Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Notat

Personopplysninger i forskningsprosjekter ved Norsk Regnesentral

Notatnr ADMIN/01/19

Forfattere Erik Vasaasen, Lars Holden, Anders Løland

Dato 26.08.2019

© Copyright: Norsk Regnesentral

Norsk Regnesentral

Norsk Regnesentral (NR) er en privat, uavhengig stiftelse som utfører oppdragsforskning for bedrifter og det offentlige i det norske og internasjonale markedet. NR ble etablert i 1952 og har kontorer i Kristen Nygaards hus ved Universitetet i Oslo. NR er et av Europas største miljøer innen anvendt statistisk-matematisk modellering inklusiv kunstig intelligens og har et senter for forskningsdrevet innovasjon, Big Insight, med finansiering fra Norges forskningsråd, bedrifter og offentlige partnere. Innen statistikk jobbes det med et bredt spekter av problemstillinger, for eksempel finansiell risiko, jordobservasjon, estimering av fiskebestander, helse og beskrivelse av geologien i petroleumsreservoarer. NR er ledende i Norge innen utvalgte deler av informasjons- og kommunikasjonsteknologi. Innen IKT-området har NR innsatsområdene e-inkludering, informasjonssikkerhet og smarte informasjonssystemer. NRs visjon er forskningsresultater som brukes og synes.

Norsk Regnesentral
Norwegian Computing Center
Postboks 114, Blindern
NO-0314 Oslo, Norway

Besøksadresse
office address
Gaustadalleen 23a
NO-0373 Oslo, Norway

Telefon · telephone
(+47) 22 85 25 00
Telefaks · telefax
(+47) 22 69 76 60

Bankkonto · bank account
8200.01.48888
Org.nr. · enterprise no.
NO 952125001 VAT

Internett · internet
www.nr.no
E-post · e-mail
nr@nr.no

Tittel	**Personopplysninger i forskningsprosjekter ved Norsk Regnesentral**
Forfattere	**Erik Vasaasen, Lars Holden, Anders Løland**
Dato	26.08.2019
År	2019
Publikasjonsnummer	ADMIN/01/19

Sammendrag
Hensikten med dette dokumentet er å dokumentere rutinene for behandling av sensitive personopplysninger i NRs **forskningsprosjekter** i tråd med NRs rutiner for internkontroll. Det sentrale formålet er å fastlegge *hvem* som er ansvarlig for *hva* når personopplysninger skal håndteres.

Dokumentet inneholder det som kreves etter Personopplysningsloven, med virkning fra 20.07.2018 som er tilpasset EØS-avtalen (forordning (EU) 2016/679) om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (GDPR).

Emneord	Personopplysninger, Personvern, Sikkerhet, Rutiner, Avvik, Risiko
Målgruppe	Ansatte ved NR
Tilgjengelighet	Intern
Prosjektnummer	
Satsningsfelt	
Antall sider	51

© Copyright	Norsk Regnesentral

Innhold

1 Innledning

1.1 Formålet med dokumentet

Hensikten med dette dokumentet er å dokumentere rutinene for behandling av personopplysninger i NRs forskningsprosjekter. Dette notatet er en del av NRs system for internkontroll.

I de fleste av NRs prosjekter med personopplysninger vil NR være databehandler og ikke behandlingsansvarlig. Dette notatet behandler begge tilfellene for å sikre at NR lever opp til sine forpliktelser som databehandler i henhold til avtale med behandlingsansvarlig og i tillegg med et selvstendig ansvar for at behandlingen er i henhold til lov og forskrifter.

I mange tilfeller behandler NR annen konfidensiell informasjon enn personopplysninger. Dette notatets beskrivelser av oppbevaring av data vil også gjelde for slike prosjekter.

1.2 Lovgrunnlaget

Behandlingen av personopplysninger reguleres av Personopplysningsloven med virkning fra 20.07.2018 som er tilpasset EØS-avtalen (forordning (EU) 2016/679) om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (GDPR). Den fulle lovteksten finnes her. Loven suppleres av forskrift 15.12.2018 nr. 876 om behandling av personopplysninger (her kalt Forskriften). Den fulle forskriftsteksten fins her.

1.3 Oppbevaring, tilgjengelighet og revisjon

Dokumentet ligger på NRs intranett.

Dokumentet skal revideres når det skjer endring i regelverk eller intern organisering av betydning for håndteringen av personopplysninger.

2 Lovens virkeområde – begrepet personopplysninger

2.1 Saklig virkeområde

Etter lovens § 2 første ledd gjelder den for

"Loven og personvernforordningen gjelder ved helt eller delvis automatisert behandling av personopplysninger og ved ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register."

For forskning er § 8 og 17 viktig:

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

§ 17: *«Retten til innsyn etter personvernforordningen artikkel 15 gjelder ikke for behandling av personopplysninger for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål i samsvar med personvernforordningen artikkel 89 nr. 1 så langt*

a) det vil kreve en uforholdsmessig stor innsats å gi innsyn eller

b) innsynsrett sannsynligvis vil gjøre det umulig eller i alvorlig grad hindre at målene med behandlingen nås.

Retten til retting og begrensning av behandling etter personvernforordningen artikkel 16 og 18 gjelder ikke for behandling for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål i samsvar med personvernforordningen artikkel 89 nr. 1 så langt rettighetene sannsynligvis vil gjøre det umulig eller i alvorlig grad hindre at målene med behandlingen nås.

Første og annet ledd gjelder ikke dersom behandlingen får rettsvirkninger eller direkte faktiske virkninger for den registrerte.»

2.2 Personopplysninger

Begrepene "personopplysninger" og "behandling av personopplysninger" mv. er definert i GDPR art 4 nr 1-2 som

"1. «personopplysninger» enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliserings-opplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,

2. «behandling» enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring,"

Begrepet sensitive personopplysninger i den forrige personopplysningsloven er erstattet med begrepet særlige kategorier av personopplysninger (GDPR art 9 nr 1) og dette begrepet omfatter:

«Behandling av personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering»

I dette notatet vil vi noen ganger bruke begrepet sensitive som et adjektiv som i stor grad overlapper med begrepet særskilte kategorier i loven.

Merk at anonyme opplysninger ikke blir regulert direkte av loven. Når NR/forskeren skal vurdere om opplysninger kan knyttes til en enkeltperson, er det viktig å understreke forskjellen på anonyme og avidentifiserte data (se også omtalen av ulike typer datasett i kap. 3 nedenfor). Dersom vi f.eks. mottar datamateriale fra annet hold (Statistisk sentralbyrå (SSB), et meningsmålingsinstitutt o.a.), og vedkommende leverandør av data *fortsatt sitter på en koblingsnøkkel* som gjør det mulig å spore opplysningene tilbake til enkeltpersoner, dreier det seg om *avidentifiserte data* (også kalt *data som er anonyme på forskerens hånd*) – ikke anonyme data. Vi står da overfor personopplysninger i lovens forstand. I vurderingen av om det er mulig å spore opplysninger tilbake, skal en ta utgangspunkt i en "worst case"-situasjon – en situasjon der datamaterialet kommer i urette hender samtidig som det foreligger en teknisk mulighet for å koble opplysninger til enkeltpersoner. Det er bare hvis det ikke foreligger noen mulighet for en slik kobling, at en kan tale om anonyme opplysninger.

3 Typer av datasett

3.1 Opplysningenes art

En del datasett vi håndterer ved NR vil inneholde opplysninger av personlig art uten nødvendigvis å være personopplysninger i lovens forstand. Det forutsetter at bl.a. at opplysningene kan knyttes til enkeltpersoner. Spesielt viktig er det om noen av opplysningene er i en særlig kategori (tidl. sensitive personopplysninger).

Mange datasett vil dessuten være taushetsbelagte eller konfidensielle etter avtale med oppdragsgiver. Dette kan også gjelde programkode, rapporter og annet informasjonsmateriale.

3.2 Graden av personidentifisering

De datasettene vi har, eller kan tenkes å ha, ved NR kan inndeles i seks kategorier i henhold til graden av muligheten for personidentifisering. Dette får betydning for hvilke prosedyrer som må følges i søknader, tillatelser, rutiner for databehandling, oppbevaring, muligheter for koblinger osv.

De seks kategoriene er:

1. Datasett med direkte identifiserbare opplysninger
Direkte identifiserbar betyr at registeret inneholder opplysninger som entydig og direkte knytter informasjon til bestemte personer. Dette kan være navn, fødselsnummer o.l. Det skal i størst mulig grad unngås at direkte identifiserbar informasjon er lagret i samme datasett som andre variabler. Der hvor det er praktisk gjennomførbart, skal dataene heller brukes i avidentifisert form som beskrevet under kategori 3.

2. Datasett med avidentifiserte opplysninger der enkelte undergrupper er små nok til at personer kan identifiseres
De direkte identifiserende opplysningene er fjernet fra datasettet og erstattet med en kode. Datasettet er imidlertid ikke fullt avidentifisert da kjennskap til en kombinasjon av variable som bostedskommune, kjønn, alder, yrke osv. kan være tilstrekkelig for identifisering av enkeltindivid. Se også under kategori 6.

3. Datasett med avidentifiserte opplysninger – NR har koblingsnøkkelen
De direkte identifiserende opplysningene er fjernet fra datasettet og erstattet med en kode. Opplysninger kan kun føres tilbake til enkeltpersoner ved å gå via en koblingsnøkkel hvor koden refererer til de identifiserende opplysningene. Sikkerhetsfokuset flyttes her fra datasettet til koblingsnøkkelen.

4. Datasett med avidentifiserte opplysninger – koblingsnøkkelen oppbevares midlertidig andre steder
Datatilsynet krever i visse tilfeller at koblingsnøkkelen oppbevares hos en tredje part (eksempelvis hos NSD eller SSB) for å sikre at datasettet og koblingsnøkkelen er tilfredsstillende avskilt i perioder der det ikke er bruk for den i prosjektsammenheng.

5. Datasett med avidentifiserte opplysninger – NR uten tilgang til koblingsnøkkelen
Datasett der SSB eller andre foretar trekking av utvalg og oppfølging i form av purrebrev e.l., vil være eksempler på datasett av denne typen. NR har i disse tilfellene ikke på noe tidspunkt tilgang til koblingsnøkkelen. Denne kategorien inkluderer også tilfeller der det bare er mulig å identifisere personer ved tilgang til de opprinnelige dataene som er oppdatert utenfor NR. I dette tilfellet vil NRs behandling ikke medføre noen risiko for identifisering, men formelt regnes de likevel til denne kategorien.

6. Datasett med anonyme opplysninger
Anonymisert betyr at det er praktisk talt umulig å spore opplysninger i registeret til bestemte

enkeltpersoner. Ikke bare mangler direkte personidentifikasjon som for eksempel navn eller fødselsnummer, men også opplysninger som indirekte kan identifisere enkeltindivider. For at et register skal være anonymisert kan det for eksempel være nødvendig å fjerne eller aggregere detaljert informasjon om de registrertes yrke eller bosted – eller begge deler. Dersom datasettet inneholder opplysninger som indirekte kan identifisere enkeltindivider, tilhører det gruppe 2.

Datasett innhentet fra en større gruppe uten at det registreres hvem som har svart, og uten informasjon som indirekte kan identifisere enkeltindivider, regnes som et anonymisert datasett. Dersom det registreres hvem som har besvart, og dette kan kobles til den enkelte besvarelse, er datasett ikke anonymisert så lenge denne koblingen består. Etter at koblingsnøkkelen er slettet, er registeret anonymisert. Tilsvarende gjelder for andre datasett der koblingsnøkkel er slettet. De enkelte prosjekter kan altså skifte kategori under prosjektets forløp.

Anonyme opplysninger faller ikke under regelverkets definisjon av personopplysninger. Imidlertid ligger utfordringen her i hvorvidt datainnsamlingen er anonym. Dersom man går via identifiserende opplysninger for å generere det anonyme datasettet, vil dette være en behandling av personopplysninger som kommer inn under regelverkets virkeområde.

Selv om anonyme opplysninger ikke blir definert som personopplysninger i lovens forstand, er det likevel viktig å vurdere i hvilket omfang anonyme registre på NR skal sikres. Selv om slike data ikke skal kunne tilbakeføres til enkeltpersoner, kan slike data inneholde sensitiv informasjon hvor en for svak sikring av data kan svekke NRs omdømme som databehandler, selv om opplysningene ikke kan tilbakeføres til enkeltpersoner.

NR har også utarbeidet en egen side på intranettet om anonymisering, der det er en mer detaljert beskrivelse av fremgangsmåter for å anonymisere et datasett. Datatilsynet har også en veileder om anonymisering.

Det må også tas hensyn til hvor sensitiv informasjonen er, hvor belastende det vil være for den registrerte om andre kjenner til informasjonen, hvor mange personer som kjenner informasjonen og om det kan ha noen direkte påvirkning for vedkommende. Antall vitenskapelige artikler en person har skrevet, om en person har vært forkjølet siste året eller om en person har kreft er alle personinformasjon, men med stor variasjon i sensitivitet. Kunnskap om personinformasjon kan påvirke personens muligheter i arbeidsmarkedet eller for å få forsikring eller informasjonen kan være uten direkte påvirkning på personen. Det må også skilles mellom om muligheten for identifisering er ikke eksisterende, meget lite sannsynlig eller er sannsynlig. Det må også skilles mellom om kunnskapen fra et forskningsprosjekt får konsekvenser for personer som har bidratt med data, eller om det bare får konsekvenser for andre som på et senere tidspunkt er i en lignende situasjon som personer som har deltatt i forskningsprosjektet, f.eks. i forbindelse med forsikringssvindel eller søknad om lån. Det er ønskelig at forskning skal ha samfunnsmessige konsekvenser, men ikke for personene som har bidratt med data. Forskningsprosjekter som har direkte konsekvenser for personer som har bidratt med data, er omtalt i § 17 i personopplysningsloven siste ledd. Se sitat i kapitel 2.1.

4 Overordnete rammer og mål for behandling av personopplysninger

4.1 Relevans

NRs behandling av personopplysninger skal begrense seg til de data som er relevante for NRs forsknings- og dokumentasjonsoppgaver.

