UiO : Det juridiske fakultet

Pasientens rettigheter og friheter ved behandling i helseregistre i lys av personvernforordningen

Kandidatnummer: 608

Leveringsfrist: 25. november 2018

Antall ord: 17 951

Innholdsfortegnelse

1 INNLEDNING

1.1 Tema

Temaet for oppgaven er behandling av personopplysninger i helseregistre. Personopplysninger samles inn i forbindelse med helsehjelp og blir registrert i pasientjournaler. Opplysningene sendes til helseregistre hvor de gjenbrukes utover det opprinnelige formålet. Pasienten har flere rettigheter og friheter i denne prosessen. Den mest sentrale rettigheten for oppgavens tema er personvern.

Det er avgjørende å ivareta pasientens rett til personvern når helseopplysninger gjenbrukes. Opplysningene kan gjenbrukes til helseanalyse eller forskning for å fremme helse, forebygge skade og forbedre helse- og omsorgstjenester vedtatt i konkrete helseregistres formål. For at en pasient skal dele frivillig sine personopplysninger, må behandlingen utføres på en etisk forsvarlig måte i tråd med gjeldende prinsipper om personvern.

Etter flere tillitsbrudd den siste tiden ved behandling av personopplysninger har det oppstått et behov for å oppdatere personvernregelverk. I 2017 fikk 110 IT-konsulenter tilgang til sensitive helseopplysninger om 2,8 millioner nordmenn fra Helse Sør-Øst.[1] IT-konsulentene fikk utvidede rettigheter til Helse Sør-Øst sitt datasystem og har hatt mulighet til å kopiere pasientjournaler uten å legge igjen spor. Flere tillitsbrudd over tid kan føre til at pasienter blir motvillige til å la seg registrere.

Temaets aktualitet tydeliggjøres ved at EU vedtok nylig en personvernforordning, kalt General Data Protection Regulation[2] (GDPR eller personvernforordning). Norge inkorporerte personvernforordningen gjennom den nye personopplysningsloven[3] (popplyl.) § 1 den 20. juli 2018. Det nye regelverket styrker den registrertes rettigheter og friheter med effektiv databeskyttelse ved behandling av personopplysninger, også i helsetjenesten.

Digitalisering og tilgjengelighet av informasjon påvirker dagens samfunn i stort omfang og økende intensitet. Opplysninger relatert til pasienter kan digitalt sammenstilles enklere med andre opplysninger, både i mengder og hastighet. I løpet av en persons liv innsamles viktige opplysninger om symptomer, medisinsk sykdomshistorie, tester og terapi i pasientjournaler. Sammen med personopplysninger utgjør dette helseopplysninger. Effektiv behandling kan være til fordel for pasienten. Dette må imidlertid vurderes opp mot risiko for svekkelse av personvernet. Oppgavens bidrag til temaet er å kartlegge det rettslige rammeverket knyttet til enkelte helseregistre ved behandling av personopplysninger og reglenes egnethet for å ivareta den registrertes rett til personvern.

[1] Remen (2017).

[2] For 679/2016/EU.

[3] Lov 15. juni 2018 nr. 38 behandling av personopplysninger.

1.2 Problemstilling og perspektiv

For å ta stilling til temaet om den registrertes rettigheter og friheter ved behandling av personopplysninger i helseregistre, reiser oppgaven følgende problemstillinger:

I. Hvordan kan behandling av personopplysninger i helseregistre føre til risiko for innskrenkning i den registrertes rettigheter og friheter.

II. I hvilken grad kan den registrertes rett til personvern ivaretas ved behandling av personopplysninger i helseregistre.

III. Hvordan oppfylles grunnprinsippene etter GDPR art. 5 ved behandling av personopplysninger i helseregistre.

Problemstillingene reiser spørsmål om den registrertes rolle i behandlingsprosessen. Deretter vurderes problemstillingene ut fra en normativ analyse av to utvalgte helseregistre. I oppgaven brukes et rettsdogmatisk perspektiv. Det innebærer at rettskildene anvendes for å kartlegge gjeldende rett. Målet med oppgaven er å gi leseren en dypere forståelse av enkelte begrep i personvernforordningen og kravene som stilles for behandlingsprosessen. Vurderinger av reglenes egnethet til å ivareta den registrertes rett til personvern foretas gradvis for de tre problemstillingene.

1.3 Avgrensning og presisering

Oppgaven undersøker sekundærbruk av helsedata og må avgrenses mot primærbruk av helseopplysninger. Primærbruk innebærer hovedsakelig helsebehandling mellom helsepersonell og pasient. I denne oppgaven vurderes sekundærbruk som består av gjenbruk og annen behandling av personopplysninger i helseregistre. Dette omfatter innsamling av helseopplysninger til statistikk, helseanalyser, forskning, kvalitetsforbedring, planlegging, styring og beredskap, jf. GDPR art. 4 nr. 2, se hregl. § 2 bokstav b. Av hensyn til oppgavens omfang kommer forholdet mellom helsepersonell og pasient på siden av problemstillingen.

Oppgaven begrenses til pasientens rettigheter og avgrenses mot helsesystemets plikter som sådan. Personvernutfordringer åpner for flere rettslige problemstillinger utover rammen av oppgaven.

Det avgrenses mot regulering som følger av den nye personopplysningsloven og personopplysningsforskriften[4] utover popplyl. § 1 og § 20. Oppgaven tar utgangspunkt i personvernforordningens implikasjoner for helseretten og ikke personvernretten generelt. Begrepene helseopplysninger og personopplysninger brukes synonymt etter hvilket begrep som er mest anvendelig for vurderingen.

[4] Forskrift 16. juni 2018 nr. 876 om behandling av personopplysninger.

1.4 Rettskildebildet

I det følgende redegjøres det for rettskilder som brukes i oppgaven og hvilke rettskildeutfordringer som må tas hensyn til.

Utgangspunktet for personvern i helseretten er Grunnloven[5] (Grl.) § 102 og menneskerettigheter etter EMK[6] art. 8. Grunnrettighetene er vesentlige for forståelsen av bakgrunnen for oppdatering av regelverket til personvern. Oppgaven bygger videre på formell lov og forskrift. For å tolke rettsregelen i norsk lov, må det ses hen til personvernforordningen og dens kilder ettersom personopplysningsloven og spesiallovgivning i helserett bygger på forordningen. Visse utfordringer kan oppstå når det skal avgjøres hvilken lov som skal legges til grunn i en konkret vurdering. Dette danner grunnlag for at tolkningsstilen blir noe annerledes enn den tradisjonelle norske rettskildelæren.[7] Tolkningsprinsipper utviklet i EØS-rett anvendes som tolkningsmomenter i oppgaven.

Den relevante loven er helseregisterloven[8] (hregl.) og to utvalgte forskrifter, meldingssystem for smittsomme sykdommer-forskriften[9] (MSIS-forskriften) og hjerte- og karregisterloven-forskriften[10]. Ordlyden i de aktuelle bestemmelsene utfylles med lovens forarbeider som tolkningsfaktorer. Disse anses for å ha tung rettskildemessig vekt. Personvernforordningens ordlyd tillegges særlig vekt ettersom den trådte i kraft nylig som gjør den til den mest sentrale rettskilden for oppgavens problemstillinger. Den tidligere personopplysningsloven fra 2000 og dens forarbeider er relevant for forståelse av den registrertes rettsstilling ved tolkning av personvernforordningen.

Istedenfor å gjennomgå EØS-rettslig metode, nevnes enkelte metodiske utfordringer som har oppstått i skrivearbeidet. Hovedutfordringen har vært mangel på kildemateriale. Personvernforordningen ble vedtatt og trådt i kraft i EU fra april 2016, men ble først innlemmet i EØS-avtalen 20. juli 2018. Personvernforordningen ble inkorporert til norsk rett ved en henvisningsbestemmelse, se popplyl. § 1. EUs tidligere personverndirektiv[11] er opphevet, se popplyl. § 1 Dette tydeliggjøres i

[5] Lov 17. mai 1814 Kongeriket Norge Grunnlov.

[6] Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter, Roma 4. november 1950.

[7] Boe (2012) s. 384.

[8] Lov 20. juni 2014 nr. 43 helseregistre og behandling av helseopplysninger.

[9] Forskrift 20. juni 2003 nr. 740 om Meldingssystem for smittsomme sykdommer.

[10] Forskrift 16. desember 2011 nr. 1250 om innsamling og behandling av helseopplysninger i Nasjonalt Register over hjerte- og karlidelser.

[11] Dir 95/46/EF.

personvernforordningens tittel. Flere mål og prinsipper er likevel videreført til personvernforordningen.[12]
Hovedkilden for oppgaven har vært den engelske versjonen av personvernforordningen supplert med norsk oversettelse fra EØS-komiteen.[13] For å utfylle personvernforordningens ordlyd, brukes fortalen som veileder for å fastslå innhold og rekkevidden av bestemmelsene. Den nye reguleringen ble vedtatt som forordning framfor direktiv for å harmonisere personvernregelverket[14] som har blitt gjennomført ulikt i EUs medlemsland og EØS.[15] Siden det foreløpig er begrenset med kildematerialer som kan anvendes som tolkningsfaktorer, blir fortalen oppgavens viktigste tolkningsfaktor for å kartlegge risikoen for at den registrertes rettigheter og friheter krenkes.

Det er nylig avsagt enkelte avgjørelser om tolkningen av personvernforordningen i europeiske datatilsyn og domstoler. Avgjørelsene brukes som støttemomenter, men får ikke stor vekt i rettskildebildet siden de ble avsagt sent i oppgavens skriveprosess. Noen eldre avgjørelser fra EU-domstolen vurdert etter EUs tidligere personverndirektiv har overføringsverdi. Dette gjelder avgjørelser som behandler bestemmelser overført til personvernforordningen. Avgjørelser fra EU-domstolen har vært nyttig for forståelsen av personsopplysningsbegrepet og styrker den registrerte som individ og dens rettigheter.

Av avgjørelser fra Høyesterett er det få som knytter seg til oppgavens problemstilling om personvern på helseområdet. Likevel har høyesterettsavgjørelsen inntatt i Rt. 2013 s. 143 hatt betydning for oppgaven. Avgjørelser fra forvaltningspraksis avsagt i Personvernnemnda er relevant i den grad de kan belyse personopplysningsbegrepet ved behandling i helseregistre. Flere teoretikere, deriblant Skoghøy anerkjenner forvaltningspraksis som en gyldig rettskildefaktor.[16] Vekten av forvaltningspraksis beror på de øvrige rettskildefaktorene som foreligger.[17] Datatilsynets uttalelser som tilsynsmyndighet, se GDPR art. 4 nr. 21, jf. art. 51, se popplyl. § 20, står sentralt for tolkingen av helselovgivningen og særlig i analysen om forskriftene oppfyller vilkårene etter personvernforordningen.

Det finnes lite juridisk litteratur som knytter helsetema til personvernforordningen. Oppgaven behandler et tema som ikke har god dekning i litteraturen, ettersom temaet ligger i grensen mellom helserett og personvernrett. Derfor har jeg vært nødt til å trekke slutninger fra rettsområdene som er relevant for oppgavens problemstilling. Dette har gitt mulighet til å reise problemstillinger om de lege lata og de lege ferenda om pasienters rett til personvern.

[12] GDPR fortalepunkt 9.
[13] 2018/EØS/46/01 art. 3.
[14] GDPR fortalepunkt 10.
[15] GDPR fortalepunkter 9 og 10.
[16] Skoghøy (1994) s. 850, se for eksempel Eckhoff (2001) s. 233-241, Boe (2012) s. 264.
[17] Boe (2012) s. 260.

Formåls- og hensiktsmessighetsbetraktninger er særdeles relevante som tolkningsmomenter i vurderingen av personvernforordningens innhold og pasienters rett til personvern. De aktuelle personvernrettslige interesser og prinsipper kom tidligere til uttrykk i personopplysningsloven 2000 og nå i personvernforordningen. Disse prinsippene anvendes som retningslinjer av avveining av den personvernsrettslige lovgivningen på helseområdet.

1.5 Begrepsforklaringer

«[P]ersonopplysninger» beskrives som identifiserbare opplysninger om en fysisk person kalt den registrerte, jf. GDPR art. 4 nr. 1. Ulike deler informasjon kan til sammen utgjøre personopplysninger ved å identifisere en spesifikk person, jf. GDPR art. 2, se art. 4 nr. 1 og 5.[18] Eksempler på personopplysninger er navn, fødselsnummer, D-nummer, bosted eller en nettindikator. Begrepet er tolket vidt i personvernforordning og omfatter alle opplysninger til en bestemt person. Personopplysningsbegrepet er en rettslig standard som varierer med tid og forholdene ellers. [19] For at personvernforordningen skal komme til anvendelse, må det foreligge en eller flere personopplysninger.

Personopplysningsvern handler om normer for behandling av personopplysninger. Begrepet er en underkategori av personvern.[20] I oppgaven brukes personvern når det er tale om både personopplysningsvern og personvern, siden personvern også omhandler i tillegg retten til privatliv. For den registrertes rettigheter ved behandling av helseopplysninger er begge begrepene relevant. Enkelte steder ville det vært mer presist å bruke begrepet personopplysningsvern i stedet for personvern. For å unngå forvirring med mange uttrykk for opplysninger brukes begrepene personopplysninger, helseopplysninger og personvern i beskrivelsen av behandling av opplysningene.

«[H]elseregister» angis som et oppbevaringssystem hvor helseopplysninger lagres systematisk slik at pasientinformasjonen kan finnes igjen, jf. hregl. § 2 bokstav c. Eksempler på helseregistre er Norsk pasientregister, Medisinsk fødselsregister, Meldingssystem for smittsomme sykdommer, Nasjonalt register over hjerte- og karlidelser og Reseptbasert legemiddelregister kalt Reseptformidleren.

«[B]ehandling» beskrives etter GDPR art. 4 nr. 2 som en operasjon som utføres med personopplysninger enten automatisk eller ikke. Eksempel på behandling av helseopplysninger i helseregistre er for eksempel innsamling, registrering, organisering, lagring, gjenfinning, sammenstilling elle sletting av opplysningene.

---

[18] GDPR fortalepunkter 14, 15, 15, 27, 29 og 30.

[19] 01248/07/EN s. 16-17.

[20] Schartum (2016) s. 20.

«[B]ehandlingsansvarlig» betegnes etter GDPR art. 4 nr. 7 som en fysisk eller juridisk person som bestemmer formålet med behandling av personopplysninger og hvilke midler som brukes. Behandlingsansvarlig i helsetjenesten kan være Folkehelseinstituttet for behandling av helseopplysninger i Dødsårsaksregisteret. Begrepene behandlingsansvarlig, databehandlingsansvarlig eller dataansvarlig brukes for å beskrive ansvaret for generell behandling av personopplysninger. Dataansvarlig anvendes i helseretten, likevel brukes begrepet behandlingsansvarlig i denne oppgaven som i den norske oversettelsen av personvernforordningen.

«[D]atabehandler» forklares etter GDPR art. 4 nr. 8 som en fysisk eller juridisk person som behandler personopplysninger på vegne av den behandlingsansvarlige. I helsetjenesten er databehandleren vanligvis et helseforetak som utfører en underleverandørtjeneste for behandlingsansvarlig, for eksempel behandle helseopplysninger i Dødsårsakregisteret. Databehandler har et selvstendig ansvar for at behandling av helse- og personopplysninger skjer i samsvar med personvernforordningen.

