt formål er en egen behandling. Det gjelder også hvis du selv eller andre ved din institusjon skal bruke opplysningene videre til andre formål. Følg da flytskjemaet fra start for den nye behandlingen.
- Rådfør deg alltid med din institusjon før deling/ny bruk til andre formål enn prosjektet. Da forankrer du vurderingen av at viderebehandling er lovlig.
- Hvis dere utleverer til annen institusjon, er mottaker dataansvarlig for den videre behandlingen. Hovedoppgaven for dere er da å sikre at selve utleveringen er lovlig.



Men sjekk rutiner ved din institusjon. Noen ønsker å inngå utleveringsavtale med mottaker som gir vilkår/begrensninger for videre bruk.

- Det kan være vanskelig å vurdere om prosjektendring innebærer nytt formål/prosjekt. Rådfør deg med din institusjon, eller REK hvis helseforskning.

## Varighet. Hva skjer med personopplysningene etterpå?

Anslå hvor lenge prosjektet trenger å behandle personopplysninger for å oppnå formålet.

Avklar hva dere skal gjøre med personopplysningene i datamaterialet når prosjektet er avsluttet.

Avklar om publikasjoner fra prosjektet vil være anonyme eller inneholde personopplysninger.

Vurder:

- Hvor lenge det er nødvendig å behandle personopplysninger for å oppnå formålet. Sett dato eller angi kriterier for når behandlingen skal opphøre.
- Avklar hva som skal skje med personopplysninger i datamaterialet når prosjektet er fullført:
  - **Slette:** Sjekk først om dere trenger opplysningene videre pga. arkiveringsplikt eller behov for videre forskning
  - **Anonymisere:** Lag en plan for hvilke tiltak prosjektet må gjøre for at opplysningene faktisk er anonyme etterpå
  - **Viderebehandle:** Avklar til hvilke formål, og hvem som er dataansvarlig
- Avklar hva som skal skje med personopplysninger i publikasjoner fra prosjektet:
  - **Publisere anonyme opplysninger:** Lag en plan for hvilke tiltak prosjektet må gjøre for at opplysningene faktisk er anonyme
  - **Publisere personopplysninger:** Avklar lovlig grunnlag for denne behandlingen av personopplysninger (samtykke er hovedregel)

Husk:

- Personopplysninger skal ikke lagres lenger enn det som er nødvendig for formålet. Når du planlegger sluttdato er det likevel lurt å ta høyde for at det kan skje uplanlagte forsinkelser, og at det kan ta tid å innhente tillatelser, få på plass avtaler, få tilgang til data og publisere.
- Det kan også oppstå uplanlagte endringer i prosjektopplegget som kan kreve nye personvern vurderinger/tillatelser, evt. ny informasjon til de registrerte.
- Hovedregelen er at personopplysninger skal slettes når formålet er oppfylt. Men før du legger en plan om å slette, må du sjekke om prosjektet omfattes av lovfestede krav og standarder for arkivering/lagring/viderebehandling, som f. eks vilkår fra REK om 5 års lagring for etterkontroll iht. helseforskningsloven og Good Clinical Practice (GCP) i helseforskning og klinisk forskning, eller 25 år i legemiddelstudier.
- For helseforskningsprosjekter med vilkår om lagring for etterkontroll, kan data kun lagres av hensyn kontroll og etterprøvbarehet, og ikke brukes av prosjektleder eller andre, i perioden mellom prosjektslutt- og slettedato.

- Det er også mulig å lagre opplysningene videre for gjenbruk i forskning på visse vilkår. Hvis det er aktuelt, er det best å planlegge dette ved prosjektstart. Rådfør deg med ressurser i din institusjon.
- Anonymisering innebærer at alle personopplysninger (definert i boks 3) må slettes eller omskrives, slik at det ikke er mulig for noen å gjenkjenne enkeltpersoner i datasettet, verken direkte eller indirekte. Anonyme data kan brukes fritt. Men vær klar over at selve anonymiseringen er en behandling av personopplysninger der du må følge personvernregelverket. Rådfør deg med din institusjon.

Se også [Normens faktaark om lagringstid og sletting](#).

## Informasjon til den registrerte

De registrerte har rett til informasjon. Utarbeid informasjon til de registrerte om behandling av deres personopplysninger i prosjektet. Eller dokumenter at vilkår for unntak er til stede.