4.2 Sikkerhet

Behandlingen skal sikre nødvendig konfidensialitet. Med sikring av konfidensialitet menes beskyttelse mot at uvedkommende får innsyn i opplysningene.

Behandlingen skal sikre nødvendig integritet. Med integritet menes at opplysningene ikke blir endret som følge av utilsiktet eller uautorisert aktivitet.

Behandlingen skal sikre nødvendig tilgjengelighet. Med tilgjengelighet menes at tilstrekkelige og relevante opplysninger er til stede når det er behov.

4.3 Oppfyllelse av den enkeltes rettigheter

Behandlingen skal sikre at den enkeltes rettigheter blir ivaretatt.

4.4 Nærmere om sikkerhetsmålene

NR er en forskningsstiftelse. NRs forskningsresultater kan få betydning for eksempel for politiske beslutninger. Det er derfor viktig å ha høy kvalitet både på dataene og på behandlingen av dem.

De personopplysninger NR sitter inne med, brukes imidlertid ikke til å treffe beslutninger som berører den enkelte, verken direkte eller indirekte. Dette har noen konsekvenser i forhold til sikkerhetsmålene for behandlingen av personopplysninger:

Ad tilgjengelighet
Det er et mål at de opplysninger NR sitter inne med, i minst mulig grad skal kunne knyttes til enkeltpersoner. I størst mulig grad bør opplysningene anonymiseres eller krypteres på en slik måte at enkeltpersonopplysninger ikke er tilgjengelige, ikke engang for de ansvarlige. Tilgjengelighetshensynet vil derfor være lavt prioritert.

Ad integritet
Det er viktig for NRs faglige integritet å sikre at de data vi har, ikke blir endret ved en feil eller av noen som ikke er autorisert til det. Siden dataene ikke brukes i forhold til enkeltpersoner, og av de grunner som er anført for tilgjengelighetsmålet, er imidlertid ikke dette det sentrale målet i personvernsammenheng.

Ad konfidensialitet
Dette er det sentrale målet for NR i personvernsammenheng og når det gjelder taushetsbelagte opplysninger. NR har ofte en rekke sensitive personopplysninger. Vi må derfor så langt som mulig sikre oss at slike opplysninger ikke er tilgjengelige for utenforstående.

5 Ansvarsplassering

5.1 Behandlingsansvarlig

Den behandlingsansvarlige er definert i loven 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" (GDPR, kap. 1, art. 4, nr 7).

Ansvarsplassering: For forskningsprosjekter som utføres av NR, er det NR ved **adm. dir.** som er behandlingsansvarlig. Dette gjelder alle prosjekter som utføres i regi av NR, også prosjekter som vi utfører på vegne av andre, f.eks. direktorater og departementer. I praksis vil deler av ansvaret være delegert til forskningssjef eller prosjektleder.

NR er kan være behandlingsansvarlig også for behandling av data som vi har overtatt fra andre, for eksempel SSB.

NR er videre behandlingsansvarlig for data som innhentes av andre på vegne av NR, for eksempel et opinionsundersøkelsesinstitutt.

5.2 Databehandler

Som databehandler regnes *"en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige"* (GDPR, kap. 1, art. 4 nr 8). I de tilfellene hvor dataene blir samlet inn på NR, er prosjektleder databehandler. Databehandlere kan også være firmaer som vi kjøper databehandlingstjenester av eller som vi har databehandleravtaler med, som DNB og Gjensidige. Det kan dreie seg om datainnsamling, men det kan også dreie seg om ren behandling av innsamlete data.

I GDPR, kap. 4 er det stilt krav både til den behandlingsansvarlige og til databehandleren angående dokumentasjon av informasjonssystemet man bruker, og av sikkerhetstiltakene man har iverksatt. Den behandlingsansvarlige må påse at også eksterne databehandlere har tilfredsstillende systemer og rutiner. Det skal tas med en passus om dette i avtalene NR inngår med databehandlere inklusiv hvordan koblingsnøkkelen skal behandles.

Ansvarsplassering: Det er **prosjektleders** ansvar å påse at så skjer.

5.3 Prosjektleders ansvar

Prosjektleders ansvar er å følge de rutinene som framgår av NRs internkontrollsystem/-rutinebeskrivelser for oppfølging av personopplysningsloven i forskningsprosjekter. Dette innebærer at prosjektleder for hvert enkelt prosjekt bl.a. skal

- sende inn utfylt meldeskjema til NSD (jf. pkt. 7.1) og eventuelt også bidra med nærmere opplysninger som er relevant for å vurdere behovet for en konsekvensvurdering (DPIA) og der hvor saken må videre til Datatilsynet for forhåndsdrøftelser. Herunder skal alle sentrale endringer meldes NSD.
- ta imot og behandle henvendelser fra enkeltpersoner ("registrerte") som ønsker innsyn i og eventuelt retting eller sletting av opplysninger om seg selv.
- registrere prosjektet i NRs prosjektdatabase ved å fylle ut prosjektkort som leveres til regnskap og dokumentere alle sentrale begivenheter som gjelder oppfølging av våre forpliktelser etter personopplysningsloven i arkivet.
- påse at eksterne databehandlere har tilfredsstillende rutiner, jf. pkt. 5.2.

5.4 Ansattes ansvar

NRs arbeidsreglement regulerer den ansattes ansvar i forhold til bl.a. taushetsplikt og bruk av NRs IT-systemer.

6 Grunnvilkår for behandling av personopplysninger

6.1 Oversikt

Grunnkravene for behandling av personopplysninger følger av GDPR, kap. 2, art. 5:

> *"**Prinsipper for behandling av personopplysninger***
>
> *1. Personopplysninger skal*
>
> *a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),*
>
> *b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal, i samsvar med artikkel 89 nr. 1, ikke anses som uforenlig med de opprinnelige formålene («formålsbegrensning»),*
>
> *c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),*
>
> *d) være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes («riktighet»),*
>
> *e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter («lagringsbegrensning»),*
>
> *f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»).*
>
> *2. Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes («ansvar»)."*

Det er **prosjektleders ansvar** å vurdere om disse grunnkravene er oppfylt. Hvordan vurderingen skal dokumenteres, fremgår av kapittel 14.

6.2 Vilkår for databehandling – hjemmelskrav

De generelle vilkår for behandling av personopplysninger fremgår av GDPR, kap. 2, art. 6 om behandlingens lovlighet, første del:

" *Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:*

a) den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål,

b) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,

c) behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,

d) behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser,

e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,

f) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn."

GDPR, kap.9, art. 89 regulerer bruk av persondata for forskningsformål:

«*Behandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal omfattes av nødvendige garantier i samsvar med denne forordning for å sikre den registrertes rettigheter og friheter. Nevnte garantier skal sikre at det er innført tekniske og organisatoriske tiltak for særlig å sikre at prinsippet om dataminimering overholdes. Nevnte tiltak kan omfatte pseudonymisering, forutsatt at nevnte formål kan oppfylles på denne måten. Dersom nevnte formål kan oppfylles ved viderebehandling som ikke gjør det mulig eller ikke lenger gjør det mulig å identifisere de registrerte, skal formålene oppfylles på denne måten.*»

Innhenting og behandling av personopplysninger kan som hovedregel bare skje på grunnlag av samtykke ut fra pkt a over. Det er viktig for NR å etterkomme dette kravet.

For at samtykket skal anses som informert, bør følgende informasjon gis til den person opplysningene registreres på:

1. navn og adresse på den behandlingsansvarlige
2. hva opplysningene skal brukes til
3. om opplysningene vil bli utlevert til andre, og eventuelt hvem som er mottaker
4. om det er frivillig å gi fra seg opplysningene
5. informasjon som gjør den registrerte i stand til å bruke sine rettigheter etter personopplysningsloven på best mulig måte, som f.eks. om hvilken rett man har til å kreve innsyn, retting og sletting
6. hvor lenge personopplysningene vil bli behandlet eller oppbevart.

Se kapittel 14 for mer utfyllende informasjon om utforming av informasjonsskriv og samtykkeerklæring. Personer under 18 år kan ikke uten videre selv samtykke. Det vil avhenge av opplysningenes karakter sammenholdt med den enkelte alder og modning. Som en tommel-

fingerregel bør samtykke innhentes også fra foresatte dersom det dreier seg om personer på ungdomsskoletrinnet eller yngre. Det kan være strengere regler for medisinsk og helsefaglig forskning.

Dersom det ikke kan innhentes samtykke, må **prosjektleder** vurdere om datainnhentingen kan begrunnes i et av de øvrige alternativene. Blant hensyn det kan legges vekt på, er prosjektets allmennytte.

Vurderingen skal fremgå av meldeskjemaet til NSD.

6.3 Datasett som inneholder særlige kategorier av personopplysninger

GDPR kap 1, art. 9 inneholder strengere regler for særlige kategorier av personopplysninger:

«1. Behandling av personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, er forbudt.

2. Nr. 1 får ikke anvendelse dersom et av følgende vilkår er oppfylt:

a) Den registrerte har gitt uttrykkelig samtykke til behandling av slike personopplysninger for ett eller flere spesifikke formål, unntatt dersom det i unionsretten eller medlemsstatenes nasjonale rett er fastsatt at den registrerte ikke kan oppheve forbudet nevnt i nr. 1.

b) Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på området arbeidsrett, trygderett og sosialrett i den grad dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett, eller en tariffavtale i henhold til medlemsstatenes nasjonale rett som gir nødvendige garantier for den registrertes grunnleggende rettigheter og interesser.

c) Behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser dersom den registrerte fysisk eller juridisk ikke er i stand til å gi samtykke.

d) Behandlingen utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, religiøs eller fagforeningsmessig art, som ledd i organets berettigede aktiviteter og med nødvendige garantier, forutsatt at behandlingen bare gjelder organets medlemmer eller tidligere medlemmer eller personer som på grunn av organets mål har regelmessig kontakt med det, og at personopplysningene ikke utleveres til andre enn nevnte organ uten de registrertes samtykke.

e) Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort.

f) Behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav eller når domstolene handler innenfor rammen av sin domsmyndighet.

g) Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.

h) Behandlingen 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 på grunnlag av unionsretten eller medlemsstatenes nasjonale rett eller i henhold til en avtale med helsepersonell og med forbehold for vilkårene og garantiene nevnt i nr. 3.

i) Behandlingen 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, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett der det fastsettes egnede og særlige tiltak for å verne den registrertes rettigheter og friheter, særlig taushetsplikt.

j) Behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1 på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.

3. Personopplysningene nevnt i nr. 1 kan behandles for formålene nevnt i nr. 2 bokstav h) dersom opplysningene behandles av en fagperson som har taushetsplikt i henhold til unionsretten eller medlemsstatenes nasjonale rett eller regler fastsatt av nasjonale vedkommende organer, eller under en slik persons ansvar, eller av en annen person som også har taushetsplikt i henhold til unionsretten eller medlemsstatenes nasjonale rett eller regler fastsatt av nasjonale vedkommende organer.»

Også her er det viktig å innhente samtykke (bokstav a). Hvis dette ikke lar seg innhente, vil særlig bokstav h være aktuell. **Prosjektleder** må da vurdere om databehandlingen er nødvendig for historiske, statistiske eller vitenskapelige formål, og om samfunnsinteressen klart overstiger eventuelle ulemper for den enkelte.

6.4 Formål med behandlingen

Det fremgår at personopplysninger bare kan nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet.

Det forutsettes at formålet konkretiseres. Det er ikke tilstrekkelig å henvise til forsknings- og/eller dokumentasjonsformål i sin alminnelighet. Videre må formålet ligge innenfor rammen av NRs virksomhet. **Prosjektleder** skal beskrive formålet i meldeskjemaet.

6.5 Dataenes relevans

Det et krav at personopplysningene er tilstrekkelige og relevante for formålet med behandlingen. Dette innebærer at det må være en relevant sammenheng mellom formålet med prosjektet og de personopplysninger som innhentes.

Dette innebærer at det ikke skal innhentes flere opplysninger enn det som er relevant for prosjektet. Dette dokumenteres gjennom beskrivelsen av metoden for datainnhenting og av datamaterialets innhold i meldeskjemaet.

6.6 Senere bruk av dataene

Data bare kan brukes til det angitte og berettigede formål. Om bruken er innenfor det angitte formål må derfor vurderes av Prosjektleder. Dette må vurderes eventuelle ulemper for den enkelte dersom opplysningene ikke allerede er anonymisert. Angående lagring av dataene gjelder følgende (GDPR, kap 2, art. 5 nr 1e):

> *"Personopplysninger skal…lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter («lagringsbegrensning»),."*

7 Identifisering av krav og plikter

7.1 Forhold til Datatilsynet/Norsk senter for forskningsdata (NSD)

Behandlingsansvarlig er ansvarlig for behandling av personopplysninger i sin virksomhet. Dette skal følges opp ved internkontroll. I tillegg er det utfyllende regler for når virksomheten er pålagt å benytte personvernombud, søke om forhåndsgodkjenning fra Datatilsynet eller få godkjenning fra REK, for prosjekter innen helse. Ofte vil imidlertid NR være databehandler og dette ansvaret vil ligge hos ekstern behandlingsansvarlig i prosjektet.

GDPR gir følgende regler for utpeking av personvernombud (GDPR, art. 37, nr 1)

«Den behandlingsansvarlige og databehandleren skal utpeke et personvernombud når

a) behandlingen utføres av en offentlig myndighet eller et offentlig organ, bortsett fra domstoler som opptrer innenfor rammen av sin domsmyndighet,

b) den behandlingsansvarliges eller databehandlerens kjernevirksomhet består av behandlingsaktiviteter som på grunn av sin art, sitt omfang og/eller formål krever regelmessig og systematisk monitorering i stor skala av registrerte, eller

c) den behandlingsansvarliges eller databehandlerens kjernevirksomhet består av behandling i stor skala av særlige kategorier av opplysninger i henhold til artikkel 9 eller personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10.»

NR har avtale med Norsk senter for forskningsdata AS (NSD) om at NSD skal være personvernombud for NR. Avtalen innebærer at NR skal gi melding om prosjekter og sende søknader om forhåndsgodkjenning til NSD – som også skal gi oss råd og veiledning. I de tilfeller hvor det kreves forhåndsgodkjenning, sender NSD saken til Datatilsynet med sin innstilling.