1.6 Den videre fremstillingen

I kapittel 2 settes temaet i en rettslig kontekst. Deretter vurderes første problemstilling om risiko for innskrenkning ved behandling av den registrertes rettigheter i kapittel 3. I kapittel 4 vurderes den andre problemstillingen om hvordan den registrertes personvern ivaretas ved behandling i helseregistre. I kapittel 5 vurderes den tredje problemstillingen om hvordan grunnprinsipper om personvern oppfylles ved behandling i helseregistre. I kapittel 6 analyseres rettskildene nevnt i kapittel 3-5 for å kartlegge hvordan den registrertes rettigheter ivaretas i to konkrete helseregistre. Avslutningsvis oppsummeres problemstillingene og trekker fram enkelte rettspolitiske perspektiver av temaet i kapittel 7.

2 GRUNNLEGGENDE PERSONOPPLYSNINGSRETTIGHETER PÅ HELSEOMRÅDET

2.1 Grunnleggende formål og hensyn bak personvernet

Hensikten bak personvernregelverket er å skape frihet, sikkerhet, rettferdighet og økonomisk fellesskap i EU og EØS-området.[21] Den fysiske persons velferd skal ivaretas ved behandling av personopplysninger.[22] Bakgrunnen for å fornye personvernreglementet i EU fra EUs tidligere personverndirektiv er hovedsakelig å skape ensartede regler i EU og EØS-området.[23] Like regler i EU gir større beskyttelse av personopplysninger på tvers av landegrensene i Europa. Digitaliseringen reduserer betydningen av fysisk avstand og administrative landegrenser. Med økte datamengder har samtidig behandlingsomfanget av personopplysninger økt betraktelig. Disse trendene lå til grunn for et økende behov for sikrere håndtering av personopplysninger. Dette gjelder i særlig grad sensitiv informasjon som helseopplysninger.

Personvernet skal sikre økonomisk og sosial framgang.[24] EU ble opprettet med grunnideen om fri bevegelse av mennesker, varer, tjenester og kapital på tvers av medlemslandenes grenser, se EØS-avtalen[25] art. 1 nr. 2. Medlemslandene i EU og EØS skal utgjøre et felles hjemmemarked. Personvernforordningen skaper nødvendig tillit hos befolkningen med streng håndheving.[26] Tillit er nødvendig for at den digitale økonomien skal kunne utvikles i det indre markedet. Personvernforordningen skal ytterligere styrke det indre markedets posisjon i det digitale verdensmarkedet.[27] Hensikten med de oppdaterte reglene er å gi enkeltpersoner større kontroll over egne personopplysninger.[28] Sentrale faktorer for å oppnå målet er rettssikkerhet og en opplevd trygghet for fysiske personer, markedsdeltakere og offentlige myndigheter.[29]

Et mål med nytt reglement for personvern er følgelig fri utveksling av personopplysninger på en sikker måte, se GDPR art. 1 (1). For å realisere og styrke det indre markedet er ensartede regler et

[21] GDPR fortalepunkt 2.
[22] GDPR fortalepunkt 2.
[23] GDPR fortalepunkt 10.
[24] GDPR art. 1 (2) og fortalepunkt 2.
[25] Lov 27. november 1992 nr. 109 gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde.
[26] GDPR fortalepunkt 7.
[27] GDPR fortalepunkt 2.
[28] GDPR fortalepunkt 7.
[29] Skullerud (2018) s. 41.

nødvendig virkemiddel. Formålsbestemmelsene art. 1 og 2 er sentrale tolkningsfaktorer ved bruk av bestemmelsene som følger av personvernforordningen.[30]

2.2 Personvern som en menneskerett

Av EMK art. 8 fremgår det at alle mennesker har rett til respekt for privatliv og familieliv. Inngrep kan kun gjøres på visse vilkår. Pasienter har på lik linje rett til respekt for sine helseopplysninger. Dersom helseopplysninger skal behandles må det godkjennes av pasienten, jf. hregl. § 9. Kjernen i personvernet er å sikre vern av fysiske personers rettigheter og friheter ved behandling av personopplysninger.[31] Ved oppbevaring av personopplysninger omtales pasienten som «den registrerte», jf. hregl. § 10, se GDPR art. 2 bokstav a.

Etter EUs charter om grunnleggende rettigheter[32] (pakten) art. 8 har borgere rett til beskyttelse av personopplysninger som gjelder seg selv. Personopplysningene skal behandles på en rettferdig måte. Et skjerpet krav etter personvernforordningen er at personopplysninger kun skal behandles for spesifikke formål, jf. GDPR art. 5 nr. 1 bokstav b. Vilkårene for å behandle personopplysninger er alternativt «samtykke» eller annet rettslig grunnlag, jf. GDPR art. 6. Pasienter har på samme måte rett til vern av sine opplysninger som er innsamlet. Helsepersonells taushetsplikt etter hregl. § 17, jf. hpl. § 21 kan anses som et forsøk på å oppfylle denne menneskerettigheten i samsvar med annen lovgivning.[33] Vern av personopplysninger kommer i tillegg til den enkeltes personlige integritet og retten til privatliv, se pakten art. 3 og 7.

2.3 Grunnlovbeskyttelse for pasienter

Personvernet har grunnlovsvern. I følge Grl. § 102 (2) skal staten sikre et vern om den personlige integritet. Registrering, lagring og annen behandling av helseopplysninger kan anses som inngrep i den personlige integriteten.[34] Til tross for at det ikke fremgår eksplisitt av ordlyden, er det lite tvil om at personvernet må innfortolkes i Grl. § 102 (2). Rett til personvern må ses ut fra forholdet mellom stat og individ. Staten er etter Grl. § 102 (2) forpliktet til å behandle borgernes personopplysninger i tråd med lovgivningen for øvrig. Bakgrunnen for vernet er å hindre maktmisbruk av staten ovenfor borgerne. Et godt personvern er en forutsetning for et rettferdig og velfungerende demokrati i rask teknologisk endring – spesielt også ved behandling av helseopplysninger.

[30] Skullerud (2018) s. 41.

[31] Skullerud (2018) s. 42.

[32] Den Europæiske Unions Charter om Grunlæggende Rettigheder. Konsolideret udgave 2016 (2016/C 202/02).

[33] Befring (2017) s. 37.

[34] Kierulf (2016) note 239A7.

Retten til personvern er ikke ubestridelig.[35] Beskyttelse av den enkeltes pasients personvern kan gå utover mulighet til å forske på helseopplysninger og kan være et hinder i utviklingen av medisiner. Forholdsmessighetsprinsippet er et sentralt prinsipp innenfor EU- og EØS-retten[36] og forvaltningsretten generelt. Prinsippet innebærer at forvaltningen kan foreta en skjønnsmessig avveiing. Prinsippet gir standarder som danner grunnlag for interesseavveininger mellom byrder og goder og sterke og svake interesser i hver enkelt vurdering.[37] Forholdsmessighetsprinsippet uttrykkes i retten til beskyttelse av privatlivet i EMK art. 8 og personvernet i Grl. § 102 (2). Ytterligere uttrykkes det i GDPR art. 5 nr. 1 bokstav b-d at all behandling av personopplysninger må være forholdsmessig. Utfordringen ved behandling av personopplysninger til sekundærbruk er at det kontinuerlig må ses ut ifra to hovedhensyn. På den ene siden vil innsamling av helseopplysninger være nyttig for samfunnet ved økt kunnskap om helse og sykdom som kan komme den enkelte pasient til gode. På den andre siden vil innhenting av informasjon gjøre et inngrep i den enkelte pasients rett til personvern.

2.4 Personopplysningsbegrepet tolket i rettspraksis og annen praksis i EU

I forbindelse med vedtak av ny personopplysningsrett måtte det tas stilling til innholdet i begrepet personopplysning. Spørsmålet om personopplysningsbegrepet ble blant annet behandlet av EU-domstolen i *Nowak* inntatt i C-434/16. Saken gjaldt en student som ønsket innsyn i en rettet eksamensbesvarelse som han hadde strøket på. Spørsmålet i saken var hvorvidt eksamensbesvarelsen ble ansett som personopplysninger etter betydningen av EUs tidligere personverndirektiv art. 2 bokstav a, i følge C-434/16 premiss 26. Retten fastslo at eksamensbesvarelsen utgjorde personopplysninger i samsvar med EU-direktivet. I sin vurdering la retten vekt på at innholdet av besvarelsen gjenspeiler eksamenskandidatens kunnskap og kompetanse på et gitt område. I besvarelsen reflekteres personens tankegang, dømmekraft og kritiske sans, se C-434/16 premiss 37. Avgjørelsen ga et særlig vidt virkeområde for hva som omfattet studentens personopplysninger. Avgjørelsen åpner ytterligere for vid innsynsadgang da retten til innsyn også omfattet innsyn til eksaminators rettelser og kommentarer til besvarelsen i følge C-434/16 premiss 51.

I *Nowak* bruker EU-domstolen en bred fortolkning av personopplysningsbegrepet. Resultatet reflekterer EU- og EØS-lovgivningens mål om å ha vidt virkeområde av begrepet og omfavner all informasjon relatert til datasubjekter, se GDPR art. 1. Generaladvokaten i *Nowak* uttalte at selv om vurderingen var etter bestemmelse fra EUs tidligere personverndirektiv, endres ikke forståelsen av personopplysningsbegrepet i personvernforordningen.[38] Dette taler for at avgjørelsen skal ha tung rettskildemessig vekt i vurderinger av innholdet av personopplysningers rekkevidde. Dermed har den

[35] GDPR fortalepunkt 4.

[36] Se for eksempel GDPR fortalepunkt 4.

[37] Befring (2017) s. 57.

[38] G.A. Sag-434/16 premiss 3.

prejudisielle anmodningen også betydning for fremtidig bruk av EU-rettens databeskyttelse. Avgjørelsen kan tas til inntekt for at EU-domstolen er forberedt på å overholde strengere databeskyttelsesregler etter personvernforordningen. Uavhengig av hvordan tidligere EU-rettspraksis har vært må fremtidige avgjørelser unngå å fortolke personvernforordningen innskrenkende.

I saken PVN-2006-04 ga Personvernnemnda uttrykk for at databehandling som ikke behandler personopplysninger, avgrenses fra virkeområdet til den tidligere personopplysningsloven 2000. Klager la ned påstand om at operativsystemet Microsoft Windows XPs automatiske oppgraderingsfunksjon var personvernstridig. Spørsmålet i saken gikk ut på om personopplysninger behandles i forbindelse med bruk av funksjonen automatiske oppdateringer. Personvernnemnda la til grunn at opplysninger som kan knyttes til enkeltpersoner ikke behandles direkte eller indirekte. Konklusjonen ble at saken falt utenfor personopplysningsloven 2000. Saken illustrerer når opplysninger i databehandling kan være utenfor rekkevidden personvernbegrepet. Ved behandling av store mengder data er det av betydning å vite om behandling av personopplysninger omfattes. Ettersom saken reiser spørsmål om omfanget til personopplysningsbegrepets tillegges saken noe vekt for fortolkningen av personvernforordningens innhold i vurderingen av oppgavens problemstillinger.

Enkelte europeiske datatilsyn og domstoler har allerede avsagt avgjørelser angående forståelsen av personvern. Avgjørelsene har betydning som tolkningsmomenter ettersom alle EU- og EØS-land skal etterleve personvernforordningen.[39]

En sak avsagt i det østerrikske datatilsynet handlet om hvor lenge en tilbyder av telekomtjenester kunne oppbevare masterdata.[40] Masterdata inneholder nødvendige opplysninger for å utføre telekomstjenestens oppgaver. Spørsmålet gjaldt om et telekomselskap hadde bevart personopplysninger for lenge ved å oppbevare dem i ti år. Skattelovgivning åpnet for bevaring inntil ti år. Det østerrikske datatilsynet la til grunn at oppbevaring i ti år var i strid med personvernforordningen fordi det ikke forelå plikt om oppbevaring så lenge etter skattelovgivningen.

I Tyskland ble en avgjørelse avsagt av en regional domstol om rett til sletting av personopplysninger.[41] Spørsmålet gikk ut på om en tidligere administrerende direktør i en veldedighetsorganisasjon kunne kreve at en søkermotortilbyder slettet navnet hans fra søkeresultatet. Søketreffene lenket ham videre til artikler om hans helse. Domstolen fastslo at det å fjerne søkeresultatet kan være omfattet av den registrertes rett til sletting. Imidlertid er denne retten begrenset. Problemstillingen måtte vurderes ut fra en interesseavveining. Det ble lagt vekt på at

[39] GDPR fortalepunkt 10.
[40] Arendt (2018).
[41] Arendt (2018).

søketreffende i utgangspunktet var lovlige. Ytterligere er lenker nødvendig for at internett skal fungere etter sitt formål. Konklusjonen ble at kravet om sletting ikke førte frem.[42] Saken har likhetstrekk til temaet når det gjelder personopplysninger relatert til helse og hvor vid rekkevidden til den registrertes rettigheter er, blant annet rett til sletting av personopplysninger.

De to sistnevnte avgjørelsene får lite rettskildemessig vekt for vurderingen av oppgavens problemstillinger ettersom de er avsagt av underinstanser og en annen europeisk tilsynsmyndighet. Imidlertid er det av betydning at det har kommet avgjørelser vedrørende fortolkningen av personvernforordningen. Det er lite tvil at det er mye som er uavklart etter personvernforordningen. Disse avgjørelsene kan brukes som tolkningsmomenter for den registrertes rett til sletting og rettens begrensninger.

2.5 Helseopplysninger som en del av personvernet

Helseopplysninger forklares som taushetsbelagt informasjon om helseforhold eller relevans for helseforhold knyttet til enkeltpersoner. I GDPR art. 4 nr. 15 betegnes helseopplysninger som personopplysninger om en persons fysiske eller psykiske helsetilstand. Begrepet inkluderer ytelse av helsetjenester. Legaldefinisjonen i hregl. § 2 bokstav a har tilsvarende ordlyd. Tidligere lover hadde ingen definisjon av helseopplysninger. Begrepet «helseopplysninger» er derimot tolket vidt i rettspraksis.[43] Ved tolkning av GDPR art. 9 nr. 1 er tidligere rettspraksis dermed relevant.[44] I *Lindqvist* inntatt i C-101/01 fastslo EU-domstolen at begrepet «helseopplysninger» skal tolkes vidt, se premiss 50-51. Saken gjaldt opplysninger om en person som var delvis sykemeldt på grunn av en fotskade. EU-domstolen kom til at denne opplysningen inneholdt sensitive personopplysninger. Informasjon om fysisk og psykisk helsetilstand oppfattes som opplysninger om helseforhold.[45] Avgjørelsen er et eksempel på at begrepet helseopplysninger kan tolkes vidt til å omfatte forhold relatert til en persons helse.

Helseopplysninger omfatter opplysninger om sosiale forhold som kan si noe om personens helsetilstand.[46] Det må vurderes i hvert tilfelle om opplysninger om sosiale forhold har sterk nok tilknytning til helseforhold.[47] Innholdet i helseopplysninger forklares som informasjon om den registrertes tidligere, nåværende og fremtidige fysiske og psykiske helsetilstand, samt om ytelser av helsetjenester etter GDPR art. 4 nr. 15.[48] Ordlyden av helseopplysninger inkluderer informasjon om

[42] Arendt (2018).
[43] Skullerud (2018) s. 68.
[44] Skullerud (2018) s. 106.
[45] Wessel-Aas (2018) s. 74.
[46] Schartum (2012) note 21.
[47] Ot.prp. nr. 92 (1998-1999) s. 104.
[48] GDPR fortalepunkt 35.

sykdommer, funksjonsnedsettelse, sykdomsrisiko, sykehistorie, helsehjelp eller den registrertes fysiske eller biomedisinske tilstand uavhengig av hvem som gir opplysningene.[49] Helseopplysninger får utvidet betydning til å gjelde personopplysninger om den registrertes familie hvis det angår genetiske og arvelige sykdommer definert i GDPR art. 4 nr.13. Den utvidede tolkningen tilsier at helseopplysninger er et omfattende begrep hvor få helserelaterte opplysninger utelukkes.