Vurder:

Hovedregel om informasjon:

- De du behandler personopplysninger om har rett på informasjon.
- Hvis du samler inn data direkte fra den registrerte (f. eks intervju, spørreskjema og observasjon), må du gi informasjonen før datainnsamlingen
- Hvis du samler data om den registrerte fra andre datakilder uten samtykke, må du informere den registrerte senest en måned etter datainnsamlingen starter.
- Informasjonen skal være kortfattet og lett forståelig, og må gis individuelt via kanaler der den når frem.
- Den kan gis skriftlig eller muntlig, men du må dokumentere at – og hvilken – informasjon som er gitt. Derfor vil det i de fleste tilfeller være fordelaktig å gi informasjonen skriftlig.
- Du må informere om:
  - Hvem som er forsknings- og dataansvarlig institusjon (kontaktopplysninger og personer i alle deltakende institusjoner)
  - Hvorfor (formål), hvor lenge, og på hvilket lovgrunnlag opplysningene behandles,
  - Hvem som vil få tilgang til personopplysningene (mottakere),
  - Hvilke datakilder opplysningene hentes fra
  - Hvilke rettigheter den registrerte har: innsyn/kopi, retting, sletting, protest/trekke samtykke, klage til Datatilsynet
  - Kontaktopplysninger til personvernombudet ved din institusjon
  - Lovlig grunnlag for å overføre personopplysningene ut av EU/EØS (hvis aktuelt)
  - Planer om utlevering/viderebehandling til andre formål (hvis aktuelt)

Unntak:

- Loven åpner for at du i enkelte situasjoner kan behandle personopplysninger uten å gi informasjon.

- Du må da dokumentere unntakshjemmel og at vilkårene er oppfylt. Rådfør deg med din institusjon.
- Her er de aktuelle unntakene for forskning/kvalitetssikring:
  - Den registrerte har allerede fått informasjonen
  - Utilrådelig å informere, av hensyn til den registrertes helse eller forhold til nærpersoner
  - Det er umulig eller krever uforholdsmessig stor innsats å informere
  - Informasjon vil sannsynligvis ødelegge for formålet (forskning/kvalitetssikring)
  - Dataansvarlig er lovpålagt å behandle personopplysningene

Hvis prosjektet ikke gir individuell informasjon fordi det er umulig, uforholdsmessig vanskelig, og/eller kan ødelegge forskningsformålet, må dere gi kollektiv informasjon. En måte er å publisere informasjon om prosjektet i kanaler/nettsider *som det er sannsynlig* at de registrerte leser, f.eks. en interesseorganisasjon.

Tips:

- Sikt personverntjenester har utarbeidet maler for informasjonsskriv i forskning: [Informasjon til deltakarane i forskingsprosjekt \(sikt.no\)](https://sikt.no)
- REK har utarbeidet maler for informasjonsskriv i helseforskning: [Hjem - Insights \(rekportalen.no\)](https://rekportalen.no)
- Vent med å sende ut informasjonsskrivene til du har fullført flytskjema.

Se også [Normens veileder om de registrertes rettigheter](#).

## Registrertes rettigheter

De registrerte har rett til innsyn (kopi), retting og sletting, og rett til å trekke samtykket, eller reservasjon. Organiser prosjektet slik at de registrerte kan utøve sine rettigheter.

Vurder og legg en plan:

Hvordan legger prosjektet til rette for at de registrerte kan utøve sine rettigheter:

- Har den registrerte fått kontaktinformasjon til prosjektansvarlige og personvernombud, så de vet hvor de kan henvende seg?
- Lagres data slik at prosjektet lett kan finne opplysningene om den registrerte (f.eks. via koblingsnøkkel prosjektet har tilgang til)?
- Vet du og andre kontaktpersoner (ved egen eller samarbeidende institusjoner) hva dere skal gjøre hvis registrerte henvender seg, slik at de får rett svar innen tidsfristen?

Husk:

- Rettighetene gjelder så lenge de registrerte kan identifiseres i datamaterialet.
- Prosjektet skal ikke lagre flere personopplysninger enn nødvendig for formålet, bare for å kunne innfri rettighetene.
- Loven åpner for unntak fra rettighetene i enkelte situasjoner, men avslag må ikke gis uten begrunnelse og lovhjemmel.
- Innsyn må kun gis til den som personopplysningene gjelder, ikke til andre (f.eks. når du har data om deltager/tredjeperson og foreldre/barn).