Datatilsynet informer på sine nettsider at

«I den nye personopplysningsloven med personvernforordning er ordningen med meldeplikt fjernet helt. Det er dermed ingen behandlinger som skal meldes til Datatilsynet via meldeskjema lenger. Det samme gjelder i all hovedsak også krav til forhåndsgodkjenning (konsesjon) fra Datatilsynet.

Det at konsesjonsordningen er fjernet betyr at det ikke lenger er nødvendig å søke om tillatelser til å starte nye behandlinger. Det er heller ikke behov for å søke om å gjøre endringer i allerede pågående behandlinger. Det er imidlertid innført overgangsregler på noen få områder i påvente av at nytt regelverk kommer på plass.

Formålet med endringene er å flytte ansvaret for behandling av personopplysninger fra Datatilsynet til virksomhetene, og fjerne byråkratiske prosesser når personopplysninger behandles. Datatilsynet skal derfor nå kontrollere etterlevelse av regelverket gjennom tilsyn i stedet for å forhåndsgodkjenne behandlinger.»

7.2 Vurdering av personvernkonsekvenser og forhåndsdrøftinger

GDPR art 35 pkt 1. sier at om det *«medfører en høy risiko for fysiske personer rettigheter og friheter»* skal det gjennomføres en vurdering av personvernkonsekvenser (DPIA). GDPR art 35 nr 3 eksemplifiserer dette ved

«En vurdering av personvernkonsekvenser som nevnt i nr. 1 skal særlig være nødvendig i følgende tilfeller:

a) en systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen,

b) behandling i stor skala av særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1, eller av personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10, eller

c) en systematisk overvåking i stor skala av et offentlig tilgjengelig område.»

GDPR art. 9 nr 1 omfatter «*personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering»*

Dersom DPIA viser at behandlingen vil medføre høy risiko for de registrertes rettigheter og friheter, og man ikke klarer å redusere denne risikoen, må prosjektet rådføre seg med Datatilsynet før behandlingen igangsettes som en forhåndsdrøftelse (GDPR, art. 36).

Det er **prosjektleders ansvar** å fylle ut NSDs meldeskjema. Dette skal gjøres for alle prosjekter som innebærer innsamling av data på individnivå ved NR. Prosjektleder skal samtidig ta standpunkt til om dataene inneholder personopplysninger i lovens forstand, herunder om det foreligger indirekte identifiserbare opplysninger. Dette skal gjøres senest 30 dager før man starter med behandlingen av personopplysningene, dvs. før innsamlingen av data starter.

Settes det i gang et nytt forskningsprosjekt som bruker data på individnivå som tidligere er brukt i andre prosjekter ved NR, eller som er samlet inn ved andre institusjoner, har **prosjektlederen for det nye prosjektet** ansvaret for å sende inn melding om dette prosjektet til NSD. Unntak fra dette gjelder eldre datasett der det er på det rene at opplysningene ikke lenger kan knyttes til personer.

Se for øvrig rutinebeskrivelse under punkt 14.1 – 14.6, (i hovedsak) underpunkt 2.

7.3 Plikter i forhold til den opplysningene gjelder

7.3.1 Klar og tydelig informasjon

GDPR art 12 nr 1 pålegger behandlingsansvarlig ansvar for klar og tydelig kommunikasjon til den registrerte:

«…behandlingen på en kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk, især når det gjelder informasjon som spesifikt er rettet mot et barn. Informasjonen skal gis skriftlig eller på en annen måte, herunder elektronisk dersom det er hensiktsmessig. På anmodning fra den registrerte kan informasjonen gis muntlig, forutsatt at den registrertes identitet bevises på andre måter.»

GDPR art 13 gir utfyllende informasjon:

1. Når personopplysninger om en registrert samles inn fra den registrerte, skal den behandlingsansvarlige på tidspunktet for innsamlingen av personopplysningene gi den registrerte følgende informasjon:

a) identiteten og kontaktopplysningene til den behandlingsansvarlige og eventuelt den behandlingsansvarliges representant,

b) kontaktopplysningene til personvernombudet, dersom dette er relevant,

c) formålene med den tiltenkte behandlingen av personopplysningene samt det rettslige grunnlaget for behandlingen,

d) dersom behandlingen er basert på artikkel 6 nr. 1 bokstav f), de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart,

e) eventuelle mottakere eller kategorier av mottakere av personopplysningene,

f) dersom det er relevant, det faktum at den behandlingsansvarlige akter å overføre personopplysninger til en tredjestat eller en internasjonal organisasjon og om hvorvidt Kommisjonen har truffet en beslutning om tilstrekkelig beskyttelsesnivå eller ikke, eller når det gjelder overføringene nevnt i artikkel 46 eller 47 eller artikkel 49 nr. 1 annet ledd, en henvisning til nødvendige eller passende garantier, hvordan man får tak i et eksemplar av dem, eller hvor de er gjort tilgjengelig.

2. I tillegg til informasjonen nevnt i nr. 1 skal den behandlingsansvarlige på tidspunktet for innsamling av personopplysninger gi den registrerte følgende ytterligere informasjon som er nødvendig for å sikre en rettferdig og åpen behandling:

a) det tidsrom personopplysningene vil bli lagret, eller dersom dette ikke er mulig, kriteriene som brukes for å fastsette dette tidsrommet,

b) retten til å anmode den behandlingsansvarlige om innsyn i og retting eller sletting av personopplysninger eller begrensning av behandlingen som gjelder den registrerte, eller til å protestere mot behandlingen samt retten til dataportabilitet,

c) dersom behandlingen er basert på artikkel 6 nr. 1 bokstav a) eller artikkel 9 nr. 2 bokstav a), retten til når som helst å trekke tilbake et samtykke uten at det påvirker lovligheten av en behandling basert på et samtykke før samtykket trekkes tilbake,

d) retten til å klage til en tilsynsmyndighet,

e) om det foreligger et lovfestet eller avtalefestet krav om å gi personopplysninger eller et krav som er nødvendig for å inngå en avtale, samt om den registrerte har plikt til å gi personopplysningene og om mulige konsekvenser dersom vedkommende ikke gjør det,

f) forekomsten av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4, og, i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte.

3. Dersom den behandlingsansvarlige har til hensikt å viderebehandle personopplysningene for et annet formål enn det opplysningene ble samlet inn for, skal den behandlingsansvarlige før nevnte viderebehandling gi den registrerte informasjon om nevnte andre formål og annen nødvendig informasjon som nevnt i nr. 2.»

Informasjonen skal normalt gis sammen med utsendelse av spørreskjema, eller når vedkommende kontaktes med sikte på deltakelse i prosjektet, og under enhver omstendighet før opplysningene gis fra den som registreres.

Vanligvis skal informasjonen gis **skriftlig**, selv om loven i og for seg ikke stiller opp dette som et krav. Unntak kan tenkes der dette er uhensiktsmessig i forhold til den måten dataene innhentes på, forutsatt at vi sikrer oss at lovens krav til innholdet av informasjonen oppfylles.

Det er **prosjektleders ansvar** at informasjon som nevnt i § 19 første ledd blir gitt.

Se for øvrig rutinebeskrivelse under punkt 14.1-14.5, underpunkt 3, som omhandler informasjonsskriv og samtykkeerklæring.

Ved innhenting av opplysninger fra andre (GDPR art 14 nr 1)

"Dersom personopplysninger ikke er blitt samlet inn fra den registrerte, skal den behandlingsansvarlige gi den registrerte følgende informasjon:

a) identiteten og kontaktopplysningene til den behandlingsansvarlige og eventuelt den behandlingsansvarliges representant,

b) kontaktopplysningene til personvernombudet, dersom dette er relevant,

c) formålene med den tiltenkte behandlingen av personopplysningene samt det rettslige grunnlaget for behandlingen,

d) de berørte kategoriene av personopplysninger,

e) eventuelle mottakere eller kategorier av mottakere av personopplysningene,

f) dersom det er relevant, at den behandlingsansvarlige har til hensikt å overføre personopplysninger til en mottaker i en tredjestat eller en internasjonal organisasjon og om hvorvidt Kommisjonen har truffet en beslutning om tilstrekkelig beskyttelsesnivå eller ikke, eller, når det gjelder overføringene nevnt i artikkel 46 eller 47 eller artikkel 49 nr. 1 annet ledd, en henvisning til nødvendige eller passende garantier, hvordan man får tak i et eksemplar av dem eller hvor de er gjort tilgjengelig."

NR driver ikke med lovbestemt innsamling eller formidling av personopplysninger. I stor grad vil NR får data som er samlet inn av andre og der andre har ansvaret for informasjon til registrerte.

7.3.2 Innsyn

Registrerte har rett til innsyn etter GDPR art 15 nr 1

"Den registrerte skal ha rett til å få den behandlingsansvarliges bekreftelse på om personopplysninger om vedkommende behandles, og, dersom dette er tilfellet, innsyn i personopplysningene og følgende informasjon:

a) formålene med behandlingen,

b) de berørte kategoriene av personopplysninger,

c) mottakerne eller kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, særlig mottakere i tredjestater eller internasjonale organisasjoner,

d) dersom det er mulig, hvor lenge det forventes at personopplysningene vil bli lagret, eller, dersom dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden,

e) retten til å anmode den behandlingsansvarlige om retting eller sletting av personopplysninger eller begrensning av behandlingen av personopplysninger som gjelder den registrerte, eller til å protestere mot nevnte behandling,

f) retten til å klage til en tilsynsmyndighet,

g) dersom personopplysningene ikke er samlet inn fra den registrerte, all tilgjengelig informasjon om hvor personopplysningene stammer fra,

h) forekomsten av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4, og, i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte."

Henvendelser om **"innsyn"** skal gå til **prosjektleder**. Svar skal gis pr. brev (f.eks. et standardbrev som til enhver tid er ajourført i forhold til hvilke typer personopplysninger som behandles mv.) og/eller ved å henvise til NSDs offentlige database over forskningsprosjekter som behandler personopplysninger.

7.3.3 Retteplikt

GDPR art 16 gir registrerte rett til å få data rettet:

> *" Den registrerte skal ha rett til å få uriktige personopplysninger om seg selv rettet av den behandlingsansvarlige uten ugrunnet opphold. Idet det tas hensyn til formålene med behandlingen skal den registrerte ha rett til å få ufullstendige personopplysninger komplettert, herunder ved å framlegge en supplerende erklæring. "*

Det er **prosjektleders ansvar** at NR på eget initiativ retter opplysninger som man blir klar over er feilaktig registrert. Likeledes er det **prosjektleders ansvar** å ta imot eventuelle henvendelser om retting fra registrerte. Dersom et slikt krav innebærer at anonymiteten må brytes, avslås kravet.

Se for øvrig rutinebeskrivelse under punkt 14.

7.3.4 Sletteplikt

GDPR art 17 gir registrerte rett til å få data slettet:

> *"Den registrerte skal ha rett til å få personopplysninger om seg selv slettet av den behandlingsansvarlige uten ugrunnet opphold, og den behandlingsansvarlige skal ha plikt til å slette personopplysninger uten ugrunnet opphold dersom et av de følgende forhold gjør seg gjeldende:*
>
> *a) personopplysningene er ikke lenger nødvendige for formålet som de ble samlet inn eller behandlet for,*
>
> *b) den registrerte trekker tilbake samtykket som ligger til grunn for behandlingen, i henhold til artikkel 6 nr. 1 bokstav a) eller artikkel 9 nr. 2 bokstav a), og det ikke finnes noe annet rettslig grunnlag for behandlingen,*
>
> *c) den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 1, og det ikke finnes mer tungtveiende berettigede grunner til behandlingen, eller den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 2,*
>
> *d) personopplysningene er blitt behandlet ulovlig,*
>
> *e) personopplysningene må slettes for å oppfylle en rettslig forpliktelse i unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige er underlagt,*
>
> *f) personopplysningene er blitt samlet inn i forbindelse med tilbud om informasjonssamfunnstjenester som nevnt i artikkel 8 nr. 1."*

I utgangspunktet skal altså personopplysninger slettes når formålet med dem er oppnådd – altså når forskningsprosjektet/-ene opplysningene brukes i, er sluttført.

GDPR art 17 nr 3 c og d inneholder imidlertid en viktig begrensning i sletteplikten:

«c) av hensyn til allmennhetens interesse på området folkehelse i samsvar med artikkel 9 nr. 2 bokstav h) og i) og artikkel 9 nr. 3,

d) for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1 i den grad rettigheten nevnt i nr. 1 sannsynligvis vil gjøre det umulig eller i alvorlig grad vil hindre at målene med nevnte behandling nås,»

Det er **prosjektleders ansvar** å sørge for at personopplysninger (altså opplysninger som er direkte identifiserbare, indirekte identifiserbare eller avidentifiserte) slettes når det ikke lenger er bruk for dem. Prosjektleder skal imidlertid først ta opp med **forskningssjefen** spørsmålet om å oppbevare/lagre opplysningene for framtidige forskningsformål. Det er **forskningssjefen** som skal ta standpunkt til dette spørsmålet. Ønsker man å lagre opplysningene, skal de anonymiseres så sant dette er mulig og det ikke går ut over den verdien de har for forskningen. Også her er det **forskningssjefen** som skal ta standpunkt til om det er tilstrekkelig å oppbevare opplysningene i anonymisert form.

Så snart personopplysninger anonymiseres, bortfaller alle plikter osv. etter personopplysningsloven.

Prosjektleder er ansvarlig for at slik sletting foretas, og at melding om dette sendes til NRs administrasjon og NSD.

Se for øvrig rutinebeskrivelse under punkt 14.

8 Risikoanalyse

8.1 Vurdering av mulige personvernkonsekvenser (DPIA)

Det følger av det som er sagt under pkt. 4.4, at det sentrale mål for NR er å bevare personopplysningers konfidensialitet. Det innebærer at det er særlig dette det bør legges vekt på ved vurderingen av sikkerhetsrisiko og akseptabelt risikonivå.

Risikoen er derfor primært knyttet til at personopplysninger kommer på avveier. Det er bare i mindre grad et problem i forhold til personopplysningslovens formål om data endres utilsiktet, eller om de ikke er tilgjengelige, siden dataene ikke brukes i forhold til enkeltpersoner. En aktuell problemstilling er om data brukes til andre formål enn det som er godkjent.