2.6 Det norske regelverket om personopplysninger i helseretten

Personopplysninger har fått en innstrammet regulering innenfor flere helselover etter at personvernforordningen trådte i kraft. Særlig gjelder innstrammingen ved behandling av helseopplysninger i helseregistre for å ivareta personvernet. For behandling av helseopplysninger er det rettslige grunnlaget helseregisterloven, helseforskningsloven[50] (hforsknl.) og andre relevante forskrifter som MSIS-forskriften. Helseregisterloven formål etter hregl. § 1 går ut på å tilrettelegge for behandling av helseopplysninger. Behandlingen skal være helsefremmende, sykdomsforebyggende og forbedre helse- og omsorgstjenester. Pasientens personvern skal ivaretas med «etisk forsvarlig» behandling, jf. hregl. § 1. Ved behandlingen av helseopplysninger skal det tas hensyn til hva som er til individets og samfunnets beste, jf. hregl. § 1. Til tross for innstrammingene videreføres gjeldende helselover så langt det er adgang etter personvernforordningen.[51]

[49] GDPR fortalepunkt 35.

[50] Lov 20. juni 2008 nr. 44 medisinsk og helsefaglig forskning.

[51] Prop. 56 LS (2017-2018) s. 183.

3 BEHANDLING AV PERSONOPPLYSNINGER I HELSETJENESTEN

3.1 Oversikt

I dette kapittelet vurderes hvordan behandling av personopplysninger i helseregistre kan føre til risiko for innskrenkning i den registrertes rettigheter og friheter. Først ses det på hvilke lovendringer som har oppstått i punkt 3.2. Deretter skal det vurderes hvilke risikoer som kan være problematisk for den registrerte i punkt 3.3. Videre redegjøres det for hvem som har behandlingsansvaret ved behandling av helseopplysninger i punkt 3.4. Avslutningsvis vurderes risikoen ved behandling for innskrenkning av personers rettigheter og friheter i punkt 3.5.

3.2 Endring i lovgivningen for behandling av helseopplysninger

Utvikling av nye informasjons- og teknologisystemer (IKT) forenkler og effektiviserer tilgangen til helsedata. Kun behandling av helseopplysninger med spesifikke formål er tillatt, se GDPR art. 5 (1) bokstav b. Slik behandling omfatter forskning, styring, statistikk, planlegging, helseanalyser, beredskap og kvalitetsforbedring, jf. hregl. § 3. Melde- og konsesjonsplikt etter hregl. § 7 bortfaller og erstattes med dokumentasjonsplikt og konsekvensvurderinger for den behandlingsansvarlige.[52] Personvernforordningen gir den registrerte rett til dataportabilitet som innebærer en rett til å overføre personopplysninger fra én tjenestetilbyder til en annen.[53] Helse- og omsorgsdepartementet opprettet i 2016 et helsedatautvalg[54] med forslag til et nytt system for behandling av helsedata.[55] Målsettingen til helseanalyseplattformen er å forenkle tilgang til og legge til rette for analyser på tvers av datakilder som helseregistre og andre kilder til helseopplysninger. Ved slik optimalisering av behandlingsprosessen er det verdt å merke seg hvilke risikoer som oppstår med hensyn til innskrenkning av den registrertes rettigheter og friheter.

3.3 Risiko for den registrertes rettigheter og friheter

3.3.1 EØS-rettslig utgangspunkt og individperspektiv

Utgangspunktet for vurderingen er hvordan norsk rett i lys av EØS-retten har tatt i bruk rettigheter og plikter knyttet til personvern. Det er av vesentlig betydning at lovendringer i personvernforordningen har ført til at individet står i sentrum.[56]

Personvernforordningen kan forstås ut fra et individperspektiv hvor reguleringen skal beskytte fysiske personers rettigheter og friheter. En persons rettigheter innebærer rett til vern av personopplysninger, jf. GDPR art. 1 nr. 2. Formålet er videreført fra EUs tidligere

[52] Prop. 56 LS (2017-2018) s. 9.

[53] Prop. 56 LS (2017-2018) s. 9.

[54] Helse- og omsorgsdepartementet (2017).

[55] Helse- og omsorgsdepartementet (2018).

[56] GDPR fortalepunkt 1.

personverndirektiv, men har også fått større plass i hele forordningen. Forankringen viser at det er nødvendig at oppmerksomheten rettes mot individet ved vurdering av behandling av personopplysninger. Behandlingen anses som et inngrep i den registrertes rett til privatliv og vern av personopplysninger. Inngrepet går derimot lenger enn dette. *Nowak* uttrykker blant annet at rekkevidden av personopplysninger strekker seg lengre enn tidligere antatt. *Nowak* er et eksempel på hvordan ikke bare opplysninger knyttet til en person kan anses som personopplysninger, men også forholdene ellers.

Ved at flere forhold anses som personopplysninger fører det til at den registrertes rettigheter får et større virkeområde. Personvernforordningen uttrykker at det må foretas en bredere vurdering av hva som regnes som en persons frihet til å bestemme hvilke opplysninger som blir registrert og hvilke som skal beskyttes av retten til privatliv.[57] Ut i fra dette bør ikke vurderingen av den registrertes rettigheter ved behandling begrenses til retten til privatliv og vern av personopplysninger.

En grunnleggende forutsetning for behandling av personopplysninger er å avverge at behandlingen medfører høy risiko for inngrep i den registrertes rettigheter og friheter. Den registrertes fundamentale friheter omfatter ytringsfrihet, tankefrihet, bevegelsesfrihet, kommunikasjonsvern, forbud mot diskriminering, retten til frihet og samvittighets- og religionsfrihet.[58] Individets friheter må ivaretas og det må gis garantier fra helsetjenesten på et systemnivå. Den registrertes rettigheter til personvern innebærer blant annet rett til informasjon, retting, sletting, å protestere, begrensning, dataportabilitet og rettigheter ved automatiserte avgjørelser. Flere av rettighetene gjør seg gjeldende i ulike deler av behandlingsprosessen av personopplysninger i helseregistre.

3.3.2 Den registrertes rolle

Begrepet «den registrerte» er ikke direkte definert i personvernforordningen eller norsk lovgivning, men fremgår indirekte av legaldefinisjonen om samtykke til behandling i hregl. § 2 bokstav e. Ordlyden tilsier at den registrerte er en person som ved erklæring kan samtykke til behandling av helseopplysninger om seg selv i samsvar med GDPR art. 4 nr. 11. Med andre ord forklares den registrerte som en person som det registreres personopplysninger om i et register eller en annen form for system. I helseretten er den registrerte enten en pasient eller en bruker.

Enkelte registrerte kan ha behov for ekstra beskyttelse som følge av at de tilhører en utsatt gruppe og er mer utsatt for forskjellsbehandling. Den registrerte kan være en mann, en kvinne, et barn under 16 år, en eldre person, en transkjønnet eller en som tilhører en annen gruppe.

[57] GDPR fortalepunkt 4.
[58] GDPR fortalepunkt 4.

Det kreves utfyllende sikkhetsgarantier for opplysninger relatert til helse eller seksuelle forhold som kan bli avslørt ved gjenbruk av personopplysninger eller ved sammenstilling av annen helsedata når helseopplysninger eller opplysninger om seksuelle forhold behandles.[59] Således kan behandling av personopplysninger innenfor helseretten føre til utilsiktede virkninger. En særlig sårbar gruppe pasienter er eldre homofile som kan forskjellsbehandles på grunn av alderdom og seksuell orientering. Det er fortsatt eldre mennesker som verken har stått fram som homofile til fastlegen sin eller står oppført med informasjon som tilsier deres seksuelle orientering i relevante helseregistre. Flere pasienter forklarer det med frykt for forskjellsbehandling og skam.[60] Ved å tilbakeholde slik informasjon kan de også tilbakeholde andre opplysninger som kunne vært sentralt for å få forsvarlig helsehjelp. Hvis derimot helseopplysninger om seksuell orientering bidrar til at den registrerte kan identifiseres, kan det ha utilsiktede virkninger for den registrerte.[61]

3.4 Behandlingsansvar for behandling av helseopplysninger i helseregistre

3.4.1 Behandlingsansvarlig sitt ansvar ved behandling i helseregistre

Hvert helseregister må ha en behandlingsansvarlig. Den behandlingsansvarlige skal bestemme formålet med behandling av helseopplysninger og hvilke hjelpemidler som skal tas i bruk. Uttrykket behandlingsansvarlig er brukt for å avgrense mot ansvarlig for behandling av helsehjelp. Behandlingsansvarlig må vurdere om et av vilkårene i GDPR art. 9 nr. 2 er oppfylt samt om det foreligger behandlingsgrunnlag etter GDPR art. 6 før behandlingen kan starte.[62]

For å sikre at den registrertes rettigheter blir ivaretatt, må databehandlingen utføres i tråd med det innstrammede regelverket for personvern. Behandlingsansvarlig har plikt til å føre internkontroll av både egen behandling og av eksterne databehandlere, se GDPR art. 24, jf. hregl. § 22. Plikten går ut på å etablere og vedlikeholde planlagte og systematiske tiltak.[63] Dersom Folkehelseinstituttet bruker eksterne samarbeidspartnere for behandling av personopplysninger har de plikt til å kontrollere behandlingsprosessen. Konsekvensene for brudd på personvernreglene er betraktelig høyere enn tidligere med gebyrer på opptil 10 000 000 euro etter GDPR art. 83 nr. 4.

Etter EUs tidligere personverndirektiv art. 24 var det opp til hvert enkelt medlemsland å fastsette sanksjoner for overtredelse av bestemmelser etter direktivet. Dette førte til forskjeller mellom hvilke sanksjoner som ble gitt i det enkelte land. I 2017 ble ni helseforetak i Helse Sør-Øst blitt varslet om overtredelsesgebyr på 800 000 kr for sikkerhetsbrudd.[64] Hendelsen fikk økonomiske konsekvenser

[59] Council of Europe (2017) s. 2.
[60] Clausen (2018).
[61] GDPR fortalepunkt 83.
[62] GDPR fortalepunkt 51.
[63] Prop. 72 L (2013-2014) s. 197.
[64] Datatilsynet (2017).

fordi helseforetakene ikke oppfylte plikten til sikkerhetsledelse, risikovurderinger og tilgangsstyring i forbindelse med tjenesteutsetting av IKT-Drift til utlandet.

3.4.2 Databehandler sitt ansvar ved behandling i helseregistre

Sammenlignet med en behandlingsansvarlig har en databehandler mindre ansvar for behandlingen. En behandlingsansvarlig kan inngå avtale med databehandler om behandling av helseopplysninger, jf. GDPR art. 4 nr. 8. En databehandler har etter GDPR art. 4 nr. 8 et større ansvar enn hva en databehandler hadde i henhold til den tidligere personopplysningen 2000 og EUs tidligere personverndirektiv.[65] For eksempel har Helsedirektoratet som behandlingsansvarlig inngått avtale med flere helseforetak som databehandlere for helseopplysninger i Norsk pasientregister etter hregl. § 11.

I behandleravtalen skal det klargjøres hvordan behandlingen av personopplysninger skal foretas. Behandleravtaler er særlig viktig i helsetjenesten hvor ulike helseforetak jobber i forskjellige helsesektorer med helseregistre. Helseopplysninger samles inn på landsbasis i sentrale helseregistre. I tillegg til nasjonale helseregistre skal helseopplysningene bli tilgjengelige gjennom en helseanalyseplattform hvor databehandlere kan søke om tilgang. Store mengder helsedata vil være tilgjengelig i portalen. Ved å gi tilgang til så mye informasjon på ett sted kan det få alvorlige personvernkonsekvenser dersom det oppstår et sikkerhetsbrudd. Ved bruk av eksterne databehandlere er behandlingsansvarlig forpliktet til å kontrollere at de overholder lovgivningen om behandling av helseopplysninger. Hendelsen med Helse Sør-Øst er et eksempel på hvilke personvernkonsekvenser som kan oppstå når det ikke gjennomføres tilstrekkelig kontroll av databehandlere.

3.5 Vurdering av behandlingens risiko for innskrenkning av personers rettigheter og friheter

Felles for personopplysninger som samles i helseregistre er at det gjelder informasjon om pasient eller bruker. Helseopplysninger er av sensitiv karakter. Særlig angår dette sykdommer registrert i helseregistrene Meldingssystem for smittsomme sykdommer og Nasjonalt vaksinasjonsregister som inneholder helseopplysninger som kan anses stigmatiserende.

For å hindre misbruk av personopplysninger som i tilfelle ved hackerangrep er det flere forebyggende tiltak den enkelte behandlingsansvarlige kan. Opplysninger i helseregistre må oppbevares i samsvar med lagringsbegrensning, jf. GDPR art. 5 nr. 2 bokstav e. Det er for eksempel ikke nødvendig å lagre alle helseopplysninger i kreftregisteret for å oppnå dens formål. Siden mange helseregistre finnes i digital form, bør det sørges for at det er teknisk sikkerhet i databasene. For å kunne oppdage sikkerhetsbrudd må det være kontinuerlig overvåking av helseregistrene. På denne

[65] Skullerud (2018) s.61.

måten kan behandlingsansvarlig iverksette sikkerhetstiltak raskt ved sikkerhetsbrudd. Hvert helseregister må ha egne rutiner for hvordan behandlingsansvarlig skal reagere ved hackerangrep.

Andre risikoer kan være at helsepersonell urettmessig undersøker i helseregistrene. For å hindre slik urettmessig tilgang kan behandlingsansvarlig foreta mange av de samme forebyggende tiltakene som ved hackerangrep. Den behandlingsansvarlige kan begrense tilgang til informasjonen blant helsepersonell. For å gi helsehjelp er det ikke nødvendig at alt helsepersonell har tilgang til alle pasienters helseopplysninger. Når det tas stilling til risikoen for inngrep i pasientens rettigheter og friheter ved registrering i helseregistre må flere faktorer enn hackerangrep vurderes.

Det er en risiko for at helsepersonell urettmessig undersøker i helseregistre informasjon de ikke behøver i arbeidet sitt. Informasjon om familie og kjente eller offentlige personer kan være fristende å få tilgang til. Derimot må det presiseres at helsepersonell bare unntaksvis avviker retningslinjer og interne arbeidsinstrukser. For å oppdage og hindre urettmessig undersøkelser, utfører IKT-avdelinger på sykehus stikkprøver. Dersom helsepersonell avviker fra sine arbeidsinstrukser kan det oppdages med denne metoden. Samtidig vil muligheten for å bli oppdaget ha en preventiv virkning for helsepersonell å unngå uautoriserte undersøkelser av helseregistre.

Kunnskap om sykdommer er viktig for å forbedre helsehjelp og forebygge utvikling av sykdomsforløpet. Behandlingsansvarlig må likevel ikke se bort fra risiko for inngrep ved behandling av den registrertes rettigheter og friheter. Behandling av helseopplysninger kan medføre risiko for andre rettigheter og friheter utover retten til privatliv og vern av personopplysninger. Brudd av konfidensialitet av et helsepersonell eller databehandler kan medføre konsekvenser som økonomisk tap, diskriminering og tap av den registrertes og behandlingsansvarliges omdømme.