- Feilvurdering av rettigheter kan føre til ulovlig behandling. Rådfør deg med din institusjon, særlig før du gir innsyn eller gir avslag.
- Institusjonen din har plikt til å vurdere om rettighetene skal/kan innfris, og svare den registrerte innen en måned.

Se også [Normens veileder om de registrertes rettigheter](#).

## Personvernkonsekvensvurdering (DPIA)

Vurder om den planlagte behandlingen av personopplysninger medfører høy risiko for den registrerte. Hvis ja, gjennomfør DPIA.

DPIA er et verktøy for å kartlegge og håndtere risikoer knyttet til behandling av personopplysninger. DPIA kreves før behandlinger som sannsynligvis gir "høy risiko for de registrertes rettigheter og friheter". Datatilsynet og EUs personvernråd (EDPB) har publisert veiledere om hva som er høy risiko.

Vurder:

- Se på kartleggingen du har gjort over. Vil behandlingen av personopplysninger i prosjektet medføre høy risiko?
- Hvis prosjektet oppfyller et eller flere av kriteriene under, eller du er usikker, bør du rådføre deg med din institusjon eller personvernombud (følg interne rutiner ved din institusjon).
- Jo flere av kriteriene som gjelder, desto mer sannsynlig at prosjektet må ha DPIA :
  - Behandling sensitive personopplysninger (særlige kategorier, straffedommer/lovovertrедelser, eller svært personlig karakter)
  - Behandling av personopplysninger i stor skala (mht. utvalgsstørrelse, mengde opplysninger, varighet, frekvens)
  - Behandling av personopplysninger om sårbare registrerte
  - Sammenstilling av datasett (f.eks. datakilder med ulike formål/dataansvarlige) som overstiger den registrertes rimelige forventninger
  - De registrerte hindres i å utøve sine rettigheter
  - Innovativ bruk av ny teknologi eller organisatorisk løsning
  - Evaluering (profilering/kartlegging av personopplysninger for å analysere eller forutsi personers adferd, helseforhold, preferanser, interesser, evner, behov el.)
  - Systematisk monitorering (ulike former for observasjon/sporing av personer, bl.a. på internett/offentlig område, f.eks. kameraovervåking, observasjon av internettaktivitet, lokasjonssporing og helseovervåking ved hjelp av sensorer og applikasjoner. ) Hvis prosjektet trenger DPIA, følg prosedyrer ved din institusjon.
- Vær oppmerksom på at Datatilsynet har utarbeidet en liste over behandlinger av personopplysninger som krever DPIA. Hvis prosjektet faller inn under noen av punktene på denne listen, må prosjektet ha DPIA. Se mer om dette i [Veiledning om DPIA | Datatilsynet](#)

I prosjekter der flere institusjoner deltar, f. eks. multisenterstudier, er det viktig å identifisere hvem som er dataansvarlig for behandlingen av personopplysninger som utgjør høy risiko. Hvis flere er ansvarlige for behandlingen, bør DPIA forankres (med eventuelle lokale

tilpasninger) hos alle dataansvarlige ved at ledelsen signerer, selv om utkast til DPIA evt. skrives av en av partene.

Husk:

- DPIA er en prosess, der dere beskriver den planlagte behandlingen, vurderer om den er lovlig og forholdsmessig, kartlegger risikoer, og foreslår risikoreduserende tiltak. Personvernombudet skal rådføres, før resultatet av DPIA fremlegges i et dokument for ledelsen ved din institusjon. Ledelsen vurderer om DPIA er godt nok utført, og om risikoen er akseptabel, slik at prosjektet kan starte. Hvis ikke, kan ledelsen bestemme at DPIA må revideres, eller at behandlingen må forhåndsdrøftes med Datatilsynet, eventuelt stoppes.
- Forhåndsdrøfting med Datatilsynet er påkrevd hvis personvernkonsekvensene fortsatt er for høye etter DPIA, og institusjonen ønsker å gjennomføre behandlingen av personopplysninger. Datatilsynet kan gi råd og/eller sette vilkår for behandlingen.