I noen tilfeller må det foretas en risikoanalyse knyttet til personvernkonsekvenser (DPIA) (GDPR art. 35, nr 1-2):

«*1. Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.*

2. Den behandlingsansvarlige skal rådføre seg med personvernombudet, dersom et personvernombud er utpekt, i forbindelse med utførelsen av en vurdering av personvernkonsekvenser.»

Det kan være aktuelt å gjennomføre forhåndsdrøfting med tilsynsmyndigheten (GDPR, art 36 nr 1)

«Den behandlingsansvarlige skal rådføre seg med tilsynsmyndigheten før behandlingen dersom en vurdering av personvernkonsekvenser i henhold til artikkel 35 tilsier at behandlingen vil medføre en høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.»

8.2 Konsekvenser dersom opplysningene kommer ut

Noen av datasettene ved NR kan inneholde meget sensitive opplysninger. Som eksempler på slike opplysninger kan det nevnes helseopplysninger, opplysninger om kriminell atferd, opplysninger om tiltak og ytelser fra det offentlige hjelpeapparatet. Det bør legges til grunn at disse opplysningene vil innebære høy grad av sosial belastning hvis de kommer på avveie og kan knyttes til enkeltpersoner.

Andre datasett inneholder bare opplysninger som i mindre grad vil være belastende hvis de blir kjent og kan knyttes til enkeltpersoner. Det gjelder for eksempel opplysninger om medlemskap i idrettsforeninger eller opplysninger om fritidsaktiviteter. Konsekvensen av en lekkasje er derfor mindre her.

I og for seg kan dette tale for et ulikt sikkerhetsnivå etter arten av opplysninger datasettene inneholder. Dette vil imidlertid gjøre våre rutiner unødig kompliserte. Vi bør derfor ta utgangspunkt i at alle datasett som faller innenfor personopplysningsloven, inneholder opplysninger som, hvis de kommer ut og kan knyttes til enkeltpersoner, kan representere en høy sosial belastning.

Tilsvarende bør vi ta utgangspunkt i at alle datasett som inneholder taushetsbelagte opplysninger, inneholder opplysninger som, hvis de kommer ut og kan skade oppdragsgiveren eller NR, kan representere en stor belastning.

8.3 Sannsynlighet for uautorisert bruk

For å redusere sjansen for datainntrengning, bør personidentifiserende opplysninger oppbevares atskilt fra datasettene for øvrig.

I noen tilfeller er datasettet av en slik karakter at de personidentifiserende opplysningene ikke lar seg skille fra de øvrige opplysningene. Dette gjelder kategori 2 i pkt. 3.2 ovenfor. I disse tilfellene må det imidlertid gjennomføres nokså omfattende analyser, i tillegg til å skaffe seg tilgang til dataene, for å kunne knytte opplysningene til konkrete personer. Det må derfor anses som akseptabel risiko å behandle disse datasettene i henhold til de normale sikkerhetsrutiner beskrevet i kap. 9.

9 Datasikkerhet

9.1 Sikkerhetsmål

Om de overordnete sikkerhetsmål vises til pkt. 4.1 med følgende delmål:

a) Vern mot datainntrengning. Datasystemet skal være sikret mot at utenforstående får tilgang til personopplysninger. Det skal også være sikret mot at filer eller andre deler av systemet ødelegges.
b) Vern mot uautorisert bruk. Bare de som arbeider med prosjektet skal, i den utstrekning det er nødvendig, ha tilgang til personidentifiserbare opplysninger.
c) Vern mot fysisk inntrengning. Personopplysninger skal oppbevares slik at utenforstående ikke har adgang til opplysningene.

9.2 Sikkerhetsnivåer

NR har definert sikkerhetsnivåer under. Disse skal anvendes på all informasjon på NRs datamaskiner: prosjektdata, administrative informasjon og andre data og programmer. Prosjektleder har ansvaret for klassifisering av prosjektdata og at dette følges opp inklusiv sletting etter at prosjektet er avsluttet. Det må tas hensyn til avtaler, krav fra kunde og evt. dataansvarlig utenfor NR. Administrasjonssjefen og IT-sjef har ansvar for Admins egne data. Adm. dir. og hele ledelsen er ansvarlig for at sikkerheten ivaretas tilfredsstillende.

Definisjoner

Bruker	Dette er en ansatt på NR, eller noen som har underskrevet nødvendige avtaler for å få en konto eller tilgang til å koble opp utstyr på NRs nettverk.
Brukerutstyr	Stasjonære datamaskiner, bærebare PCer og mobiltelefoner. Merk at mobiltelefoner skal være koblet til gjestenettverket.
Fjernstyring	Mekanisme som brukes for tilkobling til sentral eller dedikert server, hvor en har rettigheter til å kjøre programvare direkte på maskinen. Eksempler her er Remote Desktop på Windows og ssh på Linux.
Sentral server	Dette er Linux og Windows servere hvor alle ansatte (basert på gruppemedlemskap) har rettigheter til å logge på.
Dedikert server	Dette er Linux og Windows servere hvor rettighet til pålogging er begrenset til enkeltpersoner eller en gruppe med et fåtall medlemmer.
Lukket klient-nettverk	Nettverk hvor en har tilgang til sentrale servere og dedikerte servere. Brukerutstyr av typen bærbare PCer og stasjonære datamaskiner vil normalt være koblet til dette nettverket.
Gjestenettverk	Nettverk hvor en kun har tilgang til internett, ikke interne servere.

Åpen

Innhold: Informasjon om NR og forskningsresultater vi ønsker å informere om.

Krav: Skal kunne legges på ekstern web.

Intern
Innhold: De fleste prosjekter er på dette nivået. Gjelder all informasjon på NRs datamaskiner som ikke er klassifisert som åpen eller på et høyere sikkerhetsnivå. Informasjon som er tenkt for intern behandling og hvor kompromittering, tap eller utilgjengelighet kan føre til uønsket offentliggjøring og mindre økonomisk tap eller skade på NR eller samarbeidspartneres renomme.

Krav:

- Alle godkjente brukere skal signere taushetserklæring med IT-disiplininstruks.
- Brukerutstyr (alle typer elektronisk utstyr som har tilgang innenfor NRs brannmur) skal beskyttes med passord før det forlates. Unntatt er utstyr på gjestenettverk.
- Brukerutstyr skal oppdateres fortløpende.
- Filtilgang skal begrenses per datasett til en avgrenset gruppe ved hjelp av filrettigheter for brukere. Behandling av data skal skje på sentrale servere og på brukerutstyr.
- Brukerutstyr kan ha internettilgang.
- Sentrale servere kan være tilgjengelige via krypterte oppkoblinger.

Fortrolig
Innhold: Sensitiv personinformasjon inklusiv sensitiv informasjon om NRs ansatte. Prosjektdata og annen informasjon hvor kompromittering, tap eller utilgjengelighet kan føre til uønsket offentliggjøring og betydelig økonomisk tap eller skade på NR eller samarbeidspartneres renomme.

Krav: Som internt bortsett fra at behandling av data ikke kan skje på brukerutstyr og i tillegg:

- Kun NRs sentrale servere eller dedikerte servere skal brukes til behandling av data. Bruk av skytjenester må avtales spesielt.
- Dersom sensitive data skal overføres via internett, skal det skje ved hjelp av krypterte overføringer.
- Filtilgang skal begrenses per datasett til en avgrenset gruppe, bestående kun av prosjektmedlemmer, ved hjelp av filrettigheter for brukere.
- Filområdet kan være unntatt backup om ønskelig.

Strengt fortrolig
Innhold: Sensitive prosjektdata og annen informasjon hvor kompromittering, tap eller utilgjengelighet kan føre til alvorlig økonomisk tap eller skade på NR eller samarbeidspartneres renomme.

Krav: Som fortrolig bortsett fra at behandling ikke kan skje på sentrale servere og i tillegg:

- Behandling av sensitive data skal skje på dedikerte servere med egen tilgangskontroll.
- Tilgang skal skje kun via fjernstyring og krypterte oppkoblinger.
- Oppkobling til dedikert server skal komme fra NRs lukkede klient-nettverk.
- Data skal lagres på krypterte partisjoner, slik at IT-personell vil ikke ha teoretisk tilgang til å lese innhold, hverken direkte på underliggende lagring eller på backup. Prosjektleder skal taste inn ett eget passord brukt for tilgang til lagring ved hver oppstart.
- Sensitive datasett som skal brukes skal overleveres til NR på et fysisk medium (altså ikke via internett).
- Maskinene skal være herdet ut over normalt for sentrale servere.

- Eventuelt: Tilgang til dedikert server krever 2-faktorautentisering.

Hemmelig
Innhold: Sensitive prosjektdata og annen informasjon hvor kompromittering, tap eller utilgjengelighet kan føre til meget alvorlig økonomisk tap eller skade på NR eller samarbeidspartneres renomme.

Krav: Som strengt fortrolig, og i tillegg:

- Maskinene som er involvert skal være enten helt frittstående uten mulighet for nettverk, eller tilknyttet et eget separat kablet nettverk. Maskinene skal ikke ha tilknytning til internett.
- Brukerutstyr som skal ha tilgang til dedikert server skal ikke ha tilgang til annet enn separat nettverk.
- Tilgang er kun via fysisk bruk direkte av maskinen. Backup håndteres separat. Det kreves vern mot datainntrengning, f.eks. ved at maskiner låses inn i metallskap etter bruk.

Datateknisk sikring
NR skal ha oppdaterte brannmursystemer. NR skal ha løsninger for automatisk oppdatering av programvare på servere og klientmaskiner tilhørende NR og koblet til NRs nettverk

NR skal ha oppdaterte viruskontrollsystemer.

ANSVARLIG: DATAANSVARLIG

9.3 Oppbevaring av personopplysninger
Datasett tilhørende kategori 1 (det vil si datasett med direkte identifiserbare opplysninger) skal oppbevares minst på sikkerhetsnivå *Fortrolig* (eller forsvarlig nedlåst hvis opplysningene fins på andre medier).

Datasett tilhørende kategori 2 (det vil si datasett med avidentifiserte opplysninger der enkelte undergrupper er små nok til at personer kan identifiseres) kan oppbevares på sikkerhetsnivå *Fortrolig*. Hvis identifisering av enkeltpersoner vurderes som relativt enkelt, skal oppbevaring på sikkerhetsnivå *Strengt fortrolig* vurderes.

Datasett tilhørende kategori 3 (det vil si datasett med avidentifiserte opplysninger – NR har koblingsnøkkelen) kan oppbevares på sikkerhetsnivå *Fortrolig*. Koblingsnøkkelen skal oppbevares enten på dedikert maskin eller forsvarlig nedlåst.

Datasett tilhørende kategorier 4 og 5 (det vil si datasett med avidentifiserte opplysninger – koblingsnøkkelen oppbevares midlertidig andre steder eller NR uten tilgang til koblingsnøkkelen) kan oppbevares på sikkerhetsnivå *Intern* eller *Fortrolig*. Institusjonen som oppbevarer kodenøkkelen, er forpliktet til å oppbevare kodenøkkelen på en sikker og forsvarlig måte.

Datasett tilhørende kategori 6 (det vil si datasett med anonyme opplysninger) kan oppbevares på sikkerhetsnivå *Intern*. Også sikkerheten for slike anonyme data må ivaretas på en tilstrekkelig måte, slik at det formidles at NR behandler data på en forsvarlig måte, uavhengig av om de er anonyme eller ikke.

ANSVARLIG: PROSJEKTLEDER

10 Datakvalitet

Et krav i loven er at personopplysninger skal være korrekte og oppdaterte. Selv om dette kravet i personvernsammenheng ikke er prioritert sammenlignet med kravet om datasikkerhet, er det likevel essensielt for NR som forskningsinstitusjon at dataene som blir brukt, er av så høy kvalitet som mulig, og at mulige kvalitetsmangler blir vurdert i publikasjoner.

Forskere ved NR skal sikre datakvalitet og dokumentasjon av mangler ved å holde seg til det følgende:

1. Det må til enhver tid oppbevares en original datakilde som forskere i prosjektet kan gå tilbake til for å kvalitetssikre resultater når det oppstår tvil om riktigheten av resultater. For kvantitative, elektronisk lagrede data betyr dette at en skrivebeskyttet originalfil oppbevares på en sikker måte og at forandringer av datafilen bare blir foretatt på kopier av denne originalfilen. Originale datafiler forandres bare når opplysninger i originalfilen må rettes opp, eller når informasjon i filen skal slettes/aggregeres for å tilfredsstille personvernet.

2. Eventuelle problematiske sider ved datakvaliteten dokumenteres når de blir oppdaget, og må bli gjort kjent for alle forskerne som bruker dataene. Forskere som arbeider med dataene forplikter seg til å informere prosjektleder når de får kjennskap til problemer med datakvaliteten.

11 Etiske komiteer

Det fins tre nasjonale komiteer for forskningsetikk: Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora (NESH), Den nasjonale forskningsetiske komité for medisin (NEM) og Den nasjonale forskningsetiske komité for naturvitenskap og teknologi (NENT). I tillegg fins det til sammen syv regionale komiteer for medisinsk og helsefaglig forskningsetikk (REK). NESH og NENT er rådgivende organer som blant annet gir råd til forskere ved henvendelser om konkrete forskningsprosjekter. Forskningsprosjekter innen medisin og helsefag hvor det inngår forsøk på mennesker og som ikke er av en slik art at det regnes som en del av vanlig etablert behandlingsprosedyre må søkes REK før de kan bli gjennomført. NEM behandler derfor ikke enkeltprosjekter direkte, men klagesaker fra REK.

Siden 2007 er arbeidet av de etiske komiteene regulert gjennom Forskningsetikkloven. De etiske komiteene er dermed forvaltningsorganer, noe som blant annet innebærer at REK har myndighet til å godkjenne eller ikke godkjenne at forskningsprosjekter innen medisin blir gjennomført. Arbeidet til REK er videre regulert gjennom den nylig vedtatte Helseforskningsloven. En viktig nyvinning i loven er prinsippet om at medisinsk og helsefaglig forskning bare skal bli behandlet av én instans i godkjenningsprosessen. Dette innebærer at REK er det eneste organ for godkjenning av medisinsk og helsefaglig forskning, slik at man ikke behøver å søke NSD eller Datatilsynet (og andre instanser) i tillegg. Merk at dette bare gjelder prosjekter som faller innenfor loven, det vil si medisinsk og helsefaglig forskning.