For å svare på problemstillingen om hvordan kan behandling av personopplysninger i helseregistre føre til risiko for innskrenkning i den registrertes rettigheter og friheter bør disse momentene tas i betraktning. I vurderingen må det tas en grundig risikovurdering i samsvar med GDPR art. 32 og en vurdering av personvernkonsekvensene etter GDPR art. 35.

I en personvernkonsekvensutredning må det settes spørsmålstegn ved hvorfor det innsamles og lagres helseopplysninger. I den konkrete vurderingen må det tas stilling til hvorvidt det er tilstrekkelig grunn til å behandle slik at databehandler kan se bort fra risikoen for inngrep i den registrertes rettigheter og friheter. Til slutt må det tas i betrakting hva som vil skje dersom det foreligger et brudd på konfidensialitet av forsker eller helsepersonell. Databehandler må vurdere om bruddet kan føre til økonomisk tap, diskriminering eller tap av omdømme for den registrerte eller behandlingsansvarlig. Disse vurderingene må trekkes inn i konsekvensutredning av personvern etter GDPR art. 35.

4 IVARETAKELSE AV DEN REGISTRERTES RETT TIL PERSONVERN VED BEHANDLING I HELSEREGISTRE

4.1 Oversikt over hvilke opplysninger som behandles i helseregistre

I dette kapittelet vurderes det i hvilken grad den registrertes rett til personvern ivaretas ved behandling av personopplysninger i helseregistre.

Ved behandling av helseopplysninger må det sørges for at den registrertes rett til personvern ivaretas. For å vurdere behandlingsprosessen i helseregistre er det nyttig å vite hvilke opplysninger som behandles for å avdekke behovet for personvern til den enkelte registrerte. Opplysninger som registreres i helseregistre er personopplysninger, i tillegg til personopplysninger om helse fra pasientjournal, biologisk materiale, nasjonalt identifikasjonsnummer eller fingeravtrykk.[66] Disse anses som personopplysninger når de kan tilbakeføres enten direkte eller indirekte til en pasient. Resultat fra analyser av blodprøver anses som helseopplysninger til tross for at de først blir identifiserbare ved koblingsnøkler til den registrertes andre personopplysninger.[67] Dette taler for at personopplysningsbegrepet skal tolkes vidt også i helseretten.

4.2 Vilkår for å behandle helseopplysninger

Det rettslige utgangspunktet er at personvernforordningen, jf. popplyl. § 1 får anvendelse for all behandling av personopplysninger om ikke annet følger av særskilt lov. Helseregisterloven regulerer særskilt behandling av helseopplysninger, jf. hregl. § 3 og får anvendelse der loven utfyller personvernforordningens bestemmelser.

Etter GDPR art. 9 nr. 1 er det i utgangspunktet forbudt å behandle «helseopplysninger». Forbudet gjelder ettersom behandlingen kan innebære høy risiko for den registrertes rettigheter og friheter.[68] Derfor bør helseopplysninger gis et særskilt vern etter personvernforordningen.[69] Etter hregl. § 6 (1) skal helseopplysninger behandles i samsvar med prinsippene for behandling etter GDPR art. 5. I følge prinsippet om formålsbegrensning skal graden av personidentifikasjon begrenses til hva som er nødvendig for det konkrete formålet, jf. hregl. § 6 (2). Videre fremgår det av hregl. § 6 at graden av personidentifikasjon skal begrunnes. Reglene for behandlingsgrunnlag angir inngangsvilkårene for behandling av personopplysninger i GDPR art. 6.[70] Bestemmelsen lister opp en uttømmende liste over vilkår som gjør behandling av personopplysninger lovlig, jf. GDPR art. 6 nr. 1.

[66] GDPR fortalepunkt 35.
[67] GDPR fortalepunkt 35.
[68] GDPR fortalepunkt 51.
[69] Council of Europe (2017) s. 2.
[70] Prop. 56 LS (2017-2018) s. 31-37.

Det skilles hovedsakelig mellom tre hjemmelsgrunnlag for behandling av helseopplysninger. For det første kan en databehandler behandle helseopplysninger etter lov, jf. GDPR art. 5 nr. 1 bokstav a, se hregl. § 6. For det andre kan en databehandler behandle etter myndighetsutøvelse, jf. GDPR art. 6 nr.1 bokstav e. For det tredje kan en databehandler behandle helseopplysninger til en pasient etter samtykke, jf. GDPR art. 6 nr. 1 bokstav a, se hregl. § 9 bokstav a. Samtykke skal danne rettsgrunnlaget som knytter seg til et spesifikt formål.[71] Videre bør det anvendte rettsgrunnlaget være forutsigbart for den registrerte og i samsvar med rettspraksis etter EU-domstolen og EMD.[72]

Personvernforordningen deler personopplysninger inn i ulike kategorier. Helseopplysninger faller under særlige kategorier av personopplysninger etter GDPR art. 9 nr. 1. Bestemmelsen er en forbudsregel hvor visse kategorier av sensitive opplysninger er utelukket fra behandling. I den tidligere personopplysningsloven 2000[73] og i EUs tidligere personverndirektiv ble særlige kategorier av personopplysninger kalt sensitive opplysninger.[74] Bortsett fra navnendringen har ikke innholdet i særlige kategorier av personopplysninger endret seg betydelig. Likevel er det en vesentlig forskjell fra den tidligere personopplysningsloven 2000. Særlige kategorier av personopplysninger inkluderer også genetiske og biometriske opplysninger for å entydig identifisere en fysisk person, se GDPR art. 9 nr. 1. Helseopplysninger er en relevant opplysningskategori som det er verdt å merke seg i henhold til hvilken grad den registrertes rett til personvern ivaretas ved behandling av personopplysninger med slik sensitive karakter. GDPR art. 9 nr. 4 gir adgang til at det kan fastsettes flere vilkår og begrensninger for behandling av helseopplysninger i nasjonal rett, for eksempel ved forskrift.

Kravet til hjemmel skal sikre at behandlingen foretas på en etisk forsvarlig måte, jf. hregl. § 1. Den naturlige språklige forståelse tilsier at behandlingen må være minst mulig inngripende og stå i forhold til formålet det skal ivareta. Etter forarbeidene skal behandlingen utføres i samsvar med menneskeverd og menneskerettigheter.[75]

Særlige kategorier av personopplysninger underlegges et særskilt vern for å unngå å bli misbrukt.[76] Det oppstilles flere unntak fra forbudet mot behandling av særlige kategorier, jf. GDPR art. 9 nr. 2. Artikkel 29-gruppen er erstattet med et nytt EU-organ kalt European Data Protection Board. Det tidligere EU-organet uttalte at unntakene i EUs tidligere personverndirektiv videreføres i personvernforordningen for særlige kategorier av personopplysninger. Unntakene er begrensende,

[71] Skullerud (2018) s. 81.
[72] GDPR fortalepunkt 41.
[73] Lov 14. april 2000 nr. 31 behandling av personopplysninger.
[74] GDPR fortalepunkt 10.
[75] Prop. 72 L (2013-2014) s. 118.
[76] Wessel-Aas (2018) s. 74.

uttømmende og skal tolkes snevert.[77] For å ivareta den registrertes rett til personvern må enten bruken av personopplysninger minimeres så mye som mulig eller så må den registrerte selv bestemme hvilke personopplysninger som kan brukes.

GDPR art. 9 nr. 2 bokstav h regulerer behandling av særlige kategorier personopplysninger når det er nødvendig ved yting av helsetjenester. Bestemmelsen nevner ulike virkeområder som tilsynelatende dekker all behandling av personopplysninger i helsevesenet med unntak av forskning.[78] Behandling av helseopplysninger til sekundærbruk er forankret i omfattende nasjonal regulering i helseregisterloven, pasientjournalloven[79] og helsepersonelloven[80]. GDPR art. 9 nr. 2 bokstav g gir adgang til behandling av personopplysninger dersom det er nødvendig for å ivareta viktige allmenne interesser. Bestemmelsen virker som en sikkerhetsventil som åpner for behandling av særlige kategorier personopplysninger når de ikke får anvendelse i de andre unntakene i GDPR art. 9 nr. 2. [81]

4.2.1 Krav om «samtykke» for behandling

Et sentralt unntak fra forbudet mot å behandle personopplysninger er «samtykke» fra den registrerte, jf. GDPR art. 9 nr. 2 bokstav a, jf. art. 7 og hregl. § 9 bokstav a.

Begrepet «samtykke» forklares som en «frivillig, spesifikk, informert og utvetydig» viljeserklæring gitt av den registrerte, jf. GDPR art. 4 nr. 11. En alminnelig språklig forståelse av «samtykke» tilsier at en person gir tillatelse til å foreta noe, for eksempel en handling. Når det gjelder behandling av helseopplysninger kan betydningen av «samtykke» trekke i retning av at det må gis et uttrykkelig samtykke til ett eller flere spesifikke formål.[82] En forutsetning er at nasjonal lovgivning ikke begrenser at et uttrykkelig samtykke kan oppheve forbudet, jf. GDPR art. 9 nr. 2 bokstav a.[83] Behandling av helseopplysninger hvor den registrerte har samtykket til registrering etter GDPR art. 6 (1) bokstav a og art. 9 nr. 2 bokstav a vil ha hjemmel direkte i personvernforordningen.

En pasient kan samtykke til at helseopplysninger skal registreres i et helseregister. Samtykke uttrykker at pasienten har akseptert og forstått hva registrering av helseopplysninger omfatter.[84] Samtykket i seg selv må være tydelig. Det kan ikke være tvil om en pasient takker ja til behandling av helseopplysningene i et register. Dersom pasienten virker usikker om den ønsker opplysningene

[77] 00323/07/EN s. 8.
[78] Skullerud (2018) s. 111.
[79] Lov 20. juni 2014 nr. 42 behandling av helseopplysninger ved ytelse av helsehjelp.
[80] Lov 2. juli 1999 nr. 64 helsepersonell.
[81] Skullerud (2018) s. 110.
[82] Wessel-Aas (2018) s. 164.
[83] Wessel-Aas (2018) s. 164.
[84] Søvig (2016) note 36.

tilgjengelig for forskere og andre som søker tilgang er ikke dette tilstrekkelig. Pasienten må dermed gjøre noe aktivt for å uttrykke samtykke, og dette øker graden rettighetene blir ivaretatt.

4.2.2 Når foreligger det et samtykke?

Den behandlingsansvarlige skal kunne bevise at det forelå et uttrykkelig samtykke, jf. GDPR art. 7 nr. 1. I GDPR art. 9 nr. 2 bokstav a brukes formuleringen «uttrykkelig samtykke» mens det i art. 6 kreves «samtykke». Det stilles ingen formkrav til samtykke.[85] Bevishensyn tilsier at det er hensiktsmessig at samtykke til behandling av helseopplysninger gis skriftlig.[86] På grunnlag av disse momentene og innstramming av reguleringen gjennom personvernforordningen tilsier det at passivt samtykke ikke er tilstrekkelig for å være et gyldig rettslig grunnlag.

Dersom samtykket motsetningsvis kan være både muntlig og skriftlig bør det være enkelt å trekke tilbake samtykket, jf. GDPR art. 7 nr. 3. Den registrertes aksept til at helsetjenester kan lagre opplysninger må ikke være absolutt. Det må være mulig å ombestemme seg, hvis ikke måtte det stilles høyere krav til informasjon av behandlingen. Dersom samtykke blir trukket tilbake, kan ikke opplysningene behandles videre på grunnlag av samtykket. Behandlingen som allerede er gjennomført blir imidlertid ikke endret. Derfor er det vesentlig at samtykkeerklæringen må inneholde informasjon om at samtykket kan trekkes tilbake.

Personvernnemnda la til grunn i PVN-2013-17 at det ikke forelå samtykke til registrering i Nasjonalt tvillingregister ved at deltakerne hadde sluttet seg til de opprinnelige tidsbegrensede og formålsbestemte tvillingsprosjektene. I Nasjonalt tvillingregister samles opplysninger om tvillinger for å bidra til forskning på årsaker til sykdom og forståelse av hva som gir god eller dårlig helse. Folkehelseinstituttet hadde som behandlingsansvarlig søkt om konsesjon for å forlenge og utvide Nasjonalt tvillingregister. Personvernnemnda måtte ta stilling til hvorvidt samtykkeerklæringene var vide nok til å omfatte tilføring av nye personopplysninger. I avgjørelsen ble det lagt til grunn at nye opplysninger vil være en utvidelse av registeret enten ved kobling til andre registre eller ved nye analyser av blodprøver. Tilføying av nye opplysninger og analyseresultater til registeret må samsvare med det avgitte samtykke. Personvernnemnda kom fram til at utløpte prosjekter som er spesifikke, konkrete og tidsavgrensede må innhente et nytt samtykke til sammenslåing. Nemndsavgjørelsen taler for at samtykkeerklæringer begrenser seg til hva den registrerte fikk informasjon om på tidspunktet samtykket ble gitt.

Når en registrert pasient samtykker til behandling av opplysninger i et helseregister må han eller hun informeres om prosessen, jf. GDPR art. 13. Databehandler skal beskrive hvilke opplysninger som innhentes. Et eksempel er Reseptformidleren som er en sentral database og mottar elektronisk

[85] Engelschiøn (2017) kommentar til § 2.

[86] Wessel-Aas (2018) s. 165.

resepter fra leger. Det rettslige grunnlaget for behandling i Reseptformidleren er hregl. § 9 bokstav a. Dersom en sykehuslege skal gjøre oppslag i Reseptformidleren for å få tilgang til resepter fra andre leger må sykehuslegen innhente samtykke fra pasienten så lenge behandlingen varer.

4.2.3 Pasientens rett til informasjon

En av de sentrale rettighetene for pasienten er retten til informasjon og innsyn, jf. GDPR art. 13-15. Hvis det er vanskelig å få den registrertes samtykke kan personopplysninger samles inn og behandles gitt at visse vilkår blir oppfylt. Et av vilkårene er at pasienten informeres om mulig bruk av hans eller hennes opplysninger til et konkret sekundærbruk, jf. GDPR art. 13 og at pasienten ikke motsetter seg behandlingen. Pasienten har rett til å protestere eller «right to opt out».[87]

Tilfeller hvor det vil være umulig å få pasientens samtykke er hvis pasienten er død eller ikke er i stand til å samtykke. Pasienter kan være bevisstløse, barn eller ha nedsatt funksjonsevne. Dersom informert samtykke skulle gjelde for all behandling av helseopplysninger ville forskningsresultater gi et skjevt bilde fordi ikke alle pasienter ville blitt representert. Skillet vil også ekskludere grupper som oppfattes som svakere eller vanskeligstilte i samfunnet. Personer som ikke kan gi samtykke får ikke ivaretatt sine rettigheter i like stor grad som de som har samtykkekompetanse. Dette bør databehandlere vise ekstra hensyn overfor.

Ved behandling i helseregistre er det av vesentlig betydning å vite hvor lenge personopplysningene blir oppbevart, om de blir oppbevart elektronisk eller i papirform. I tillegg ivaretas den registrertes rettigheter når den har oversikt over hvordan forskere og helsepersonell anvender opplysningene. Den registrerte må informeres på forhånd hvorvidt opplysningene vil bli oppbevart i helseregisteret i anonym, pseudonymifisert eller direkte identifiserbar form. Hvordan opplysningene presenteres i helseregisteret kan ha betydning for om pasienten samtykker til behandlingen eller ikke.