Tips:

- Direktoratet for e-helse har utgitt [Mal og veiledning for utfylling av personvernkonsekvensvurdering \(DPIA\) - ehelse](#)
- Hvis du skal melde prosjekt til Sikt, utarbeider Sikt en DPIA for prosjektet i samarbeid med deg, basert på Sikt sin DPIA-mal
- Det kan være nyttig å undersøke om det er gjennomført DPIA i lignende prosjekter som har brukt samme metodikk og behandling av personopplysninger, med vurderinger du kan gjenbruke. Det er imidlertid viktig at vurderingene i DPIA tilpasses ditt prosjekt.

## Tillatelser

Søk nødvendige tillatelser

Vurder:

Basert på kartleggingen du har gjort over, sjekk om prosjektet trenger godkjenning fra en eller flere instanser:

- Helseforskning: Forhåndsgodkjenning fra REK
- Klinisk utprøving av legemidler og medisinsk utstyr og ytelsesstudier av in-vitro diagnostisk utstyr: Godkjenning fra Statens legemiddelverk (SLV), inkludert godkjenning fra REK KULMU
- Humant biologisk materiale:
  - til Helseforskning, Annen forskning, Kvalitetssikring på tvers og Medisinsk kvalitetsregister: Godkjenning fra REK
  - til Intern kvalitetssikring og Befolkningsbasert helseundersøkelse: Melding til Biobankregisteret ved FHI
- Helseopplysninger fra pasientjournal eller andre behandlingsrettede helseregistre, uten samtykke:
  - til forskningsformål (helseforskning og annen forskning): Dispensasjon fra taushetsplikten fra REK

- til kvalitetssikringsformål: Dispensasjon fra taushetsplikten fra Helsedirektoratet
- Helseopplysninger fra helseregistre omfattet av Forskrift om nasjonal løsning for tilgjengeliggjøring av helsedata:
  - Vedtak fra om tilgjengeliggjøring av helseopplysninger fra Helsedataservice
  - Vedtak om dispensasjon fra taushetsplikten for helseopplysninger fra helseregistre, eventuelt sammenstilt med helseopplysninger fra pasientjournal eller andre behandlingsrettede registre
- Helseopplysninger fra registre som ikke er omfattet av forskriften over:
  - Vedtak fra registerforvalter om tilgjengeliggjøring
  - til forskningsformål (helseforskning og annen forskning): Dispensasjon fra taushetsplikten fra REK
  - til kvalitetssikringsformål: Dispensasjon fra taushetsplikten fra Helsedirektoratet
- Andre taushetsbelagte personopplysninger uten samtykke: Vedtak fra aktuelt fagdepartement- eller direktorat (f. eks NAV, Bufdir, UDI, SSB mv.)
- Helseopplysninger til intern kvalitetssikring: Dokumentere at prosjektet og behandlingen av personopplysninger er forankret hos institusjonens ledelse.

Husk:

- Med "samtykke" menes samtykke fra den enkelte registrerte (den som opplysningene gjelder) i forkant av behandlingen av personopplysninger.
- Tillatelsene over gjelder for alle typer prosjekt, med mindre annet er spesifisert.
- I noen tilfeller må du sende søknader til flere instanser. Merk da at alt du søker til REK om, sendes i samme søknad, f. eks (vedtak om forhåndsgodkjenning for helseforskning, dispensasjon fra taushetsplikt og forskningsbiobank)
- Hvis oppslag i pasientjournal er nødvendig for å rekruttere deltagere, må prosjektet ha dispensasjon fra taushetsplikt for dette, selv om de registrerte samtykker etterpå til deltagelse i prosjektet (f.eks. intervju).
- Hvis prosjektet skal samle data ved observasjon i helse- og omsorgstjenesten, må taushetsplikten først oppheves ved samtykke fra den enkelte pasient eller dennes pårørende. Helsepersonelloven § 29 åpner ikke for at REK, Helsedirektoratet eller Helsedataservice kan gi dispensasjon for observasjon.
- For intern kvalitetssikring gir helsepersonelloven § 26 og pasientjournalloven § 6 unntak fra taushetsplikten. Du trenger derfor ikke vedtak om dispensasjon. Det er likevel viktig å dokumentere at gjennomføringen av prosjektet og behandlingen av personopplysninger er forankret hos institusjonens ledelse. Vi anbefaler at du følger interne rutiner ved din institusjon mht. dette.
- Direktoratet for e-helse v/Helsedataservice har vedtaksmyndighet for følgende helseregistre: Dødsårsaksregisteret, Kreftregisteret, Medisinsk fødselsregister, Meldingssystem for smittsomme sykdommer (MSIS), System for vaksinasjonskontroll (SYSVAK), Norsk pasientregister (NPR), Nasjonalt register over hjerte- og karlidelser, System for bivirkningsrapportering, Kommunalt pasient- og brukerregister (KPR), Legemiddelregisteret, Helsearkivregisteret.