Alle prosjekter skal som sagt forelegges REK dersom det inngår forsøk på mennesker og som ikke er av en slik art at det regnes som en del av vanlig etablert behandlingsprosedyre. En må bare søke godkjenning fra REK når prosjektet i sin helhet kan defineres som et helsefaglig eller medisinsk prosjekt. Det er ikke nødvendig å søke REK når enkelte helsespørsmål er inkludert i undersøkelsen, hvis dette prosjektet ellers er å regne som et samfunnsvitenskapelig prosjekt. Det er derved sjelden at forskere ved NR skal søke om å få prosjektet godkjent av REK.

I tillegg har forskningsinstituttene etablert et eget rådgivende forskningsetisk utvalg, FEU. Alle forskningsinstitusjoner er pålagt å ha sin egen forskningsetiske komite. NR er tilsluttet den felles forskningsetiske komiteen til instituttene, FEK. NRs ledelse har ansvar for dialog med FEU og FEK, men dette kan initieres av prosjektleder eller andre med innsikt i prosjektet.

Det er **prosjektleders ansvar** å søke om godkjenning av prosjektet hos REK eller å legge fram prosjektet til vurdering hos NENT eller NESH hvis dette er nødvendig.
NRs adm.dir. har ansvar for dialogen med FEU og FEK og ansatte skal rådføre seg med **adm. dir.** før man initierer en dialog med NESH eller NENT.

12 Særskilte rutiner for behandling av personopplysninger og taushetsbelagte opplysninger

12.1 Dedikert pc

For prosjekter med sikkerhetsnivå *Hemmelig* skal NR ha en eller flere datamaskiner som ikke er knyttet til det eksterne nettverket. Disse maskinene skal brukes til å oppbevare og behandle personidentifiserbare data, navnelister, koblingsnøkler og lignende som kan benyttes for å identifisere ellers avidentifiserte opplysninger.

Bare personell autorisert av behandlingsansvarlig skal ha adgang til å bruke de enkelte maskiner, som skal passordbeskyttes på vanlig måte. Kryptering kan vurderes i tillegg, se kapittel 9.

Hvert prosjekt som bruker de dedikerte maskinene, skal i tillegg benytte særskilt passordbeskyttelse for de filer som er knyttet til prosjektet.

12.2 Bruk av elektronisk post

E-post kan brukes til å oversende data med personopplysninger forutsatt at de sikres på en forsvarlig måte før de legges på sikkerhetsnivå *Internt* og klargjøres som vedlegg. Ta kontakt med dataansvarlig hvis du ønsker å sende eller å motta personopplysninger per e-post. Anonyme data kan sendes som vedlegg med e-post uten **kryptering**.

Taushetsbelagte opplysninger skal i utgangspunktet ikke sendes som vedlegg med e-post uten **kryptering,** med mindre oppdragsgiver ønsker det.

12.3 Utskrift og kopiering

Det skal i så liten grad som mulig tas utskrift og kopier av dokumenter som inneholder personopplysninger eller taushetsbelagte opplysninger. Hvis en likevel trenger utskrift/kopier som arbeidsdokument, skal disse makuleres så snart det ikke er behov for dem lenger. Inntil da skal dokumentene oppbevares innelåst.

12.4 Makulering av dokumenter og elektroniske oppbevaringsmedier

Papirdokumenter som skal destrueres, blir makulert med makuleringsmaskinen. Når personopplysninger som er lagret på elektroniske medier (dvd/cd, minnepenn, diskett, lydbånd, etc.) skal slettes, ta kontakt med IT-drift som er ansvarlig for forsvarlig sletting av slike data.

12.5 Sikkerhet og orden på eget kontor

Dokumenter med personopplysninger skal oppbevares i låsbare skap/skuffer. Oppbevares de i permer, skal permene tilsvarende være innelåst. Sørg for en slik orden på kontoret at ingen personopplysninger blir liggende framme pga. uaktsomhet.

12.6 Adgangskontroll

Adgang til bygningen er sikret med låst inngangsdør og personale i resepsjonen. Systemet forhindrer ikke helt og fullt at personer som ikke er blitt "klarert", kan slippe inn i bygningen og på kontorene. Forskere og andre som er i gang med å arbeide med personopplysninger, og som forlater kontoret en stund, bes om å sørge for at opplysningene ikke kan bli tilgjengelig for uvedkommende, se punkt 9.2. Alle brukere av NRs datasystemer skal dessuten ha skjermsparer med passord som går på ved ti minutters inaktivitet.

12.7 Permisjon og avsluttet arbeidsforhold

Når lederen av et prosjekt eller medarbeidere i et prosjekt går i permisjon eller avslutter sitt arbeidsforhold ved NR, forplikter de seg til å ikke ta med seg personopplysninger fra NR uten at dette er skriftlig avtalt med NRs ledelse. Prosjektledere som tar permisjon eller avslutter sitt arbeidsforhold forplikter seg videre til at prosjektets status er oppdatert både hva som angår prosjektkortet og dokumentasjonen i arkivet. Ansatte ved NR som slutter er videre

forpliktet til å sørge for at alle data fra ikke-avsluttede prosjekter blir gjort tilgjengelig til de som skal fortsette med prosjektet, samtidig som at alle personopplysninger eller taushetsbelagte opplysninger fra forskningsprosjekter blir slettet fra deres eget område på NRs server.

12.8 Bruk av hjemmekontor

NRs nettverk er et administrativt nettverk som er delt inn i flere sikkerhetsnivåer. Personopplysninger der enkeltpersoner ikke er direkte identifiserbare (kategoriene 2-5) skal lagres på sikkerhetsnivå *Fortrolig*. Anonymiserte data kan lagres og jobbes med på sikkerhetsnivå *Intern*. Medarbeidere kan koble seg opp til sikkerhetsnivå *Fortrolig* via egne løsninger for oppkobling og autentisering også utenfra NR, dersom dette ikke er sperret på prosjektnivå. Det betyr at medarbeidere som har hjemmekontor også vil kunne jobbe med personopplysninger hjemme.

Legg også merke til at man gjennom meldeskjema til personvernombudet og ved eventuell forhåndsuttalelse fra Datatilsynet kan få restriksjoner på om personidentifiserbare opplysninger kan bringes ut av huset, og om hvordan disse skal behandles.

13 Prosjektdatabase og arkivering

Det skal føres en prosjektdatabase over **alle prosjekter** ved NR som innebærer behandling av datasett som nevnt i pkt. 3.2 1-6. Det gjelder så vel behandling av personopplysninger i lovens forstand som behandling av anonymiserte datasett innhentet av NR og anonymiserte datasett overtatt fra andre.

Det er **prosjektleders** ansvar å sørge for at informasjonen til enhver tid er oppdatert.

Videre er **prosjektleder** ansvarlig for å sørge for at alle sentrale begivenheter av betydning for oppfyllelsen av våre forpliktelser etter personopplysningslovgivningen er dokumentert i prosjektets mappe i NRs arkiv. Det vil si at korrespondanse med NSD, Datatilsynet, NESH, REK eller liknende instanser blir arkivert i arkivet.

For ytterligere rutiner i forbindelse med oppstart og avslutning av et prosjekt, henviser vi til NRs interne prosjekthåndbok.

14 Drift av prosjekter – sjekkliste

Dersom ikke annet er avtalt, er det **prosjektleder** for det enkelte prosjekt som har ansvar for at følgende rutiner følges. Det forutsettes at prosjektet er godkjent av adm. dir., og at prosjektets formål og (planlagte) datasett er beskrevet i vedtatte prosjektplaner. Dersom prosjektets data omfatter opplysninger om enkeltpersoner, skal du bruke nedforstående sjekkliste for å sikre at NRs rutiner i forhold til gjeldende retningslinjer blir overholdt. Alle prosjekter skal registreres i prosjektstyringsverktøyet Instipro. Arkivet skal inneholde kopi av sentrale dokument vedrørende prosjektet.

NSDs rolle som personvernombud for NR (jf. pkt. 7.1 ovenfor) innebærer at forskningsprosjekter osv. ved NR som medfører behandling av personopplysninger, skal meldes NSD. Ombudet vurderer prosjektopplegg i forhold til personopplysningsloven og helseregisterloven og *gir veiledning og råd*. Spørsmål om mange av forholdene beskrevet under kan derfor rettes dit.

Da ulike typer datasett utløser ulike krav til sikkerhet, lagring, DPIA, forhåndsuttalelser osv. er det viktig å først avklare hvilken av de følgende kategorier ditt datasett kommer inn under. Hovedprinsippet er at datasett med personopplysninger (kategori 2-5) skal lagres i henhold til sikkerhetsnivå *Fortrolig* eller *Strengt fortrolig* avhengig av sensitivitet og krav stilt til oppbevaring, mens anonymiserte data (kategori 6) kan lagres på sikkerhetsnivå *Intern*. Bare svært unntaksvis (f.eks. ved analyse av kriminell virksomhet) skal sikkerhetsnivå *Hemmelig* brukes.

Om de ulike typer datasett vises til pkt. 3.2.

14.1 Datasett med direkte identifiserbare opplysninger (kategori 1)

Dersom datasettet kommer inn under kategori 1, og det er NR eller noen på oppdrag av NR som samler inn data, skal følgende prosedyre følges:

1. Hjemmelsgrunnlag
Vurdere hva som er hjemmelsgrunnlaget for innhentingen av personopplysningene; dvs. skal det innhentes samtykke fra personene (eller deres foresatte), eller er det tungtveiende grunner for å innhente informasjonen uten samtykke? Et eksempel på at man innhenter informasjon uten samtykke kan være at man ønsker informasjon om et stort antall personer fra helseregistre e.l. Da vil en begrunnelse for ikke å innhente samtykke kunne være at det ville være en belastning for mange av de registrerte å bli bedt om samtykke til at registerinformasjonen brukes til forskningsformål, og det ville forringe datakvaliteten betydelig om man bare kunne basere seg på informasjon fra registrerte som hadde gitt samtykke. For noen slike registre vil det også være en forutsetning (fra registereiers side) at man ikke tar kontakt med de registrerte.

2. Melding av prosjekt
Melde prosjektet til Norsk senter for forskningsdata (NSD). Dette må gjøres senest 30 dager før informasjonen innhentes. Meldeskjemaet finnes på NSDs hjemmeside. Her finner du også informasjon om hvordan skjemaet skal fylles ut, og hvordan ord og uttrykk i skjemaet skal forstås. Kopi av meldeskjema legges i arkivet. Prosjektleder skal melde fra til registeransvarlig når datainnsamlingen begynner.

3. Informasjonsskriv og samtykkeerklæring
Dersom informasjonsinnhentingen er basert på informert samtykke[1] fra respondentene, skal det utformes et informasjonsskriv som skal presenteres muntlig eller skriftlig for respondentene. Informasjonsskrivet skal vedlegges meldeskjemaet. Dersom undersøkelsen omfatter mindreårige, skal informasjonen også gis til foreldre eller andre foresatte. Man kan da vurdere om utformingen av informasjonen som gis til de mindreårige bør være enklere enn den som gis til foreldre/foresatte. Informasjonen bør inneholde følgende punkter:

1. Prosjektets tittel.
2. Prosjektets bakgrunn og formål.
3. Hvilke metoder som skal benyttes for å innhente opplysninger, og hvilke opplysninger som innhentes.
4. Hva opplysningene om respondentene konkret skal brukes til.
5. Navn og adresse på institusjon prosjektleder er tilknyttet.
6. Navn og adresse på prosjektleder. Ved studentprosjekt også navn på veileder, evt. navn på andre som behandler personopplysninger på vegne av prosjektleder.
7. Finansiering av prosjektet.
8. At det er frivillig å delta, og at det er mulig å trekke seg på et hvilket som helst tidspunkt.
9. At det å trekke seg ikke medfører erstatnings- eller begrunnelsesplikt, eller andre konsekvenser.
10. Tid for prosjektslutt, om opplysningene skal anonymiseres eller oppbevares videre med personidentifikasjon og begrunnelser for eventuell lagring med personidentifikasjon.
11. At foresatte/verge har rett til å se spørreskjema som skal forelegges en umyndig, før det besvares.
12. Om opplysningene vil bli utlevert til andre og eventuelt til hvem.
13. At forsker er underlagt taushetsplikt, og at data behandles konfidensielt.
14. Om opplysningene som framkommer i publikasjoner fra prosjektet, kan tilbakeføres til enkeltpersoner.
15. Eventuelle andre rettigheter de registrerte har, som for eksempel innsynsrett.
16. At prosjektet er meldt til Personvernombudet for forskning, Norsk senter for forskningsdata AS.

Det skal lages et opplegg for hvordan informert samtykke kan gis fra respondenter og eventuelt foreldre/foresatte. For innhenting av sensitive personopplysninger bør man ha et aktivt samtykke[2]. Samtykket kan gis skriftlig (f.eks. på en ferdig utformet samtykkeerklæring, på e-post eller SMS) eller muntlig. Hva man velger her, må vurderes i forhold til viktigheten av å kunne dokumentere i ettertid at det er gitt samtykke og praktiske hensyn. Av praktiske årsaker har man i en del prosjekter som omfatter mindreårige (f.eks. på videregående skole), basert seg på passivt samtykke fra foreldre/foresatte, dvs. at foreldre/foresatte etter å ha fått informasjon om prosjektet og planlagt informasjonsinnhenting, gir samtykke dersom de ikke melder fra at de ikke ønsker at deres barn skal delta.

Dersom datainnhentingen ikke er basert på informert samtykke, skal det gis en begrunnelse for dette (også i meldeskjemaet til NSD). Dersom data innhentes fra et register, må det søkes registereier om tilgang til personopplysningene. For innhenting av data fra f.eks. helseregistre må det også søkes om dispensasjon fra taushetsplikten.