4.3 Behandlingsformer av personopplysninger

4.3.1 Direkte identifiserbare personopplysninger

Direkte identifiserbare personopplysninger er navn, identifikasjonsnummer som fødsels- eller personnummer eller andre personentydige kjennetegn, jf. GDPR art. 4 nr. 1. Det kan være nyttig for databehandler å ha identifiserbare opplysninger registrert.[88] Identifisering kan bidra til å kvalitetssikre helseregistre ved å sammenlikne opplysningene i ett register med et annet register. MSIS kan samkjøres med det nasjonale vaksineregisteret SYSVAK for å kartlegge eventuelle sammenhenger mellom hvem som blir smittet og hvem som ikke er vaksinert mot en type sykdom. Direkte identifisering gjør at opplysninger kan føres tilbake til den konkrete pasienten. Ved behandling kan identifiserbare personopplysninger skape risikoer ved inngrep i personvernet som

[87] Ploem (2006) s. 42.

[88] GDPR fortalepunkt 26.

skal vurderes nærmere i kapittel 6. I helseregistre med direkte identifiserbare personopplysninger stilles strenge krav til sikkerhet og personvern for å ivareta den registreres rettigheter og friheter.

4.3.2 Anonymisering av personopplysninger

Anonymisering innebærer å fjerne det identifiserbare i personopplysningene slik at opplysningene ikke kan lenger kan knyttes til en enkeltperson, se for eksempel MSIS-forskriften § 1-2a. Avidentifisering brukes for å innhente informasjon ved dataanalyse av helseopplysninger.[89] Dette bidrar også til å redusere risikoen for å krenke den registrertes rettigheter om personvern. Anonymiserte opplysninger anses ikke som personopplysninger i personvernforordningens forstand.[90] Rekkevidden av personopplysningsbegrepet blir dermed sentral for hvilke opplysninger som behøver personvern.

Omfanget av helsedata samt mer avansert analyseteknologi øker risikoen for reidentifisering. Avidentifisere opplysninger må kobles via en koblingsnøkkel for å reidentifisere opplysningene til en person. For å redusere risikoen bør det utføres grundige risikovurderinger før opplysningene anonymiseres og gjøres tilgjengelig.[91] Behandlingsansvarlig må vurdere om interne eller eksterne aktører vil ha stor nytte av personopplysningenes verdi. For å avgjøre om det foreligger en slik risiko må det tas hensyn til hvor sensitive opplysningene er og hva slags type personopplysninger det er tale om. Ettersom anonyme opplysninger ikke er personopplysninger foreligger det ikke behov for strenge krav til sikkerhet og personvern for å ivareta den registrertes rettigheter og friheter etter anonymisering.

4.3.3 Pseudonymisering

Et pseudonym forklares som et dekknavn hvor formålet er å skjule identiteten til personen, se GDPR art. 4 nr. 5. Identiteten skjules bak et pseudonym for at verken helsepersonell eller forskere skal vite hvem opplysningene tilhører ved behandling i helseregistre.[92] Hvert pseudonym har en unik indikator. Pseudonymisering ivaretar pasientens personvern i større grad enn direkte identifisering.[93]

Derimot kan det hevdes at pseudonymisering er en form for personidentifikasjon på samme måte som personidentifiserbare registre.[94] Bruk av rask utviklingsteknologi i behandling i helseregistre vil vise om personvernforordningen setter strenge nok juridiske rammer for å samle sensitive opplysninger i massedata på samme sted som ved en helseanalyseportal.

---

[89] Engelschiøn (2017) kommentar til § 2.
[90] GDPR fortalepunkt 26.
[91] Wessel-Aas (2018) s. 171.
[92] Prop. 72 L (2013-2014) s. 157.
[93] Prop. 72 L (2013-2014) s. 157.
[94] NOU 1993: 22 s. 228.

Bruk av pseudonymisering kan være en måte å ivareta interessen for personvern, forskning og helsevern samtidig. Likevel vil det være enklere å finne identiteten til tross for bruk av pseudonymer. Jo større datamengde som er lagret om en pasient, desto nærmere er det mulig å finne identiteten til tross for bruk av pseudonymer.[95]

I forarbeidene til tidligere helseregisterlov[96] uttalte Stortinget at målet er å bruke registerløsninger som ivaretar hensynet til folkehelsen samtidig som det ikke går utover hensynet til personvernet. Interesseavveiningen mellom helsevern og personvern har pågått i flere tiår. Til tross for at dette er eldre forarbeider har de rettskildemessig vekt idet forarbeidene har bidratt til å legge grunnlag for ulike behandlingsformer som brukes i helseregistre i dag.

4.4 Ivaretakelse av den registrertes rettigheter ved brudd på sikkerheten

For å ivareta den registrertes rettigheter ved sikkerhetsbrudd må en vite hva som kjennetegner et sikkerhetsbrudd. Et brudd på sikkerheten defineres vidt i GDPR art. 4 nr. 12. Et brudd kan være «tap, endring, uautorisert utlevering av eller tilgang til personopplysninger».

I Personvernnemnda har det blitt avsagt seks saker i 2013 om uautorisert uthenting av helseopplysninger gjennom leverandørs fjerntilgang. Disse er PVN-2013-05, 08, 09, 10, 11 og 12. I behandlingen av helseopplysninger brukte flere sykehus en type maskin som var koblet til internett. Personopplysninger ble via internett automatisk sendt til leverandøren i USA. Uthenting av personopplysninger til pasientene var ikke avtalt. Det følger ingen varslingsplikt for slik uthenting etter ordlyden til hregl. § 23 nr. 3 og 5, jf. tidligere personopplysningsloven 2000 § 19 bokstav c og e. Det sentrale spørsmålet i sakene var om det kunne gjøres en utvidende tolkning for å pålegge en varslingsplikt til pasienter hvor utlevering allerede har skjedd. Etter en interesseavveiing la Personvernnemda til grunn at det forelå rettslig grunnlag for å pålegge sykehuset en varslingsplikt i disse sakene.

Et grunnprinsipp i personvernregelverket er rett til å kontrollere opplysninger om seg selv. Dersom det ikke er mulig, må den registrerte få informasjon om behandlingsprosessen. Avgjørelsene viser at teknologisk utvikling og automatisering av dataprosesser kan føre til helseopplysninger på avveie. Som følge av at alle avgjørelsene kom fram til samme konklusjon kan disse anses å ha rettskildemessig vekt i vurderingen av den registrertes rettigheter og friheter etter problemstillingene.

[95] St.meld. nr. 43 (2003-2004) s. 24.
[96] Innst.O. nr. 62 (2000-2001) kapittel 2.1.

Ved sikkerhetsbrudd eller avvik i systemet kan personopplysninger komme på avveie. Dersom den registrertes opplysninger blir lagret av en uautorisert person kan det skje et inngrep i den registrertes rett til personvern.[97] Sikkerhetsbruddet medfører risiko for den registrertes rettigheter og friheter som kan svekkes ved identitetstyveri. Dersom taushetsbelagte helseopplysninger blir spredt på internett kan det både gi økonomiske og sosiale ulemper for den registrerte.

Behandlingsansvarlig må vurdere sannsynligheten for at et sikkerhetsbrudd innebærer en risiko for den registrertes rettigheter.[98] I risikovurderingen skal det for det første tas stilling til hvilket sikkerhetsbrudd som foreligger, for eksempel tap av opplysninger eller integritetskrenkelse. For det andre skal opplysningenes art og omfang vurderes. For det tredje skal den konkrete risikoen identifiseres. For det fjerde er det sentralt å overveie hvilke virkninger sikkerhetsbrudd kan medføre for den registrerte. Dersom det er tale om en pasient som fortsatt får helsebehandling må det vurderes om sikkerhetsbruddet kan gå utover den videre helsehjelpen. For det femte må behandlingsansvarlig vurdere om bruddet omfatter særlige utsatte grupper som barn eller personer med nedsatt funksjonsevne.

Til slutt er det vesentlig å få oversikt over hvor mange fysiske personer som er rammet av sikkerhetsbruddet. I Helse Sør-Øst-tilfellet ble 2,8 millioner mennesker rammet av sikkerhetsbruddet. Antall rammede personer tilsvarer halve Norges befolkning og var derfor et særlig grovt brudd på norske pasienters rettigheter og friheter. Ved bruk av digitale tjenester er det nesten umulig å verne seg helt mot sikkerhetsbrudd. Et annet tilfelle hvor personopplysninger kom på avveie var et dataangrep mot Facebook i 2017 der opptil 50 millioner Facebook-brukere ble rammet.[99] Hendelsen tyder på at personvernet for brukernes personopplysninger var i liten grad beskyttet.

I takt med den teknologiske utviklingen blir også metoder for dataangrep som svekker den registrertes personvern mer avanserte. Pasienter har blitt en gruppe registrerte som er utsatt for brudd på retten til personvern.[100] Samtidig utvikles bedre sikkerhetsmetoder for å unngå hackerangrep og andre avvik i digitale tjenester som helseregistre. Dette krever imidlertid at behandlingsansvarlig og utviklere av digitale tjenester tar den registrertes personvern på alvor.

I dette kapittelet har det blitt vurdert i hvilken grad den registrertes rett til personvern blir ivaretatt ved behandling av personopplysninger i helseregistre. Det stilles krav til behandling om for eksempel samtykke og at pasienten får kontroll over egne personopplysninger eller informasjon om behandlingen. Personopplysninger kan oppbevares i ulike identifikasjonsformer som ivaretar den

[97] Region Sjælland (2018) s. 3.
[98] Region Sjælland (2018) s. 3.
[99] Høgseth (2018).
[100] Wierda (2018) s. 240.

registrertes rett til personvern i ulik grad. Pseudonymisering er identifikasjonsformen som utsetter den registrerte for minst mulig risiko for inngrep, men anvendes ikke så mye i sentrale helseregistre. Behandlingsprosessen i helseregistre viser at det tas hensyn til den registrertes rett til personvern. Dersom nytteverdien for helseforskning eller kvalitetssikring for helsetjenestene er større enn personvernulempen, kan personopplysningene behandles.

5 BEHANDLING AV HELSEOPPLYSNINGER I SAMSVAR MED PERSONVERNPRINSIPPENE

I dette kapittelet vurderes hvordan grunnprinsippene etter GDPR art. 5 oppfylles ved behandling av personopplysninger i helseregistre. Det må således tas stilling til hvilke personvernkonsekvenser som oppstår i behandlingen. Det avgrenses mot andre bestemmelser i personvernforordningen og rettes oppmerksomhet mot grunnprinsippene i GDPR art. 5.

5.1 Oversikt over prinsipper for behandling

Ved behandling av personopplysninger i helseretten må databehandler overholde visse generelle prinsipper for personvern. GDPR art. 5 oppstiller grunnprinsipper som gjelder for all behandling av personopplysninger. Bestemmelsen er i stor grad en videreføring av EUs tidligere personverndirektiv art. 6 og personopplysningsloven 2000 § 11 (1).[101] Det er likevel noen vesentlige endringer og presiseringer av prinsippene som har større betydning i dagens samfunn enn tidligere. Målene og prinsippene fra EUs tidligere personverndirektiv gjelder fortsatt i personvernforordningen.[102] Likevel skal personvernforordningen i større grad enn EU-direktivet hindre en fragmentert oppfatning av vernet av personopplysninger og skape rettslig sikkerhet.[103]

Prinsippene skaper klare rammer for tolkning av personvernforordningens øvrige bestemmelser og annen regulering av personopplysninger. Når det skal avgjøres hvorvidt helseopplysninger kan behandles i helseregistre etter hregl. § 6, jf. § 9 må behandling skje i samsvar med prinsippene i GDPR art. 5. EU- og EØS-land har etter personvernforordningen handlingsrom til å gi nasjonal særlovgivning på helseområdet.[104] Regler for behandling av helseopplysninger bør imidlertid ikke hindre fri flyt av personopplysninger relatert til helse i EU og EØS-området.[105] Heretter redegjøres det for innholdet av de ulike prinsippene som fremgår av GDPR art. 5 nr. 1-2 med utgangspunkt i helseopplysninger.

5.2 Lovlighet, rettferdighet og åpen behandling

For å kunne behandle helseopplysninger må behandlingen være «lovlig», «rettferdig» og «åpen» for den registrerte, jf. GDPR art. 5 nr. 1 bokstav a.

[101] Innst. 278 L (2017-2018) s. 2.
[102] GDPR fortalepunkt 9.
[103] GDPR fortalepunkt 10.
[104] GDPR fortalepunkter 10 og 53.
[105] GDPR fortalepunkt 53.

Ordlyden av «lovlig» tolkes slik at det må foreligge et rettslig grunnlag. Behandlingsgrunnlag er uttømmende regulert i GDPR art. 6, 9 og 10. Det rettslige grunnlaget må innfri kravene etter EMK art. 8 om nødvendighet og angitt formål. I norsk rett stilles det på samme måte krav til lovhjemmel for å behandle helseopplysninger. For å innfri kravene etter prinsippene er det nødvendig at rettsgrunnlaget er klart. Jo mer inngripende behandlingen er, desto høyere krav bør det stilles til tydelig rettsgrunnlag.[106]

Enhver behandling må ha behandlingsgrunnlag etter GDPR art. 6 nr. Forbudet mot behandling av særlige kategorier tillater behandling dersom et av vilkårene i GDPR art. 9 nr. 2 er oppfylt. For behandling av helseopplysninger som er basert på samtykke er rettsgrunnlaget GDPR art. 6 nr. 1 og art. 9 nr. 2 bokstav a. En vesentlig endring er at behandlingsansvarlig må selv vurdere om behandlingen er tillat etter lovbestemmelsene. Som hovedregel krever gjenbruk av helseopplysninger et gyldig samtykke eller hjemmel i lov, jf. GDPR art. 6 nr. 4. Dersom det ikke foreligger et behandlingsgrunnlag kan bare opplysningene gjenbrukes til forenlige formål.

De fleste helseregistre kan behandle helseopplysningene basert på hjemmel i hregl. § 6 som viser til at prinsippene i GDPR art. 5. Lovbestemte helseregistre kan opprettes ved forskrift om behandling av helseopplysninger som er direkte identifiserbare, jf. hregl. § 11 (1), se § 8. Disse opplysningene kan behandles uten den registrertes samtykke hvis det er nødvendig for å oppnå formålet med helseregisteret. Det rettslige grunnlaget for behandling av helseopplysninger fastsatt i unionsretten eller medlemsstatenes nasjonalrett, jf. GDPR art. 9 nr. 4 kan også være det rettslige grunnlaget for viderebehandling, for eksempel gjenbruk av helseopplysninger til styring og beredskap.[107]

Videre må behandlingen være «rettferdig», jf. GDPR art. 5 nr. 1 bokstav a. Sammenhengen mellom innsamling av opplysningene og formålet for behandlingen må fremstå som rimelig for den registrerte.[108] Dette innebærer at den registrerte oppfatter det som forståelig og naturlig at den aktuelle behandlingsansvarlige behandler de konkrete opplysningen for det aktuelle formålet, ettersom helseopplysninger trenger et sterkere vern.[109] Pasienter skal få tydelig informasjon om i hvilket omfang personopplysningene behandles eller skal behandles.[110] Innsamling av helseopplysninger gjøres hovedsakelig ved at helsepersonell stiller pasienten spørsmål om personopplysninger og noterer dem i pasientjournalen. Andre helseopplysninger innsamles etter undersøkelse ved for eksempel blodprøve eller gynekologisk undersøkelse. Prinsippet om rettferdig

[106] Skullerud (2018) s. 75.
[107] GDPR fortalepunkt 50.
[108] GDPR fortalepunkt 39.
[109] GDPR fortalepunkt 53.
[110] GDPR fortalepunkt 39.

behandling er nært knytte til åpenhetskravet. Ut fra lovtolkningen lagt til grunn i *Nowak* taler det for at pasienter på lik linje skal ha større innsynsrett.