Tips:

- Send søknader i god tid før datainnsamling. Send gjerne søknadene samtidig.
- Vær nøye med å beskrive prosjektet på samme måte i alle søknader.



- Hvis du er usikker på hvilke godkjenninger og tillatelser prosjektet trenger, kontakt din institusjon i god tid før datainnsamling.

## Avtaler

Etabler nødvendige avtaler

Vurder:

- Vurder hvilke avtaler prosjektet må ha for behandling av personopplysninger, basert på kartleggingen av ansvar og datadeling (se boks 4 og 7 over):
  - Avtale om felles dataansvar - når din institusjon er felles dataansvarlig sammen med en eller flere institusjoner
  - Databehandleravtale med leverandør - når din institusjon er dataansvarlig og bruker databehandler
  - Databehandleravtale med dataansvarlig - når din institusjon er databehandler
- Sjekk om din institusjon pålegger prosjektet å inngå andre typer avtaler i tillegg, f.eks.:
  - Avtale om utlevering av personopplysninger til ny dataansvarlig/nytt formål (uten felles dataansvar)
  - Avtale om utlevering av humant biologisk materiale - din institusjon skal utlevere eller motta humant biologisk materiale
  - Samarbeidsavtale – regulerer avtalepartenes rettigheter og plikter vedrørende andre forhold ved prosjektet, som finansiering, oppgavefordeling, publiseringspoeng, rettigheter til forskningsresultater og data mv.
- Følg prosedyrer og maler for avtaleinngåelse ved din institusjon.

Husk:

- Hvis prosjektet kun bruker leverandører i tråd med lagringsguiden ved din institusjon, kan du gå ut fra at institusjonens avtaler med databehandlere er dekkende. Bruker prosjektet leverandører som ikke står på listen, må du be din institusjon inngå projektspesifikk databehandleravtale.
- Rådfør deg med din institusjon hvis du er usikker på hvilke avtaler som bør inngås i prosjektet.
- Avtale om felles dataansvar/databehandler må inngås før behandling av personopplysninger starter.
- En samarbeidsavtale som ikke regulerer behandlingen av personopplysninger er ikke tilstrekkelig, hvis partene har tilgang til personopplysninger.
- Deling av humant biologisk materiale innebærer ofte behandling av personopplysninger. Materialet kan være merket med et ID-nummer eller det skal foretas analyser som gir helseopplysninger. Da kan det være nødvendig med avtaler som også dekker behandling av personopplysninger.

Tips:

- Direktoratet for e-helse har utgitt mal for standard databehandleravtale med veileder: [Standard databehandleravtale med veileder - ehelse](#)

Se også [Normens faktaark om bruk av databehandler](#).

## Dokumentasjon

Sørg for at din institusjon protokollfører prosjektet og arkiverer dokumentasjon på at behandlingen av personopplysninger er lovlig.

Beskriv:

- I protokollen trenger institusjonen din følgende informasjon om hvordan prosjektet behandler personopplysninger:
  - hvem som er dataansvarlig
  - formålet/ene (hvorfor personopplysningene behandles)
  - kategorier registrerte og typer personopplysninger,
  - hvilke mottakere som får tilgang (hvis utenfor EU/EØS - oppgi land og garantier)
  - tidspunkt/kriterier for når dere skal slette personopplysningene
  - og sikkerhetstiltak ved behandlingen

Husk:

- Din institusjon trenger også mer dokumentasjon for å sikre at behandlingen av personopplysninger er i samsvar med personvernregelverket. Spør din institusjon om hvor og hvordan du skal dokumentere dette for ditt prosjekt.

## Klart for datainnsamling

Etter at du nå har fullført alle stegene i malen over, og innhentet alle nødvendige tillatelser, kan du starte prosjektet og datainnsamlingen.

Vær oppmerksom på at hvis prosjektet endres underveis (mht. punktene over), må du foreta ny vurdering av relevante punkter.