---

1 Se NSDs meldeskjema for nærmere beskrivelse av hva som menes med informert samtykke.

2 Gitt uttrykkelig samtykke til at personopplysningene brukes i henhold til den informasjonen som er gitt.

Kopi av informasjonsskriv og eventuell samtykkeerklæring legges i arkivet.

4. Vurdering av risiko og oppbevaring av data:
Ettersom det her dreier seg om direkte identifiserbare personopplysninger, er det uhyre viktig at uvedkommende ikke på noen måte kan få tilgang til opplysningene. Slike data skal lagres på sikkerhetsnivå *Strengt fortrolig*, eller ved svært sensitive data *Hemmelig*. Dersom det gjøres unntak skal slike data kun lagres på dedikert kryptert maskinvare som ikke er tilkoblet internett. I tillegg skal brukeren gis opplæring av utstyret, programvare, forslag til backup-rutiner samt få informasjon om fysisk sikring og oppbevaring av utstyret.

Eventuelle skrevne lister med navn og personnummer skal oppbevares i låste skap. Det samme gjelder utskrifter, lydopptak og lignende med personidentifiserbare opplysninger. Lydopptak skal overføres til kryptert elektronisk lagringsmedium snarest mulig, og originale opptaksmedium bør bare lagres når det er spesifikke krav om dette. Man bør vurdere å avidentifisere personopplysningene og lage en koblingsnøkkel (f.eks. liste med løpenummer og personnummer) som lagres hver for seg. I så fall går prosjektets data fra kategori 1 til kategori 3 eller 4.

5. Endringer i prosjektet
Endringer i prosjektets formål, avvik fra oppsatt strategi for datainnsamling, nye personer som skal ha tilgang til data, større forsinkelser etc. skal meldes NSD, som vil gi råd og vurdering av videre forløp. I enkelte tilfeller vil eksempelvis konsesjonen måtte vurderes på nytt. Dersom data i løpet av prosjektperioden avidentifiseres, vil kravene til oppbevaring av data og registrertes rettigheter mht. innsyn, retting og sletting også endres. Kopi av melding om endringer skal legges i arkivet.

6. Sletting eller anonymisering av data
Konsesjonsbelagte prosjekt vil ha en slettedato gitt av Datatilsynet. Prosjektleder er ansvarlig for at sletting eller eventuelt anonymisering utføres i henhold til konsesjonsvilkårene, og at nødvendig melding om dette sendes NSD/Datatilsynet. Kopi av slettemelding skal legges i arkivet. Se for øvrig boksen/oppsummeringen i pkt. 7.2.4.

7. Registrertes rettigheter i forhold til innsyn, retting og sletting
Hvem som helst skal kunne ta kontakt med NR og få grunninformasjon om hvilke behandlinger av personopplysninger vi foretar, se pkt. 7.2.2. Da skal NR oppgi navn og adresse på den behandlingsansvarlige, hvem som eventuelt har det daglige ansvaret, formålet med behandlingen, hvilke typer personopplysninger som behandles, hvor opplysningene er hentet fra, og eventuelt hvem de vil bli utlevert til. Henvendelser kan går til HR-konsulenten eller prosjektleder.

NR skal rette eller slette opplysninger når de er feilaktige, mangelfulle eller unødvendige. Dette skal i utgangspunktet skje på initiativ fra prosjektleder, evt. etter anmodning fra den registrerte. Opplysninger man ikke lenger behøver for å oppfylle formålet med behandlingen, skal slettes.

Alle henvendelser om innsyn, retting og sletting skal dokumenteres i arkivet. Det samme gjelder sletting som foretas på prosjektleders initiativ.

14.2 Datasett med avidentifiserte opplysninger der enkelte undergrupper er små nok til at personer kan identifiseres (kategori 2)

Dersom datasettet kommer inn under kategori 2, og det er NR eller noen på oppdrag fra NR som samler inn data, skal følgende prosedyre følges:

1. Hjemmelsgrunnlag
Vurdere hva som er hjemmelsgrunnlaget for innhentingen av personopplysningene; dvs. skal det innhentes samtykke fra personene (eller deres foresatte), og/eller er det tungtveiende grunner for å innhente informasjonen uten samtykke (se 6.2 og 6.3)? Et eksempel på at man innhenter informasjon uten samtykke kan være at man ønsker informasjon om et stort antall personer fra helseregistre e.l. Da vil en begrunnelse for ikke å innhente samtykke kunne være at det ville være en belastning for mange av de registrerte å bli bedt om samtykke til at registerinformasjonen brukes til forskningsformål, og det ville forringe datakvaliteten betydelig om man bare kunne basere seg på informasjon fra registrerte som hadde gitt samtykke. For noen slike registre vil det også være en forutsetning (fra registereiers side) at man ikke tar kontakt med de registrerte. Hjemmelsgrunnlaget skal lagres i arkivet

2. Melding av prosjekt
Melde prosjektet til Norsk senter for forskningsdata (NSD). Dette må gjøres senest 30 dager før informasjonen innhentes. Meldeskjema finnes på NSDs hjemmeside.

Her finner du også informasjon om hvordan skjemaet skal fylles ut, og hvordan ord og uttrykk i skjemaet skal forstås. Kopi av meldeskjema legges i arkivet. Prosjektleder skal melde fra til registeransvarlig når datainnsamlingen begynner.

3. Informasjonsskriv og samtykkeerklæring
Dersom informasjonsinnhentingen er basert på informert samtykke[3] fra respondentene, skal det utformes et informasjonsskriv som skal presenteres muntlig eller skriftlig for respondentene. Informasjonsskrivet skal vedlegges meldeskjemaet. Dersom undersøkelsen omfatter mindreårige, skal informasjonen også gis til foreldre eller andre foresatte. Man kan da vurdere om utformingen av informasjonen som gis til de mindreårige bør være enklere enn den som gis til foreldre/foresatte. Informasjonen bør inneholde følgende punkter:

1. Prosjektets tittel.

2. Prosjektets bakgrunn og formål.

3. Hvilke metoder som skal benyttes for å innhente opplysninger, og hvilke opplysninger som innhentes.

4. Hva opplysningene om respondentene konkret skal brukes til.

5. Navn og adresse på institusjon prosjektleder er tilknyttet.

6. Navn og adresse på prosjektleder. Ved studentprosjekt også navn på veileder, evt. navn på andre som behandler personopplysninger på vegne av prosjektleder.

7. Finansiering av prosjektet.

8. At det er frivillig å delta, og at det er mulig å trekke seg på et hvilket som helst tidspunkt.

9. At det å trekke seg ikke medfører erstatnings- eller begrunnelsesplikt, eller andre konsekvenser.

10. Tid for prosjektslutt, om opplysningene skal anonymiseres eller oppbevares videre med personidentifikasjon og begrunnelser for eventuell lagring med personidentifikasjon.

---

[3] Se NSDs meldeskjema for nærmere beskrivelse av hva som menes med informert samtykke.

11. At foresatte/verge har rett til å se spørreskjema som skal forelegges en umyndig, før det besvares.

12. Om opplysningene vil bli utlevert til andre og eventuelt til hvem.

13. At forsker er underlagt taushetsplikt, og at data behandles konfidensielt.

14. Om opplysningene som framkommer i publikasjoner fra prosjektet, kan tilbakeføres til enkeltpersoner.

15. Eventuelle andre rettigheter de registrerte har, som for eksempel innsynsrett.

16. At prosjektet er meldt til Personvernombudet for forskning, Norsk senter for forskningsdata AS.

Det skal lages et opplegg for hvordan informert samtykke kan gis fra respondenter og eventuelt foreldre/foresatte. For innhenting av sensitive personopplysninger bør man ha et aktivt samtykke[4]. Samtykket kan gis skriftlig (f.eks. på en ferdig utformet samtykkeerklæring, på e-post eller SMS) eller muntlig. Hva man velger her, må vurderes i forhold til viktigheten av å kunne dokumentere i ettertid at det er gitt samtykke og praktiske hensyn. Av praktiske årsaker har man i en del prosjekter som omfatter mindreårige (f.eks. på videregående skole), basert seg på passivt samtykke fra foreldre/foresatte, dvs. at foreldre/foresatte etter å ha fått informasjon om prosjektet og planlagt informasjonsinnhenting, gir samtykke dersom de ikke melder fra at de ikke ønsker at deres barn skal delta.

Dersom datainnhentingen ikke er basert på informert samtykke, skal det gis en begrunnelse for dette (også i meldeskjemaet til NSD). Dersom data innhentes fra et register, må det søkes registereier om tilgang til personopplysningene. For innhenting av data fra f.eks. helseregistre må det også søkes om dispensasjon fra taushetsplikten.

Kopi av informasjonsskriv og eventuell samtykkeerklæring legges i arkivet.

4. Vurdering av risiko og oppbevaring av data
Kategori 2 datasett skal kun lagres på sikkerhetsnivå *Fortrolig* eller *Strengt fortrolig,* avhengig av sensitivitet og krav stilt til oppbevaring. Ettersom det her dreier seg om potensielt indirekte identifiserbare personopplysninger, er det viktig at uvedkommende ikke på noen måte kan få tilgang til opplysningene. Man bør vurdere om det er nødvendig å ha informasjon på et så detaljert nivå at det kan være mulig å identifisere enkeltpersoner. Det skal i prosjektarkivet komme fram hvor data befinner seg, og hvem som har tilgang til dataene.

5. Endringer i prosjektet
Endringer i prosjektets formål, avvik fra oppsatt strategi for datainnsamling, nye personer som skal ha tilgang til data, større forsinkelser etc. skal meldes NSD, som vil gi råd og vurdering av videre forløp. I enkelte tilfeller vil eksempelvis konsesjonen måtte vurderes på nytt. Kopi av melding om endringer legges i arkivet.

6. Sletting eller anonymisering av data
Konsesjonsbelagte prosjekt vil ha en slettedato gitt av Datatilsynet. Prosjektleder er ansvarlig for at sletting eller eventuelt anonymisering utføres i henhold til konsesjonsvilkårene, og at

[4] Gitt uttrykkelig samtykke til at personopplysningene brukes i henhold til den informasjonen som er gitt.

nødvendig melding om dette sendes NSD/Datatilsynet. Kopi av slettemelding skal legges i arkivet. Se for øvrig boksen/oppsummeringen i pkt. 7.2.4.

7. Registrertes rettigheter i forhold til innsyn, retting og sletting
Hvem som helst skal kunne ta kontakt med NR og få grunninformasjon om hvilke behandlinger av personopplysninger vi foretar, se pkt. 7.2.2. Da skal NR oppgi navn og adresse på den behandlingsansvarlige, hvem som eventuelt har det daglige ansvaret, formålet med behandlingen, hvilke typer personopplysninger som behandles, hvor opplysningene er hentet fra, og eventuelt hvem de vil bli utlevert til.

NR skal rette eller slette opplysninger når de er feilaktige, mangelfulle eller unødvendige. Dette skal i utgangspunktet skje på initiativ fra prosjektleder, evt. etter anmodning fra den registrerte. Opplysninger man ikke lenger behøver for å oppfylle formålet med behandlingen, skal slettes.

Alle henvendelser om innsyn, retting og sletting skal dokumenteres i arkivet. Det samme gjelder sletting som foretas på prosjektleders initiativ.

14.3 Datasett med avidentifiserte opplysninger – NR har koblingsnøkkelen (kategori 3)

Dersom datasettet kommer inn under kategori 3, og det er NR eller noen på oppdrag fra NR som samler inn data, skal følgende prosedyre følges:

1. Hjemmelsgrunnlag
Vurdere hva som er hjemmelsgrunnlaget for innhentingen av personopplysningene; dvs. skal det innhentes samtykke fra personene (eller deres foresatte), og/eller er det tungtveiende grunner for å innhente informasjonen uten samtykke (se 6.2 og 6.3)? Et eksempel på at man innhenter informasjon uten samtykke kan være at man ønsker informasjon om et stort antall personer fra helseregistre e.l. Da vil en begrunnelse for ikke å innhente samtykke kunne være at det ville være en belastning for mange av de registrerte å bli bedt om samtykke til at registerinformasjonen brukes til forskningsformål, og det ville forringe datakvaliteten betydelig om man bare kunne basere seg på informasjon fra registrerte som hadde gitt samtykke. For noen slike registre vil det også være en forutsetning (fra registereiers side) at man ikke tar kontakt med de registrerte. Hjemmelsgrunnlaget skal oppbevares i prosjektarkivet.

2. Melding av prosjekt
Melde prosjektet til Norsk senter for forskningsdata (NSD). Dette må gjøres senest 30 dager før informasjonen innhentes. Meldeskjema finnes på NSDs hjemmeside. Her finner du også informasjon om hvordan skjemaet skal fylles ut, og hvordan ord og uttrykk i skjemaet skal forstås. Kopi av meldeskjema legges i arkivet. Prosjektleder skal melde fra til registeransvarlig når datainnsamlingen begynner.

3. Informasjonsskriv og samtykkeerklæring
Dersom informasjonsinnhentingen er basert på informert samtykke[5] fra respondentene, skal det utformes et informasjonsskriv som skal presenteres muntlig eller skriftlig for respondentene. Informasjonsskrivet skal vedlegges meldeskjemaet. Dersom undersøkelsen omfatter mindreårige, skal informasjonen også gis til foreldre eller andre foresatte. Man kan da vurdere om utformingen av informasjonen som gis til de mindreårige bør være enklere enn den som gis til foreldre/foresatte. Informasjonen bør inneholde følgende punkter:

1. Prosjektets tittel.

[5] Se NSDs meldeskjema for nærmere beskrivelse av hva som menes med informert samtykke.

2. Prosjektets bakgrunn og formål.

3. Hvilke metoder som skal benyttes for å innhente opplysninger, og hvilke opplysninger som innhentes.

4. Hva opplysningene om respondentene konkret skal brukes til.

5. Navn og adresse på institusjon prosjektleder er tilknyttet.

6. Navn og adresse på prosjektleder. Ved studentprosjekt også navn på veileder, evt. navn på andre som behandler personopplysninger på vegne av prosjektleder.