Deretter må behandlingen være «åpen», jf. GDPR art. 5 nr. 1 bokstav a. Med «åpen» menes at behandlingen er transparent for den registrerte. Pasienten burde forstå og forutse hvordan behandlingen blir. Bakgrunnen for regelen er at pasienten skal kunne innrette seg etter behandlingen og ha tillit til behandlingsprosessen. Et sentralt moment er at den registrertes rett til informasjon har blitt styrket ved gjennomføringen av personvernforordningen.[111] Informasjonskravet kan opprettholdes ved å den registrerte innsyn i behandlingen og bli informert ved eventuelle sikkerhetsbrudd, jf. GDPR art. 14 og 34.

5.3 Formålsbegrensning

Et sentralt prinsipp for behandling av helseopplysninger er prinsippet om formålsbegrensning etter GDPR art. 5 nr. 1 bokstav b. Prinsippet går ut på at innsamling og behandling av opplysningen kan kun gjøres i den grad det er gjort for «spesifikke, uttrykkelig angitte og berettigede formål» i følge GDPR art. 5 nr. 1 bokstav b.

Unntaksvis kan pasientens opplysninger gjenbrukes uten samtykke hvis det er nødvendig for å nå formålet helseregisteret. Formålsbegrensningen er en videreføring av kravet etter personopplysningsloven 2000 § 11 (1) bokstav b. For å oppfylle prinsippet om formålsbegrensning oppstilles det seks vilkår i GDPR art. 5 nr. 1 bokstav b som redegjøres for nærmere under.

For det første har formålet betydning når det trekkes opp en rettslig ramme for den aktuelle behandlingen av helseopplysninger. Formålet angir rekkevidden for hvilken behandling den registrerte har samtykket til, hvilke opplysninger som kan lovlig behandles, når behandlingen skal avsluttes og hvilke operasjoner som kan anses å utgjøre samme behandling.[112] Formålet skal være førende for hvilke rettsregler som kommer til anvendelse i behandlingen.[113] Helseregisterloven er rettslig grunnlag ved behandling av helseopplysninger til analyse, jf. hregl. § 1. Dersom helseopplysninger samles inn til forskningsformål gjelder helseforskningsloven i stedet, jf. hforsknl. § 2. En pasient samtykker til spesifikke behandlingsaktiviteter av sine helseopplysninger. Formålet med behandling kan være førende for hvilke behandlingsaktiviteter et samtykke gjelder for.

For det andre må formålet være spesifikt, jf. GDPR art. 5 nr. 1 bokstav b. Overordnede formål som kvalitetsforbedring av helsehjelp må konkretiseres til andre formål. For eksempel må det være tydelig ut fra formålet å finne årsaker til konkrete sykdommer og måle effekten av behandling og

[111] GDPR fortalepunkt 39.
[112] GDPR fortalepunkt 45.
[113] Skullerud (2018) s. 76.

kvalitet på helsetjenestene. For å være tilstrekkelig spesifikt må det være mulig ut i fra formålet å vurdere om de registrertes opplysninger er nødvendige ved å etterprøve om behandlingen skjer i samsvar med personopplysningslovens øvrige bestemmelser.

For det tredje er ikke vilkåret om konkrete formål absolutt. Mindre konkrete formål for behandling har vært tillatt innen helseforskning i Norge, jf. hforsknl. § 1. Det kan gis et «bredt samtykke» til helseforskning, jf. hforsknl. § 13, se § 14. Det er adgang til å gi samtykke til forskning på de forskningsområdene som samsvarer med anerkjente etiske forskningsprinsipper.[114]

For det fjerde må formålet være uttrykkelig, jf. GDPR art. 5 nr. 1 bokstav b. Med dette menes at formålet må formidles tydelig allerede når helseopplysningene samles inn.[115] Det er ikke tilstrekkelig at databehandleren regner med at den registrerte har fått med seg formålet.

For det femte bør formålet være berettiget. Å være berettiget innebærer at behandlingen er legitimt ved å samsvare med annet regelverk og ivaretar andre samfunnskrav.[116] Formålet må være saklig begrunnet av den behandlingsansvarliges virksomhet. For eksempel må Helsedirektoratet som er behandlingsansvarlig for Nasjonalt pasientregister sørge for at formålet om behandling om de spesifikke helseopplysningene er saklig begrunnet. Dette innebærer at formålet må tilsvare hva som normalt kan forventes i en helsetjenestevirksomhet.

Til sist fremgår det av GDPR art. 5 nr. 1 bokstav b at helseopplysninger ikke kan behandles på nytt til uforenlige formål med det opprinnelige formålet for innsamlingen. Bestemmelsen viderefører norsk rett etter personopplysningsloven 2000 § 11 (1) bokstav c. Formål som ikke anses som uforenlige formål er fremtidig behandling i offentlige arkiv, vitenskapelig eller historisk forskning eller statistisk bruk i tråd med GDPR art. 89 nr. 1. Bestemmelsen stiller krav til behandlinger for at disse formålene skal samsvare med personvernforordningens øvrige bestemmelser.

I høyesterettsavgjørelsen *Avfall* inntatt i Rt. 2013 s. 143 ble den tidligere praksisen til Personvernnemnda for gjenbruk av personopplysninger til nye formål innstrammet av Høyesterett. Saken gjaldt en sjåfør som ble oppsagt etter at innleverte timelister ikke samsvarte med GPS-loggen. Avfallsservice AS brukte opplysningene fra kjøretøyenes GPS-systemer til å kontrollere arbeidstakernes arbeidstid. Høyesterett skulle ta stilling til om opplysningene fra GPS-loggen var brukt i strid med kravene etter personopplysningsloven 2000 § 11 (1) bokstav c. Bestemmelsen gikk ut på at opplysninger ikke kan brukes til uforenlige formål med innsamlingsformålet uten samtykke

[114] GDPR fortalepunkt 33.
[115] GDPR fortalepunkt 39.
[116] Skullerud (2018) s. 76.

fra den registrerte. Høyesterett besluttet at det ikke var tilstrekkelig at den nye bruken av opplysningene oppfyller kravene i personopplysningsloven § 11 (1) bokstav c, men §§ 8 og 9 må også tilfredsstilles, se *Avfall* avsnitt 48.[117] Sammenstillingen var brukt i strid med kravene og hadde ikke grunnlag i personopplysningsloven § 11 (1) bokstav c.

Avfall vil ikke være fullt ut egnet etter personvernforordningen. Personvernforordningen stiller krav til at all bruk av personopplysninger til nye formål må ha et selvstendig grunnlag i personvernforordningen. Dette kan være rettslig grunnlag som følger av GDPR art. 6 nr. 1 bokstav a-f. Dersom ingen av rettsgrunnlagene er oppfylt, kan ikke personopplysninger anvendes til nye formål.

5.4 Dataminimering

GDPR art. 5 n. 1 bokstav c oppstiller et prinsipp om dataminimering. Prinsippet går ut på at helseopplysninger kan innsamles og behandles dersom de er adekvate, relevante og begrenset til det som er nødvendig for formålet.[118] Helseopplysninger og behandlingsmetoden av helseopplysningene må være nødvendige for å oppnå det spesifikke formålet. Ordlyden i bestemmelsen er snevrere enn ordlyden i hregl. § 6 (3) bokstav a.[119] I norsk rett oppfattes innholdet av «tilstrekkelig» som et krav om at opplysningsgrunnlaget må være fullstendig slik som behandlingsformålet krever.[120] Sammenlignet forstås det danske begrepet «tilstrækkelige» etter forarbeidene til personopplysningsloven 2000 som at det ikke må samles inn flere opplysninger enn påkrevd for å kunne oppnå formålet.[121] Utfordringen med en slik tolkning er at vilkåret kan trekke i retning av å være et krav om flere opplysninger, og ikke en minimering som følger av prinsippet.

Dataminimeringsprinsippet kalles for et forbud mot behandling av overskuddsinformasjon.[122] Andre helseopplysninger som er overflødige for å oppnå formålet regnes som overskuddsinformasjon. Det samme gjelder hvis formålet kan oppnås med anonyme opplysninger i stedet for direkte identifiserbare personopplysninger. Registrering av en pasients helseopplysninger skal begrenses til hva som er nødvendig. Prinsippet om dataminimering kommer også til uttrykk i GDPR art. 11 hvor den behandlingsansvarlige ikke må beholde identifiserbare opplysninger bare for å oppfylle den registrertes rettigheter. Krav om dataminimering kan også ses i sammenheng med GDPR art. 25 hvor den behandlingsansvarlige skal ordne innebygd personvern ved behandling av personopplysninger i helsetjenesten.

---

[117] Se også Ot.prp. nr. 92 (1998-1999) s.112-113.

[118] GDPR fortalepunkt 39.

[119] Datatilsynet (2018) s. 5.

[120] Ot.prp.nr. 92 (1998-1999) s. 114.

[121] Blume (2018) s. 73.

[122] Skullerud (2018) s. 77.

Etter EUs tidligere personverndirektiv art. 6 nr. 1 bokstav c at skulle personopplysningene være «adekvate, relevante» og ikke for omfattende i forhold til det opprinnelige formålet. Ut i fra dette kan EU-direktivet anses for å ha gitt mer uttrykk for prinsippet om dataminimering enn de norske bestemmelsene i personopplysningsloven 2000. Ettersom personvernforordningen ble gjennomført som norsk lov i år vil situasjonen trolig endre seg.

Spørsmål om prinsippene om dataminimering og formålsbegrensning ble reist i EU-domstolen i en avgjørelse inntatt i C-293/12. Saken gjaldt de nevnte prinsippene etter datalagringsdirektivet.[123] Et av spørsmålene var om lagring av data var egnet til å gjennomføre formålet som følger av datalagringsdirektivet, se C-293/12 premiss 49. Retten kom fram til at dataopplysningene som lagres i medhold av datalagringsdirektivet må ses i sammenheng med den økende grad av betydning for elektronisk kommunikasjonsmidler. Lagring av data vil gi kompetente nasjonale myndigheter tilgang til opplysninger og er dermed et brukbart redskap i etterforskning av straffesaker. Retten fremhevet i C-293/12 premiss 49 at lagring av slik data kan likevel være egnet til å gjennomføre målet som følger av datalagringsdirektivet. Retten hevdet dermed at personopplysninger som var pålagt lagret etter datalagringsdirektivet oppfylte formålet i seg selv.

Videre drøftet retten spørsmålet om lagring av opplysninger var nødvendig for formålet om kriminalitetsbekjempelse, se C-293/12 premiss 56. Retten la avgjørende vekt på at datalagringsdirektivet forutsatte lagring av kommunikasjonsopplysninger om alle borgere. Retten la til grunn at dette var for bredt og dermed ikke tilfredsstilte kravet til dataminimering. Samlet sett utgjorde datalagringen et uforholdsmessig inngrep overfor borgene.

Saken gjaldt bruk av opplysninger lagret via elektroniske kommunikasjonsmidler som kunne bidra i straffesaker. Dermed har ikke saken direkte overføringsverdi til behandling av helseregistre. Likevel viser avgjørelsen et eksempel på virkeområdene til prinsippene om dataminimering og formålsbegrensning. Dommen anerkjenner at risikoen ved behandling med aggregerte metadata kan tilrettelegge for å trekke svært konkrete konklusjoner om den registrertes privatliv, se C-293/12 premiss 27. Dommen er imidlertid noe mangelfull fordi den ikke stiller spørsmål om hvorfor det er hensiktsmessig med datalagring som et middel for å bekjempe alvorlig kriminalitet, se C-293-12 premiss 49.

5.5 Riktighet

I følge GDPR art. 5 nr. 1 bokstav d skal helseopplysningene være «korrekte» til enhver tid. Dersom endringer forekommer, skal helseopplysningene også oppdateres. Behandlingsansvarlig for prosessen har ansvar for at ukorrekte helseopplysninger blir rettet ellet slettet uten ugrunnet

[123] Dir. 2006/24/EF.

opphold.[124] Prinsippet om riktighet gjengis også i GDPR art. 16 om å få opplysningene rettet og art. 18 nr. 1 bokstav a om en begrenset behandling dersom den registrerte mener at enkelte personopplysninger ikke stemmer. Prinsippet ble innført i norsk rett etter personopplysningsloven 2000 § 11 (1) bokstav e, jf. §§ 27 og 28. I tilfeller hvor det skal treffes tiltak eller fattes beslutninger for videre helsehjelp er det særlig sentralt at helseopplysningene er oppbevart riktig i helseregisteret. Reglene skal sikre at den registrertes rettigheter ivaretas i samsvar med resten av personvernforordningen ved blant annet å få rettet og slettet uriktige helseopplysninger.[125]

For å sikre at helseopplysningene er korrekte er det hensiktsmessig at den registrerte selv har adgang til å kontrollere og rette opplysningene. I dag er det enklere for pasienter å gjennomføre egenkontroll. Nettsiden www.helsenorge.no gir innsyn i egne personopplysninger i de ulike helseregistrene. Slike innloggingsløsninger er ofte sikret ved at den registrerte må verifisere identiteten sin. Verifiseringen kan gjøres ved hjelp av biometriske opplysninger som bruk av fingeravtrykk på smarttelefon eller to-faktoridentifisering på to ulike digitale kanaler. Ved å åpne for at den registrerte kan kontrollere og rette egne opplysninger, legges ansvaret i større grad på den registrerte.

5.6 Lagringsbegrensning

GDPR art. 5 nr. 1 bokstav e viser til et forbud mot å behandle helseopplysninger som er identifiserbare lengre enn nødvendig for formålet.[126] Ordlyden tilsier at prinsippet om lagringsbegrensning setter en tidsramme for hvor lenge den behandlingsansvarlige kan oppbevare helseopplysningene. Forbudet innebærer at opplysningene skal slettes eller anonymiseres når formålet er oppnådd eller det kan oppnås uten at opplysningene er personidentifiserbare.[127] Prinsippet kan ses i sammenheng med nødvendighetskravet i hregl. § 6 (1) hvor graden av personidentifikasjon skal begrenses til hva som er nødvendig for formålet. Sletteplikten eller plikten til å anonymisere etter personvernforordningen kan inntreffe før behandlingsformålet oppnås.[128] Det er noe betenkelig at personvernforordningen inneholder få tidsfrister. Det fremgår ikke av GDPR art. 5 nr. 1 bokstav hvor lang tid det kan gå før en personopplysning må slettes.[129]

For å sikre de registrertes personvern er det en forutsetning at det settes i gang nødvendige tekniske og organisatoriske tiltak.[130] For å oppnå dette må prinsippet om dataminimering også oppfylles. Nødvendige tiltak kan være pseudonymisering av opplysningene eller særskilte sikkerhetstiltak for å sikre opplysningenes konfidensialitet. I lys av at prinsippet om dataminimering er en videreføring av

[124] GDPR fortalepunkt 59.
[125] GDPR fortalepunkt 59.
[126] GDPR fortalepunkt 39.
[127] Skullerud (2018) s. 78.
[128] GDPR fortalepunkt 65, jf. 26.
[129] Wessel-Aas (2018) s. 128.
[130] GDPR fortalepunkt 156.

tilsvarende prinsipp i EUs tidligere personverndirektiv har tidligere avgjørelser relevans for fortolkningen av innholdet i prinsippet. I saken inntatt i C-553/07 fremhevet EU-domstolen at den behandlingsansvarlige har mulighet til å lagre ulike personopplysninger for ulike tidsrom. Saken gjaldt personopplysninger om den registrertes navn og adresse, se C-553/07 premiss 33, jf. 66. Spørsmålet var om personopplysningene kunne lagres over en lengre periode.