7. Finansiering av prosjektet.

8. At det er frivillig å delta, og at det er mulig å trekke seg på et hvilket som helst tidspunkt.

9. At det å trekke seg ikke medfører erstatnings- eller begrunnelsesplikt, eller andre konsekvenser.

10. Tid for prosjektslutt, om opplysningene skal anonymiseres eller oppbevares videre med personidentifikasjon og begrunnelser for eventuell lagring med personidentifikasjon.

11. At foresatte/verge har rett til å se spørreskjema som skal forelegges en umyndig, før det besvares.

12. Om opplysningene vil bli utlevert til andre og eventuelt til hvem.

13. At forsker er underlagt taushetsplikt, og at data behandles konfidensielt.

14. Om opplysningene som framkommer i publikasjoner fra prosjektet, kan tilbakeføres til enkeltpersoner.

15. Eventuelle andre rettigheter de registrerte har, som for eksempel innsynsrett.

16. At prosjektet er meldt til Personvernombudet for forskning, Norsk senter for forskningsdata AS.

Det skal lages et opplegg for hvordan informert samtykke kan gis fra respondenter og eventuelt foreldre/foresatte. For innhenting av sensitive personopplysninger bør man ha et aktivt samtykke[6]. Samtykket kan gis skriftlig (f.eks. på en ferdig utformet samtykkeerklæring, på e-post eller SMS) eller muntlig. Hva man velger her, må vurderes i forhold til viktigheten av å kunne dokumentere i ettertid at det er gitt samtykke og praktiske hensyn. Av praktiske årsaker har man i en del prosjekter som omfatter mindreårige (f.eks. på videregående skole), basert seg på passivt samtykke fra foreldre/foresatte, dvs. at foreldre/foresatte etter å ha fått informasjon om prosjektet og planlagt informasjonsinnhenting, gir samtykke dersom de ikke melder fra at de ikke ønsker at deres barn skal delta.

---

[6] Gitt uttrykkelig samtykke til at personopplysningene brukes i henhold til den informasjonen som er gitt.

Dersom datainnhentingen ikke er basert på informert samtykke, skal det gis en begrunnelse for dette (også i meldeskjemaet til NSD). Dersom data innhentes fra et register, må det søkes registereier om tilgang til personopplysningene. For innhenting av data fra f.eks. helseregistre må det også søkes om dispensasjon fra taushetsplikten.

Kopi av informasjonsskriv og eventuell samtykkeerklæring legges i arkivet.

4. Vurdering av risiko og oppbevaring av data
Avidentifiserte personopplysninger skal kun lagres på sikkerhetsnivå minst nivå Fortrolig. Ettersom koblingsnøkkelen finnes ved NR, er det viktig å sikre seg mot uautorisert kobling. Koblingsnøkkelen skal derfor oppbevares atskilt fra datasettet for øvrig, enten på dedikert pc eller forsvarlig nedlåst (hvis denne er en utskrift). Det skal i prosjektarkivet komme fram hvor data befinner seg, og hvem som har tilgang til dataene.

5. Endringer i prosjektet
Endringer i prosjektets formål, avvik fra oppsatt strategi for datainnsamling, nye personer som skal ha tilgang til data, større forsinkelser etc. skal meldes NSD, som vil gi råd og vurdering av videre forløp. I enkelte tilfeller vil eksempelvis konsesjonen måtte vurderes på nytt. Dersom koblingsnøkkelen i løpet av prosjektperioden slettes, vil kravene til oppbevaring av data og registrertes rettigheter mht. innsyn, retting og sletting også endres. Kopi av melding om endringer legges i arkivet.

6. Sletting eller anonymisering av data
Konsesjonsbelagte prosjekt vil ha en slettedato gitt av Datatilsynet. Prosjektleder er ansvarlig for at sletting eller eventuelt anonymisering utføres i henhold til konsesjonsvilkårene, og at nødvendig melding om dette sendes NSD/Datatilsynet. Kopi av slettemelding skal legges i prosjektarkivet. Se for øvrig boksen/oppsummeringen i pkt. 7.2.4.

7. Registrertes rettigheter i forhold til innsyn, retting og sletting
Hvem som helst skal kunne ta kontakt med NR og få grunninformasjon om hvilke behandlinger av personopplysninger vi foretar, se pkt 7.2.2. Da skal NR oppgi navn og adresse på den behandlingsansvarlige, hvem som eventuelt har det daglige ansvaret, formålet med behandlingen, hvilke typer personopplysninger som behandles, hvor opplysningene er hentet fra, og eventuelt hvem de vil bli utlevert til.

NR skal rette eller slette opplysninger når de er feilaktige, mangelfulle eller unødvendige. Dette skal i utgangspunktet skje på initiativ fra prosjektleder, evt. etter anmodning fra den registrerte. Opplysninger man ikke lenger behøver for å oppfylle formålet med behandlingen, skal slettes.

Alle henvendelser om innsyn, retting og sletting skal dokumenteres i arkivet. Det samme gjelder sletting som foretas på prosjektleders initiativ.

14.4 Datasett med avidentifiserte opplysninger – koblingsnøkkelen oppbevares midlertidig andre steder enn på NR (kategori 4)

Dersom data kommer inn under kategori 4, og det er NR eller noen på oppdrag fra NR som samler inn data, skal følgende prosedyre følges:

1. Hjemmelsgrunnlag
Vurdere hva som er hjemmelsgrunnlaget for innhentingen av personopplysningene; dvs. skal det innhentes samtykke fra personene (eller deres foresatte), og/eller er det tungtveiende grunner for å innhente informasjonen uten samtykke (se 6.2 og 6.3)? Et eksempel på at man innhenter informasjon uten samtykke kan være at man ønsker informasjon om et stort antall personer fra helseregistre e.l. Da vil en begrunnelse for ikke å innhente samtykke kunne være at det ville være en belastning for mange av de registrerte å bli bedt om samtykke til at

registerinformasjonen brukes til forskningsformål, og det ville forringe datakvaliteten betydelig om man bare kunne basere seg på informasjon fra registrerte som hadde gitt samtykke. For noen slike registre vil det også være en forutsetning (fra registereiers side) at man ikke tar kontakt med de registrerte. Hjemmelsgrunnlaget skal føres i prosjekt-registreringsskjemaet på intranettet.

2. Melding av prosjekt
Melde prosjektet til Norsk senter for forskningsdata (NSD). Dette må gjøres senest 30 dager før informasjonen innhentes. Meldeskjema finnes på NSDs hjemmeside.

Her finner du også informasjon om hvordan skjemaet skal fylles ut, og hvordan ord og uttrykk i skjemaet skal forstås. Kopi av meldeskjema legges i arkivet. Prosjektleder skal melde fra til registeransvarlig når datainnsamlingen begynner.

3. Informasjonsskriv og samtykkeerklæring
Dersom informasjonsinnhentingen er basert på informert samtykke fra respondentene, skal det utformes et informasjonsskriv som skal presenteres muntlig eller skriftlig for respon-dentene. Informasjonsskrivet skal vedlegges meldeskjemaet. Dersom undersøkelsen omfatter mindreårige, skal informasjonen også gis til foreldre eller andre foresatte. Man kan da vurdere om utformingen av informasjonen som gis til de mindreårige bør være enklere enn den som gis til foreldre/foresatte. Informasjonen bør inneholde følgende punkter:

1. Prosjektets tittel.

2. Prosjektets bakgrunn og formål.

3. Hvilke metoder som skal benyttes for å innhente opplysninger, og hvilke opplysninger som innhentes.

4. Hva opplysningene om respondentene konkret skal brukes til.

5. Navn og adresse på institusjon prosjektleder er tilknyttet.

6. Navn og adresse på prosjektleder. Ved studentprosjekt også navn på veileder, evt. navn på andre som behandler personopplysninger på vegne av prosjektleder.

7. Finansiering av prosjektet.

8. At det er frivillig å delta, og at det er mulig å trekke seg på et hvilket som helst tidspunkt.

9. At det å trekke seg ikke medfører erstatnings- eller begrunnelsesplikt, eller andre konsekvenser.

10. Tid for prosjektslutt, om opplysningene skal anonymiseres eller oppbevares videre med personidentifikasjon og begrunnelser for eventuell lagring med personidentifikasjon.

11. At foresatte/verge har rett til å se spørreskjema som skal forelegges en umyndig, før det besvares.

12. Om opplysningene vil bli utlevert til andre og eventuelt til hvem.

13. At forsker er underlagt taushetsplikt, og at data behandles konfidensielt.

14. Om opplysningene som framkommer i publikasjoner fra prosjektet, kan tilbakeføres til enkeltpersoner.

15. Eventuelle andre rettigheter de registrerte har, som for eksempel innsynsrett.

16. At prosjektet er meldt til Personvernombudet for forskning, Norsk senter for forskningsdata AS.

Det skal lages et opplegg for hvordan informert samtykke kan gis fra respondenter og eventuelt foreldre/foresatte. For innhenting av sensitive personopplysninger bør man ha et aktivt samtykke[7]. Samtykket kan gis skriftlig (f.eks. på en ferdig utformet samtykkeerklæring, på e-post eller SMS) eller muntlig. Hva man velger her, må vurderes i forhold til viktigheten av å kunne dokumentere i ettertid at det er gitt samtykke og praktiske hensyn. Av praktiske årsaker har man i en del prosjekter som omfatter mindreårige (f.eks. på videregående skole), basert seg på passivt samtykke fra foreldre/foresatte, dvs. at foreldre/foresatte etter å ha fått informasjon om prosjektet og planlagt informasjonsinnhenting, gir samtykke dersom de ikke melder fra at de ikke ønsker at deres barn skal delta.

Dersom datainnhentingen ikke er basert på informert samtykke, skal det gis en begrunnelse for dette (også i meldeskjemaet til NSD). Dersom data innhentes fra et register, må det søkes registereier om tilgang til personopplysningene. For innhenting av data fra f eks helseregistre må det også søkes om dispensasjon fra taushetsplikten.

Kopi av informasjonsskriv og eventuell samtykkeerklæring legges i arkivet.

4. Vurdering av risiko og oppbevaring av data
Det dreier seg her om avidentifiserte opplysninger – der koblingsnøkkelen oppbevares midlertidig hos for eksempel NSD. Det er viktig at uvedkommende ikke kan få tilgang til personopplysningene. Risikoen for dette anses imidlertid som ganske liten. I utgangspunktet bør likevel denne type datasett lagres på minst sikkerhetsnivå *Fortrolig*, avhengig av om NR er pålagt strengere oppbevaring eller ikke. Hvis dataene er å regne som lite sensitive kan en likevel i enkelte tilfeller vurdere å lagre dem på sikkerhetsnivå *Intern*. Det skal i prosjektarkivet komme fram hvor data befinner seg, og hvem som har tilgang til dataene.

5. Endringer i prosjektet
Endringer i prosjektets formål, avvik fra oppsatt strategi for datainnsamling, nye personer som skal ha tilgang til data, større forsinkelser etc. skal meldes NSD, som vil gi råd og vurdering av videre forløp. I enkelte tilfeller vil eksempelvis konsesjonen måtte vurderes på nytt. Kopi av melding om endringer legges i arkivet, og opplysninger om utfall føres i prosjektets arkivmappe.

6. Sletting eller anonymisering av data
Konsesjonsbelagte prosjekt vil ha en slettedato gitt av Datatilsynet. Prosjektleder er ansvarlig for at sletting eller eventuelt anonymisering utføres i henhold til konsesjonsvilkårene, og at nødvendig melding om dette sendes NSD/Datatilsynet. Kopi av slettemelding skal legges i arkivet. Se for øvrig boksen/oppsummeringen i pkt. 7.2.4.

7. Registrertes rettigheter i forhold til innsyn, retting og sletting
Ettersom NR ikke har koblingsnøkkelen og derfor ikke kan identifisere enkeltpersoner, kan registrerte ikke få innsyn i opplysninger om seg selv og følgelig heller ikke få endret eller slettet opplysninger om seg selv. Men under enhver omstendighet gjelder:

---

[7] Gitt uttrykkelig samtykke til at personopplysningene brukes i henhold til den informasjonen som er gitt.

Hvem som helst skal kunne ta kontakt med NR og få grunninformasjon om hvilke behandlinger av personopplysninger vi foretar, se pkt. 7.2.2. Da skal NR oppgi navn og adresse på den behandlingsansvarlige, hvem som eventuelt har det daglige ansvaret, formålet med behandlingen, hvilke typer personopplysninger som behandles, hvor opplysningene er hentet fra, og eventuelt hvem de vil bli utlevert til.

NR skal rette eller slette opplysninger når de er feilaktige, mangelfulle eller unødvendige. Dette skal i utgangspunktet skje på initiativ fra prosjektleder, evt. etter anmodning fra den registrerte. Opplysninger man ikke lenger behøver for å oppfylle formålet med behandlingen, skal slettes.

Alle henvendelser om innsyn, retting og sletting skal dokumenteres i arkivet. Det samme gjelder sletting som foretas på prosjektleders initiativ.

14.5 Datasett med avidentifiserte opplysninger – NR uten tilgang til koblingsnøkkelen (kategori 5), innsamlet på oppdrag fra NR

Dersom datasettet kommer inn under kategori 5, og det er noen på oppdrag fra NR som samler inn data, skal følgende prosedyre følges:

1. Hjemmelsgrunnlag
Vurdere hva som er hjemmelsgrunnlaget for innhentingen av personopplysningene; dvs. skal det innhentes samtykke fra personene (eller deres foresatte), og/eller er det tungtveiende grunner for å innhente informasjonen uten samtykke (se 6.2 og 6.3)? Et eksempel på at man innhenter informasjon uten samtykke kan være at man ønsker informasjon om et stort antall personer fra helseregistre e.l. Da vil en begrunnelse for ikke å innhente samtykke kunne være at det ville være en belastning for mange av de registrerte å bli bedt om samtykke til at registerinformasjonen brukes til forskningsformål, og det ville forringe datakvaliteten betydelig om man bare kunne basere seg på informasjon fra registrerte som hadde gitt samtykke. For noen slike registre vil det også være en forutsetning (fra registereiers side) at man ikke tar kontakt med de registrerte. Hjemmelsgrunnlaget skal føres i prosjektregistreringsskjemaet på intranettet.