5.7 Integritet og konfidensialitet

Prinsippet om sikring av integritet og konfidensialitet følger av GDPR art. 5 nr. 1 bokstav f. Integritet kan forklares som en persons selvstendige og ukrenkelige individualitet. Pasienter er i en sårbar situasjon når de oppsøker helsehjelp. Det er særlig behov for å sikre at integriteten ivaretas når pasienten gir fra seg sensitiv informasjon. Konfidensialitet kan betegnes som at fortrolig informasjon ikke bør deles videre. Helsepersonell har taushetsplikt til ikke å meddele sensitiv informasjon med mindre det er gitt samtykke, jf. hpl. § 21.

Prinsippet om integritet og konfidensialitet skal sikre at helseopplysninger behandles i samsvar med GDPR art. 32 om sikkerhet ved behandling. For å opprettholde sikkerheten og hindre behandling av helseopplysninger i strid med personvernforordningen bør behandlingsansvarlig vurdere risikoer med behandlingen og gjennomføre tiltak for å begrense risikoene.[131] Grunnprinsippet om integritet og konfidensialitet verner mot uautorisert eller ulovlig innsyn av behandlingen. Prinsippet skal beskytte mot «utilsiktet tap», «ødeleggelse eller skade» av helseopplysningene som noen av risikoene nevnt i GDPR art. 5 nr.1 bokstav f. Tekniske og organisatoriske sikkerhetstiltak begrenser hvem som har tilgang til opplysningene. Loggføring i informasjonssystemene kan benyttes ved behandling av helseopplysninger.

5.8 Ansvar

5.8.1 Behandlingsansvarliges plikter

Etter GDPR art. 5 nr. 2 stilles behandlingsansvarlige til ansvar for oppfyllelse av grunnprinsippene om behandling av personopplysninger i nr. 1 blir oppfylt. I personvernforordningen blir prinsippet om ansvarlighet kalt «accountability». Begrepet går ut på at en person eller en bedrift tar risikoen for behandlingen og skal ta ansvar dersom det foreligger avvik. Prinsippet er tydeligere i GDPR art. 5 nr. 2 enn i EUs tidligere personverndirektiv art. 6. Plikten innebærer at behandlingsansvarlig skal påvise at prinsippene i GDPR art. 5 nr. 1 etterleves. Den behandlingsansvarlige bør føre internkontroll for å påvise behandling i helseregistre.

Internkontroll gir oversikt over hvilke opplysninger som blir behandlet til hvilke formål og hvordan de behandles. Som vist i punkt 5.3 kan enkelte formål med helseregistre være for generelle til den konkrete behandlingen. I tilfeller hvor det er uklart hvorvidt det generelle formålet dekker

[131] GDPR fortalepunkt 83.

behandlingen må behandlingsansvarlig ta stilling til om formålet med gjenbruk av helseopplysninger må spesifiseres i større grad. Etterkontroll av behandlingen kan bidra til å lukke eventuelle sikkerhetshull som ikke ble oppdaget under behandlingen. Videre kan etterkontroll sørge for at alle prinsippene etter GDPR art. 5 nr. 1 er ivaretatt for den registrerte.

Prinsippet om ansvarlighet innebærer ytterligere at tilsynsmyndigheter skal i begrenset grad forhåndsgodkjenne behandling av helseopplysninger. Plikten har i liten grad bidratt til å forbedre vernet av personopplysninger og har medført en administrativ og økonomisk byrde.[132] I visse tilfeller er det nødvendig å konsultere og få godkjenning av tilsynsmyndighetene etter GDPR art. 5 nr. 1.

Samlet sett er grunnprinsippene etter GDPR art. 5 er sentrale for forståelsen om reglene om behandling av personopplysninger i helseregistre. I samsvar med at helsehjelp utvikler seg oppstår det større behov for å opprette nye helseregistre eller gjøre nye behandling er av allerede registrerte helseopplysninger slik at personopplysninger tilgjengeliggjøres i større grad. Bakgrunnen for å vedtak personvernforordningen er blant annet at hensynet til personvern og dens grunnprinsipper blir gradvis tillagt mindre vekt. Det må foretas en konkret vurdering ved for eksempel gjenbruk av helseopplysninger hvorvidt grunnprinsippene oppfylles i tilstrekkelig grad.

5.8.2 Vurdering av personvernkonsekvenser i helseregistre

Personvernforordningen gir klare regler for hvilken tilsynsmyndighet som skal lede vurdering av personvernkonsekvenser, I den engelske versjonen av personvernforordningen kalles dette Data Protection Impact Assessment (DPIA), jf. GDPR art. 35. Den ansvarlige for DPIA velges etter lokalisering og organisasjonen til virksomheten til den behandlingsansvarlige. Behandling av personopplysninger i helsetjenesten kan medføre en høy risiko for den registrertes rettigheter og friheter som pasient. For å avgjøre om det foreligger høy risiko er analysemetoden DPIA et nyttig verktøy.

Behandling av personopplysninger med bruk av ny teknologi bør ta hensyn til følgende momenter. Det bør tas hensyn til behandlingens art, omfang, formål og konteksten behandlingen utføres i, jf. GDPR art. 35. Hvis de nevnte momentene trekker i retning av at behandlingen medfører en høy risiko for den registrertes rettigheter og friheter må den behandlingsansvarlige vurdere hvilke personvernkonsekvenser som kan oppstå.

En grunnleggende forutsetning for å behandle personopplysninger i helsetjenesten er at prinsippene etter GDPR art. 5 oppfylles. Kravet om vurdering av personvernkonsekvenser, jf. GDPR art. 35 er ny i personvernregelverket. Datatilsynet har derimot anbefalt en slik vurdering i tilknytning til innebygd

[132] GDPR fortalepunkt 89.

personvern. Anbefalingen må nå følges av helsevirksomhetene som ønsker å behandle helseopplysninger i analyser og for å forbedre kvaliteten til helsebehandling.

6 ANALYSE AV UTVALGTE HELSEREGISTRE

6.1 Utvalg og analysestrategi

I kapittel 3-5 er det redegjort for de tre problemstillingene på et generelt grunnlag. I kapittel 6 analyseres problemstillingene i to utvalgte helseregistre. Meldingssystem for smittsomme sykdommer og Hjerte- og karregisteret ble valgt for å gi et bilde av varierte helseopplysninger og ulik grad av sensitivitet. MSIS er interessant å undersøke på grunn av sin sensitive karakter og hva som er mulige konsekvenser dersom helseopplysningene ble misbrukt. Hjerte- og karregisteret er derimot interessant å undersøke ettersom det inneholder helseopplysninger om vanlige folkesykdommer i Norge. Helseregistrene analyseres i det følgende hver for seg under de tre problemstillingene.

6.2 Innholdet i MSIS og hjerte- og karregisteret

I det sentrale helseregisteret MSIS behandles helseopplysninger relatert til smittsomme sykdommer. Behandling av helseopplysninger i MSIS reguleres av MSIS-forskriften. Folkehelseinstituttet er behandlingsansvarlig for MSIS, jf. MSIS-forskriften § 1-5. Smittsomme sykdommer er av særlig sensitiv karakter og deles inn i tre kategorier i MSIS, se MSIS vedlegg I. I gruppe A samles særlig smittefarlige sykdommer som meslinger. Seksuelt overførbare sykdommer samles i gruppe B. Andre mindre smittefarlige som influensalignende sykdommer kategoriseres i gruppe C. Folkehelseinstituttet kan inngå skriftlig avtale med helseforetak om innsamling og behandling av helseopplysninger i MSIS, jf. MSIS-forskriften § 1-6 (1).

I hjerte- og karregisteret behandles helseopplysninger relatert til hjertesykdommer som hjertekrampe, hjerteinfarkt og hjerneslag. Behandling av helseopplysninger i hjerte- og karregisteret reguleres av hjerte- og karregisterforskriften. I likhet med MSIS er Folkehelseinstituttet behandlingsansvarlig for hjerte- og karregisteret, se hjerte- og karregisterforskriften § 1-3 (1). Det sentrale helseregistre består av et basisregister og tilknyttede medisinske kvalitetsregistre, jf. hjerte- og karregisterforskriften § 1-1 (1). Folkehelseinstituttet kan inngå skriftlig avtale med helseforetak om innsamling og behandling i følge hjerte- og karregisterforskriften § 1-3 (2).

6.3 Vurdering av behandlingens risiko for innskrenkning i personers rettigheter og friheter (I)

6.3.1 Meldingssystem for smittsomme sykdommer (MSIS)

Ved gjenbruk av personopplysninger registrert i MSIS oppstår en risiko for den registrertes rettigheter og friheter siden opplysningene er av særlig sensitiv karakter. Sammen med helseopplysninger relatert til sykdommen kan også andre opplysninger indirekte registreres, for eksempel informasjon om seksuell orientering eller en kvinnes fruktbarhet.

For helseopplysninger om seksuelt overførbare sykdommer er det viktig å ta hensyn til risikoer som oppstår. Det kan være en påkjenning for pasienten å oppgi helseopplysninger om seksuelt overførbare sykdommer til helsepersonell. Pasienten må kunne stole på at sine helseopplysninger som sammenstilles og gjenbrukes til nye formål ikke utsetter pasientens rettigheter for unødvendig risiko. Med hensyn til helseopplysningenes sensitivitet må behandlingsansvarlig sørge for den registrerte i MSIS får et sterkt vern.[133]

Bakgrunnen for å registrere personopplysninger i MSIS er å forebygge spredning av smitte og kontrollere smittsomme sykdommer i samsvar med formålet, jf. MSIS-forskriften § 1-3.[134] Smittevern er et viktig hensyn for å ivareta folkehelsen. Ved bruk av digitale plattformer kan smittsomme sykdommer kontrolleres mer effektivt ved å overvåke smittesituasjonen på landsbasis. Samtidig kan datasystemene raskere oppdatere store mengder helsedata og varsle hvis det er fare for helsesikkerheten. [135]

Registrering av smittsomme sykdommer og gjenbruk til helseforskning bidrar til mer kunnskap om sykdommene. Dersom befolkningen får tilstrekkelig informasjon om smittesykdommer kan det redusere stigma rundt seksuelt overførbare sykdommer. Digital behandling av personopplysninger i MSIS bidrar til enklere og mer effektiv gjenbruk av opplysningene.

Hensyn til mer kunnskap og tilgjengelighet kan neppe føre til at Folkehelseinstituttet kan se bort fra risikoer ved behandling for den registrertes rettigheter og friheter. Dersom et helsepersonell eller en databehandler bryter taushetsplikten knyttet til behandling i MSIS kan føre til store personlige konsekvenser for den registrerte. Den registrerte kan bli diskriminert på jobb eller taper sitt omdømme ettersom sykdommene er så stigmatisert. Derfor bør stilles ulik gradering av datasikkerhet ut fra hvilken gruppe sykdommen det gjelder. Samlet sett bør behandlingsansvarlig gjennomføre tiltak som minimerer risikoen ved behandling av helseopplysninger i MSIS.

Sikkerhetsbrudd kan føre til at helseopplysninger om seksuelt overførbare sykdommer blir kopiert. Dersom det først skjer et sikkerhetsbrudd kan det få store konsekvenser hvis datahackere får tilgang til koblingsnøkler for personopplysninger og avidentifiserte opplysninger. Det kan få store økonomiske konsekvenser for behandlingsansvarlig og tap av tillit fra pasienter og resten av samfunnet. Den registrerte utsettes for risiko av tap av omdømme, rett til privatliv og rett til personvern som grunnleggende rettigheter etter personvernforordningen.

[133] GDPR fortalepunkt 53.
[134] GDPR fortalepunkt 52.
[135] GDPR fortalepunkt 52.

Etter en gjennomgang av risikoer for innskrenkning i den registrertes rettigheter og friheter er det flere momenter som er sentrale. Samlet sett kan det oppstå en risiko for tap av tillit overfor helsetjenesten, men samtidig kan bruk av digitale plattformer gir mer effektivt og kontrollert behandling. Databehandling av helseopplysninger åpner for risikoer som uautorisert innsyn og sikkerhetsbrudd. Disse momentene bør tas i betraktning for vurderingene om behandling av personopplysninger i MSIS og risikovurdering etter GDPR art. 32 og personvernkonsekvenser, se art. 35. Lovendringer som følge av personvernforordning og endringer av helseregisterloven og MSIS-forskriften skal i større grad ivareta den registrertes rettigheter og friheter ved behandling av helseopplysninger og redusere risikoen for utilsiktede virkninger.

6.3.2 Hjerte- og karregisteret

Ved sammenstilling av helseopplysninger kan det oppstå risiko for innskrenkning i den registrertes rettigheter og friheter siden helseopplysninger i basisregisteret inneholder sammenstilte opplysninger fra Dødsårsaksregisteret, Norsk pasientregister og Folkeregisteret, jf. hjerte- og karregisterforskriften § 1-4. I tillegg jevnlig kobles helseopplysningene i basisregisteret med kvalitetsregistrene for å kvalitetssikre opplysningene.[136] Etableringen av helseregistret i seg selv dannet en risiko for at personopplysningene kunne komme på avveie eller bli misbrukt.[137] Det er behov for et nasjonalt register over hjertesykdommer og karlidelser fordi det inneholder helseopplysninger om alvorlige sykdommer som rammer mange. Å kartlegge helseopplysningene har nytteverdi for å forbedre helsebehandlingen og for å identifisere forebyggende tiltak.

Ved behandling av helseopplysninger er det nødvendig å ta stilling til hvor sensitive helseopplysninger er. Sammenlignet med smittsomme sykdommer anses ikke helseopplysninger i hjerte- og karregisteret like sensitive fordi de forbindes ikke med fordomsfullt. Årsaken til hjerte- og karsykdommer er imidlertid ofte forårsaket av høyt kolesterol, fedme og overvekt. Slike livsstilsykdommer kan være forbundet med fordommer. Likevel er dette ikke tilstrekkelig for at helseopplysningene anses å være av like sensitiv karakter som seksuelt overførbare sykdommer.

I vurderingen av hva slags risiko den registrerte står ovenfor må det gjøres en interesseavveining av to hovedhensyn. På den ene siden tas hensyn til folkehelsen og på den andre siden må inngrep i personvernet unngås.[138] Kravet om å verne den registrertes personopplysninger er vesentlig for å skape tillit til at opplysningene ikke blir spredd til uvedkommende. Flere tiltak kan sikre personvernet. Informasjonssikkerhet utvikles kontinuerlig med for eksempel IKT-systemer i helse- og omsorgssektoren. Samtidig vil det i fremtiden kunne reises nye sikkerhetsutfordringer som ikke kan ivaretas etter dagens teknologi. En annen risiko kan oppstå ved samarbeid mellom flere

[136] Prop. 23 L (2009-2010) s. 11.
[137] Prop. 23 L (2009-2010) s. 11.
[138] Prop. 72 L (2013-2014) s. 55.

helseforetak i behandlingen mellom basisregisteret og de medisinske kvalitetsregistrene. Ved å bruke digital kommunikasjon og automatisk overføring av helseopplysninger til helseregistre er det en risiko for at opplysningene ikke alltid behandles i tråd med personvernregelverket.