2. Melding av prosjekt
Melde prosjektet til Norsk senter for forskningsdata (NSD). Dette må gjøres senest 30 dager før informasjonen innhentes. Meldeskjema finnes på NSDs hjemmeside. Her finner du også informasjon om hvordan skjemaet skal fylles ut, og hvordan ord og uttrykk i skjemaet skal forstås. Kopi av meldeskjema legges i arkivet. Prosjektleder skal melde fra til registeransvarlig når datainnsamlingen begynner.

3. Informasjonsskriv og samtykkeerklæring
Dersom informasjonsinnhentingen er basert på informert samtykke[8] fra respondentene, skal det utformes et informasjonsskriv som skal presenteres muntlig eller skriftlig for respondentene. Informasjonsskrivet skal vedlegges meldeskjemaet. Dersom undersøkelsen omfatter mindreårige, skal informasjonen også gis til foreldre eller andre foresatte. Man kan da vurdere om utformingen av informasjonen som gis til de mindreårige bør være enklere enn den som gis til foreldre/foresatte. Informasjonen bør inneholde følgende punkter:

1. Prosjektets tittel.

[8] Se NSDs meldeskjema for nærmere beskrivelse av hva som menes med informert samtykke.

2. Prosjektets bakgrunn og formål.

3. Hvilke metoder som skal benyttes for å innhente opplysninger, og hvilke opplysninger som innhentes.

4. Hva opplysningene om respondentene konkret skal brukes til.

5. Navn og adresse på institusjon prosjektleder er tilknyttet.

6. Navn og adresse på prosjektleder. Ved studentprosjekt også navn på veileder, evt. navn på andre som behandler personopplysninger på vegne av prosjektleder.

7. Finansiering av prosjektet.

8. At det er frivillig å delta, og at det er mulig å trekke seg på et hvilket som helst tidspunkt.

9. At det å trekke seg ikke medfører erstatnings- eller begrunnelsesplikt, eller andre konsekvenser.

10. Tid for prosjektslutt, om opplysningene skal anonymiseres eller oppbevares videre med personidentifikasjon og begrunnelser for eventuell lagring med personidentifikasjon.

11. At foresatte/verge har rett til å se spørreskjema som skal forelegges en umyndig, før det besvares.

12. Om opplysningene vil bli utlevert til andre og eventuelt til hvem.

13. At forsker er underlagt taushetsplikt, og at data behandles konfidensielt.

14. Om opplysningene som framkommer i publikasjoner fra prosjektet, kan tilbakeføres til enkeltpersoner.

15. Eventuelle andre rettigheter de registrerte har, som for eksempel innsynsrett.

16. At prosjektet er meldt til Personvernombudet for forskning, Norsk senter for forskningsdata AS.

Det skal lages et opplegg for hvordan informert samtykke kan gis fra respondenter og eventuelt foreldre/foresatte. For innhenting av sensitive personopplysninger bør man ha et aktivt samtykke[9]. Samtykket kan gis skriftlig (f.eks. på en ferdig utformet samtykkeerklæring, på e-post eller SMS) eller muntlig. Hva man velger her, må vurderes i forhold til viktigheten av å kunne dokumentere i ettertid at det er gitt samtykke og praktiske hensyn. Av praktiske årsaker har man i en del prosjekter som omfatter mindreårige (f.eks. på videregående skole), basert seg på passivt samtykke fra foreldre/foresatte, dvs. at foreldre/foresatte etter å ha fått informasjon om prosjektet og planlagt informasjonsinnhenting, gir samtykke dersom de ikke melder fra at de ikke ønsker at deres barn skal delta.

Dersom datainnhentingen ikke er basert på informert samtykke, skal det gis en begrunnelse for dette (også i meldeskjemaet til NSD). Dersom data innhentes fra et register, må det

[9] Gitt uttrykkelig samtykke til at personopplysningene brukes i henhold til den informasjonen som er gitt.

søkes registereier om tilgang til personopplysningene. For innhenting av data fra f.eks. helseregistre må det også søkes om dispensasjon fra taushetsplikten.

Kopi av informasjonsskriv og eventuell samtykkeerklæring legges i arkivet.

4. Vurdering av risiko og oppbevaring av data
Det dreier seg her om avidentifiserte opplysninger – der koblingsnøkkelen befinner seg hos ekstern databehandler. Risikoen for at uvedkommende skal få tilgang til personopplysningene, anses som liten. I utgangspunktet bør likevel denne type datasett lagres på minst sikkerhetsnivå *Fortrolig*, avhengig av om NR er pålagt strengere oppbevaring eller ikke. Hvis dataene er å regne som lite sensitive kan en likevel i enkelte tilfeller vurdere å lagre dem på sikkerhetsnivå *Intern*. Det skal i prosjektarkivet komme fram hvor data befinner seg, og hvem som har tilgang til dataene.

5. Endringer i prosjektet
Endringer i prosjektets formål, avvik fra oppsatt strategi for datainnsamling, nye personer som skal ha tilgang til data, større forsinkelser etc. skal meldes NSD, som vil gi råd og vurdering av videre forløp. I enkelte tilfeller vil eksempelvis konsesjonen måtte vurderes på nytt. Kopi av melding om endringer legges i arkivet.

6. Sletting eller anonymisering av data
Konsesjonsbelagte prosjekt vil ha en slettedato gitt av Datatilsynet. Prosjektleder er ansvarlig for at sletting eller eventuelt anonymisering utføres i henhold til konsesjonsvilkårene og at nødvendig melding om dette sendes NSD/Datatilsynet. Kopi av slettemelding skal legges i arkivet. Se for øvrig boksen/oppsummeringen i pkt. 7.2.4.

7. Registrertes rettigheter i forhold til innsyn, retting og sletting
Ettersom et ikke er mulig å identifisere enkeltpersoner, kan registrerte ikke få innsyn i opplysninger om seg selv og følgelig heller ikke få endret eller slette opplysninger om seg selv. Men under enhver omstendighet gjelder:

Hvem som helst skal kunne ta kontakt med NR og få grunninformasjon om hvilke behandlinger av personopplysninger vi foretar, se pkt. 7.2.2. Da skal NR oppgi navn og adresse på den behandlingsansvarlige, hvem som eventuelt har det daglige ansvaret, formålet med behandlingen, hvilke typer personopplysninger som behandles, hvor opplysningene er hentet fra, og eventuelt hvem de vil bli utlevert til.

NR skal rette eller slette opplysninger når de er feilaktige, mangelfulle eller unødvendige. Dette skal i utgangspunktet skje på initiativ fra prosjektleder, evt. etter anmodning fra den registrerte. Opplysninger man ikke lenger behøver for å oppfylle formålet med behandlingen, skal slettes.

Alle henvendelser om innsyn, retting og sletting skal dokumenteres i arkivet. Det samme gjelder sletting som foretas på prosjektleders initiativ.

14.6 Datasett med avidentifiserte opplysninger – NR uten tilgang til koblingsnøkkelen (kategori 5), sekundæranalyser

Dersom datasettet kommer inn under kategori 5, og det er samlet inn av andre og gjort tilgjengelig for NR for sekundæranalyser, skal følgende prosedyrer følges:

1. Melding av prosjekt
Melde prosjektet til Norsk senter for forskningsdata (NSD). Dette må gjøres senest 30 dager før informasjonen innhentes. Meldeskjema finnes på NSDs hjemmeside. Her finner du også

informasjon om hvordan skjemaet skal fylles ut, og hvordan ord og uttrykk i skjemaet skal forstås. Kopi av meldeskjema legges i arkivet.

2. Vurdering av risiko og oppbevaring av data
Det dreier seg her om avidentifiserte opplysninger der koblingsnøkkelen befinner seg hos den instans som har samlet inn dataene. Risikoen anses som liten. I utgangspunktet bør likevel denne type datasett lagres på minst sikkerhetsnivå *Fortrolig*, avhengig av om NR er pålagt strengere oppbevaring eller ikke. Hvis dataene er å regne som lite sensitive kan en likevel i enkelte tilfeller vurdere å lagre dem på sikkerhetsnivå *Intern*. Det skal i prosjektarkivet komme fram hvor data befinner seg, og hvem som har tilgang til dataene.

3. Endringer i prosjektet
Endringer i prosjektets formål, avvik fra oppsatt strategi for datainnsamling, nye personer som skal ha tilgang til data, større forsinkelser etc. skal meldes NSD. Kopi av evt. melding om endringer samt opplysninger om arkiveres i arkivet.

4. Sletting av data
Slike data medfører ikke nødvendigvis krav om slettedato - avhengig av om slettedato er avtalt med datasettets eier. Dersom slettedato er avtalt med eieren, instituttledelsen ved NR og/eller NSD, skal kopi av slettemelding legges i arkivet.

5. Registrertes rettigheter i forhold til innsyn, retting og sletting
Ettersom et ikke er mulig å identifisere enkeltpersoner, kan registrerte ikke få innsyn i opplysninger om seg selv og følgelig heller ikke få endret eller slettet opplysninger om seg selv. Men under enhver omstendighet gjelder:

Hvem som helst skal kunne ta kontakt med NR og få grunninformasjon om hvilke behandlinger av personopplysninger vi foretar, se pkt. 7.2.2. Da skal NR oppgi navn og adresse på den behandlingsansvarlige, hvem som eventuelt har det daglige ansvaret, formålet med behandlingen, hvilke typer personopplysninger som behandles, hvor opplysningene er hentet fra, og eventuelt hvem de vil bli utlevert til.

NR skal rette eller slette opplysninger når de er feilaktige, mangelfulle eller unødvendige. Dette skal i utgangspunktet skje på initiativ fra prosjektleder, evt. etter anmodning fra den registrerte. Opplysninger man ikke lenger behøver for å oppfylle formålet med behandlingen skal slettes.

Alle henvendelser om innsyn, retting og sletting skal dokumenteres i arkivet. Det samme gjelder sletting som foretas på prosjektleders initiativ.

14.7 Datasett med anonyme opplysninger (kategori 6)

Dersom datasettet kommer inn under kategori 6:
Denne kategorien omfatter anonymiserte datasett. Det dreier seg om datasett der det ikke finnes navnelister/personnummerlister eller koblingsnøkler som kan knytte personer til de enkelte opplysninger. Det er en forutsetning at vedkommende heller ikke kan identifiseres indirekte, jf. kategori 2.

Dette omfatter datasett

a. innhentet av NR og hvis lister/nøkler er slettet
b. overtatt fra andre etter at lister/nøkler er slettet hos den som har hatt slike lister/nøkler
c. innhentet av NR på en slik måte at man ikke på noe tidspunkt kan vite hvem som har svart hva.

Disse datasettene faller utenfor personopplysningsloven. Følgende rutiner skal likevel følges:

1. Ad a:
Prosjektet er (forutsetningsvis) registrert med et prosjektkort hos regnskap. Der skal det fremgå når og av hvem lister/nøkler er slettet. Etter dette tidspunkt er datasettet å regnes som anonymisert.

Dreier det seg om eldre prosjekter der anonymisering er foretatt før opprettelsen av prosjektregisteret, skal datasettet likevel føres som eget prosjekt. Det skal fremgå hvilket formål prosjektet har, og hvilke data som er innhentet. Det skal også fremgå når og av hvem datasettet ble anonymisert.

2. Ad b:
Datasettet skal føres som eget datasett. Det skal fremgå hvilket formål prosjektet har, og hvilke data som er innhentet. (Man kan godt bruke Meldepliktskjemaet). Det skal også fremgå at prosjektleder har forsikret seg om at datasettet var anonymisert da det ble overlatt til NR.

3. Ad c
Datasettet skal føres som eget prosjekt. I disse tilfellene bør man ta kontakt med NSD for å avklare om prosjektet utløser meldeplikt eller ikke. Dersom NSD mener at prosjektet utløser meldeplikt eller er i tvil om dette, skal det meldes til NSD. I så fall gjelder rutinene i pkt. 12.3.

Meldeskjemaet skal under enhver omstendighet fylles ut så langt det passer. Vurderingen av hvorfor datasettet regnes som anonymisert, skal fremgå uttrykkelig.

Også ved innhenting av anonymiserte data bør man så langt det er praktisk følge de rutiner for informasjon og samtykke som er skissert under pkt 12.3.

15 Kvalitetssikring

15.1 Periodisk kontroll med prosjekt

Prosjektleder er ansvarlig for at opplysninger om prosjektet er løpende oppdatert. Prosjektleder har videre ansvar for at all nødvendig dokumentasjon om prosjektet i forhold til datasikkerhet og personvern er arkivert i prosjektets mappe i arkivet.

15.2 Periodisk kontroll av datasikkerhet

Dataansvarlig skal løpende sørge for oppdatering av sikkerhetsprogrammene ved NR, herunder at de oppdateres på de enkelte maskiner. I forbindelse med utarbeidelsen av NRs årsmelding skal det rapporteres om hvilke tiltak som er iverksatt i løpet av året. Dette skjer i form av rapporten «Risikovurdering teknisk it ved Norsk Regnesentral».

15.3 Avviksbehandling i prosjekt

Prosjektleder skal dokumentere all uautorisert bruk av datasett i arkivet. Slik bruk skal også rapporteres til direktøren, som vurderer hvilke tiltak som skal iverksettes.

15.4 Avviksbehandling mht. datasikkerhet

Forsøk på inntrengning i datasystemet skal dokumenteres av **dataansvarlig**. Det skal også rapporteres til direktøren, som vurderer hvilke tiltak som skal iverksettes.

Dersom det avdekkes avvik i prosjekter der NR er involvert, skal adm. dir. involveres raskest mulig. Databehandler skal rapportere avvik til Datatilsynet så snart som mulig.

16 Ekstern datastøtte eller databehandler

Ved bruk av **ekstern datastøtte** (f.eks. drift av NRs dataanlegg) skal **behandlingsansvarlig** forvisse seg om at vedkommende har tilfredsstillende sikkerhetsrutiner. Om nødvendig skal det stilles vilkår i kontrakten knyttet til dette. Eksterne skal ikke ta data ut av huset. Ekstern datastøtte skal underskrive taushetserklæring.

Ved bruk av **ekstern datainnsamler** skal **prosjektleder** forvisse seg om at vedkommende har tilfredsstillende sikkerhetsrutiner. Om nødvendig skal det stilles vilkår i kontrakten knyttet til dette.