Store mengder helsedata samles inn i basisregisteret og kvalitetsregistrene til hjerte- og karregisteret. Ved sikkerhetsbrudd kan helsedata tilgjengeliggjøres på internett. En annen risiko er uautorisert tilgang av helsepersonell for å undersøke i helseopplysninger de ikke skal ha tilgang til. Slike sikkerhetsbrudd kan det gå utover tilliten befolkningen har til spesialisthelsetjenesten som samler inn helseopplysningene og Folkehelseinstituttet som behandlingsansvarlig. Sikkerhetsbrudd og urettmessig tilgang til helseopplysninger av helsepersonell vil over tid skape tvil og kan føre til at pasienter ønsker å reservere seg fra oppbevaring av helseopplysninger i hjerte- og karregisteret.

Risikoene må samlet sett tas i betraktning for å vurdere behandling av personopplysninger i hjerte- og karregisteret. Særlig er de nevnte risikoene i en vurdering i samsvar med GDPR art. 32 og personvernkonsekvenser, se art. 35.

6.4 Vurdering av ivaretakelse av den registrertes rett til personvern ved behandling (II)

6.4.1 Meldingssystem for smittsomme sykdommer

Sykdommer i gruppe A meldes inn til registeret med full pasientidentitet i følge MSIS-forskriften § 1-7 (3). Dermed kreves det et sterkt vern av personopplysningene. Det er betenkelig at så følsomme helseopplysninger skal kunne være identifiserbare. Til andre helseopplysninger som for eksempel gruppe C av mindre sensitivitet stilles det strengere krav til å skjule identifiserbare opplysninger, jf. MSIS-forskriften § 1-8. Sykdommenes smittefarlige karakter gjør at noen av de mest sensitive helseopplysningene kan føres i et personidentifiserbart register.

I forbindelse av rapportering av B-gruppe sykdommer, skal det oppgis den smittedes fødselsmåned og -år, kjønn og bostedskommune, jf. MSIS-forskriften § 1-7 (3). Sammenlignet med A-sykdommer stilles det strengere krav til å skjule pasientens identitet for seksuelt overførbare sykdommer. Likevel kan betegnelsen anonym være misvisende fordi opplysningene kan bidra til å identifisere personen dersom for eksempel pasienten kommer fra en liten kommune hvor den smittsomme sykdommen er lite utbredt. Slike momenter gir grunn til å verne om pasienter med gruppe B-sykdommer sitt personvern. For å ivareta den registrertes rett til personvern stilles det særlig strenge krav til at disse avidentifiserbare helseopplysningene ikke skal identifiseres ved kobling til andre opplysninger.

For å ivareta retten til personvern er det sentralt at den registrerte får tilstrekkelig informasjon om hvilke helseopplysninger registrert i MSIS er identifiserbare og hvilke anses ikke som personopplysninger. Tilstrekkelig informasjon bygger tillit mellom pasienten og helsepersonellet. En utfordring knyttet til pasientens autonomi er at behandling av personopplysninger i MSIS krever ikke

samtykke fra den registrerte, jf. MSIS-forskriften § 1-7, jf. Hregl. § 11. Dersom pasienten kunne ta en informert avgjørelse om å samtykke eller trekke tilbake samtykke ville det gitt pasienten større autonomi.

Den registrertes rett til personvern ivaretas ved at behandlingen utføres slik at smittsomme sykdommer blir registrert med riktig identifikasjonsform, jf. MSIS-forskriften § 1-2. Ettersom samtykke ikke er et vilkår for behandling i MSIS bør det stilles enda høyere krav til at sikkerhetsrutinene etterleves i tråd med reglene gitt i personvernforordningen, helseregisterloven og spesifisert i MSIS-forskriften.

Graden av ivaretakelse av personvernet avhenger av hvilken gruppe den smittsomme sykdommen kategoriseres i. Opplysninger knyttet til sykdommer i gruppe B ivaretas med strenge krav til rettslig grunnlag og ved at personopplysningene er ikke direkte identifiserbare. Begrunnelsen for å gi forskjellig personvern av helseopplysninger i ulike grupper smittsomme sykdommer er noe ufullstendig. Derfor bør det argumenteres i større grad hvorfor enkelte helseopplysninger som er så sensitive ikke skal skjule pasientidentiteten til alle helseopplysningene registrert i MSIS.

6.4.2 Hjerte- og karregisteret

Personvernforordningen, helseregisterloven og hjerte- og karregisterforskriften skal sikre at hensynet til personvern vektlegges tungt når helseopplysninger skal samles inn, brukes og oppbevares. Tekniske sikkerhetsløsninger begrenser antall personer som har tilgang til sensitive helseopplysninger i registeret.[139]

I hjerte- og karregisterforskriften er det også fastsatt unntak fra GDPR art. 9 nr. 2 bokstav a om kravet til samtykke. Helseopplysningene som kan unntas fra samtykkekravet er direkte identifiserbare opplysninger, administrative opplysninger og medisinske opplysninger, se hjerte- og karregisterforskriften § 1-4 (1) I-III. Risiko for den registrertes personvern er høy ved direkte identifikasjonsopplysninger som fødselsnummer.

Grunnlaget for å opprette et helseregister som er personidentifiserbart og uten krav til samtykke ble begrunnet med at det forelå et behov for et slikt register.[140] Av den grunn kan det virke som det er foretatt en noe ufullstendig vurdering av om det finnes alternative behandlingsformer av personopplysninger knyttet til hjertesykdommer. Til tross for at helseopplysningene skal utleveres anonyme er det en stor personvernulempe at helseopplysningene registreres som

[139] PRE-2011-12-16-1250 kapittel 3.
[140] Prop. 23 L (2009-2010) s. 7.

personidentifiserbare uten krav om samtykke. Dette er en begrensning i den registrertes rett til å bestemme over egne helseopplysninger.[141]

Den registrerte skal ha tillit til at deres personlige integritet blir ivaretatt på best mulig måte. I hjerte- og karregisterforskriften fremheves betydningen av at den registrerte skal ha tillit til at helseopplysninger ikke misbrukes eller kommer på avveie.[142] Den registrertes rett til personvern skal ivaretas etter reglene i hjerte- og karregisterforskriften om taushetsplikt, jf. § 4-1, informasjonssikkerhet, jf. § 4-2, kryptering, jf. § 4-3 og internkontroll, jf. § 4-4. Den registrerte skal ha tillit til at databehandlere behandler helseopplysninger med fortrolighet og hindre at andre får kjennskap til helseopplysningene, jf. hregl. § 17, jf. hpl. § 21.

Tekniske og organisatoriske tiltak skal gjennomføres for å oppnå et sikkerhetsnivå som tar hensyn til risikoen, jf. GDPR art. 32 og hregl. § 21. Den registrertes navn og adresse skal ikke registreres, se antitetisk tolkning av hjerte- og karregisteret § 1-4. Personidentifiserbare opplysninger som kan registreres er fødselsnummer, D-nummer, bostedskommune, fødested og sivilstand, jf. hjerte- og karregisterforskriften § 1-4. For å ivareta den registrertes rett til personvern skal særlige sensitive opplysninger som biologisk materiale eller resultat av prediktive undersøkelser ikke inngå i registeret, se hjerte- og karregisterforskriften § 1-4 (3).

I helsetjenesten er det etablert systemer for loggføring av elektroniske spor ved all tilgang til helseregisteret.[143] Imidlertid er det ikke gitt instruks i forskrift om hvordan loggføringen skal kontrolleres. Misbruk av helseopplysninger blant helsepersonell kan for eksempel oppdages ved stikkprøver i loggen eller ved avanserte datasystem som melder fra ved potensiell misbruk. Sistnevnte kan føre til problemer ettersom det kan mistenkeliggjøre helsepersonell som bare forsøker å utføre arbeidet sitt. Stikkprøver på den andre siden vil ikke fange opp alle tilfeller av misbruk. Det vil i realiteten resultere i få avsløringer av urettmessig tilgang av helsepersonell i registeret ettersom sannsynligheten for å oppdage ved en stikkprøve er liten.[144]

I vurderingen er det tatt stilling til hvordan den registrertes rett til personvern ivaretas ved behandling i hjerte- og karregisteret. Den viktigste måten å ivareta den registrertes rett til personvern og unngå personopplysninger på avveie er å ha gode sikkerhetsrutiner samt å anonymisere personopplysninger ved kryptering. § § 4-3. Ved å skille fødselsnumre fra øvrige helseopplysninger gjør det vanskeligere å knytte helseopplysningene direkte til en pasient ved sikkerhetsbrudd.

[141] Prop. 23 L (2009-2010) s. 11.
[142] PRE-2011-12-16-1250 kapittel 3.
[143] PRE-2011-12-16-1250 kapittel 3.
[144] PRE-2011-12-16-1250 kapittel 3.

6.5 Vurdering av behandling av personopplysninger i helseregistre i samsvar med grunnprinsippene (III)

6.5.1 Meldingssystem for smittsomme sykdommer

I dette kapittelet vurderes det om grunnprinsippene etter GDPR art. 5 oppfylles ved behandling av helseopplysninger i MSIS. Ved behandling av smittsomme sykdommer i MSIS må Folkehelseinstituttet sørge for at de selvstendige pliktene etter GDPR art. 5 nr. 1 blir oppfylt, jf. GDPR art. 5 nr. 2.

I utgangspunktet er det forbudt å behandle helseopplysninger om smittsomme sykdommer og seksuelle forhold. jf. GDPR art. 9 nr. 1 i samsvar med prinsippet om lovlighet.[145] Det legges til grunn at det rettslige grunnlaget for behandling av personopplysninger i MSIS er GDPR art. 6 nr. 1 bokstav e, jf. art. 9 nr. 2 bokstav h om yting av helsetjenester. Det som er mer uklart, er hvorvidt det er adgang for lovlig behandling av personopplysninger i MSIS etter GDPR art. 9 nr. 2 bokstav g om viktige allmenne interesser.

Prinsippet om lovlighet ivaretas i nasjonal lovgivning ved at MSIS er et lovbestemt sentralt helseregister, jf. hregl. § 11 bokstav h, jf. § 8 i samsvar med GDPR art. 9 nr. 2 bokstav h eller bokstav g. Helseregistre etter hregl. § 11 er den mest personverninngripende typen helseregistre.[146] Helseopplysninger kan behandles i MSIS, jf. MSIS-forskriften § 4-5.

Videre må den nasjonale lovgivningen stå i forhold til formålene som søkes oppnådd med behandlingen, jf. GDPR art. 9 nr. 2 bokstav g. MSIS-forskriften anses å stå i forhold til formålet fordi sammenstilling av helseopplysninger i MSIS med andre helseopplysninger kan bidra til å oppklare utbrudd av smittsomme sykdommer eller beskrive forekomsten i Norge, jf. MSIS-forskriften § 1-3 nr. 1 og 2.

For at behandlingen skal anses lovlig etter GDPR art. 9 nr. 2 bokstav g må den være «nødvendig» av hensyn til «viktige allmenne interesser». Ordlyden av «viktige allmenne interesser» tilsier at behandlingen må være av særlig betydning for samfunnet som helhet. Et lignende vilkår fulgte av personopplysningsloven 2000 § 9 og ble anvendt av helsetjenesten for behandling av personopplysninger etter naturkatastrofer og av 22. juli-kommisjonen for granskningsarbeid.[147] Dette trekker i retning at det skal være særegne omstendigheter som kommer hele samfunnet til gode.

[145] GDPR fortalepunkt 51.

[146] Søvig (2016) note 42.

[147] Skullerud (2018) s. 110.

Den allmenne interessen må veie tyngre enn hensynet til den enkeltes personvern. Slike tilfeller kan være helseformål som folkehelse og helsetjenesteforvaltning.[148] Behandling av opplysninger knyttet til smittsomme sykdommer anses som nødvendig ut fra hensynet til smittevern og internasjonale forpliktelser, jf. MSIS-forskriften § 1-2, se § 2-7.

I følge MSIS-forskriften § 1-2 meldes sykdommene med full pasientidentitet fordi det er nødvendig å ha detaljerte opplysninger for å overvåke sykdommene nøye. For å unngå spredning av smittefarlige sykdommer som meslinger må det foretas smitteverntiltak for å beskytte folkehelsen.[149] Deretter skal behandlingen sikres med «egnede og særlige tiltak» for å verne den registrertes grunnleggende rettigheter og friheter, jf. GDPR art. 9 nr. 2 bokstav g.

For gruppe A-sykdommer er behovet for behandling av identifiserbare personopplysninger begrunnet med viktige helsehensyn. Likevel er argumentasjonen for at pasienten skal kunne identifiseres med sensitive personopplysninger nokså svakt bygd opp med henvisning til smittevern uten videre forklaring. En begrunnelse for hvorfor nettopp pasientidentiteten er sentral for å verne mot smitte vurderes nødvendig når det er tale om så stort inngrep i den registrertes personvern. Andre tiltak og deres egnethet vurderes i punkt 6.4.1.

For at behandlingen skal være i tråd med prinsippene om rettferdighet og åpenhet, må den registrerte få tilstrekkelig informasjon om behandlingen av sine personopplysninger og innsyn i MSIS, jf. MSIS-forskriften § 6-2. Dette anses som egnet for å verne den registrertes grunnleggende rettigheter og friheter etter GDPR art. 9 nr. 2 bokstav g.

MSIS-forskriften gir lite veiledning om hvordan informasjonsplikten skal ivaretas bortsett fra henvisning til GDPR art. 13-15, jf. hregl. § 24. Av MSIS-forskriften bør det fremgå tydelig hva som skal informeres om og når den registrerte skal få informasjon. Uten tilstrekkelig informasjon bryter behandlingsansvarlig informasjonsplikten og den registrerte kan ikke ivareta sine grunnleggende rettigheter. Det er opp til den behandlingsansvarlig til å treffe egne tiltak for å gi informasjon, jf. GDPR art. 12 nr. 1. Tiltakene for dette bør fremgå av MSIS-forskriften, slik at kravet om informasjon ivaretas likt ved hver behandling av personopplysninger i samsvar med prinsippet om rettferdighet.

Formålet med oppsamling og behandling av helseopplysninger i MSIS er i følge MSIS-forskriften § 1-3 (1) å bidra til overvåking av smittsomme sykdommer hos mennesker i Norge gjennom innsamling, analyse, tolkning og rapportering av opplysninger om tilfeller av smittsomme

[148] GDPR fortalepunkt 52.
[149] GDPR fortalepunkt 52.

sykdommer. Behandling til sekundærbruk vil ikke tjene den registrerte direkte, men hjelper andre pasienter ved å få kunnskap til å utvikle medisiner, behandlingsformer og redusere spredning av smittsomme sykdommer.[150] Dette er i tråd med prinsippet om formålsbegrensning, jf. GDPR art. 5 nr. 1 bokstav b. Ved å trekke opp en rettslig ramme for behandling og gi spesifikt formål for hvordan helseopplysninger skal brukes for å verne mot sykdommer anses det å oppfylle prinsippet.

For å ivareta dataminimeringsprinsippet kan gruppe A-sykdommer med å redusere pasientidentiteten, jf. MSIS-forskriften § 17 (3). Formålet kan fortsatt oppnås med færre personidentifikatorer eller ved å avidentifisere opplysningene uten at det går utover kvalitetssikringen av behandlingen. Prinsippet ivaretas ved sammenstilling av helseopplysninger i MSIS med helseopplysninger i andre registre nevnt i MSIS-forskriften § 4-1 (1) hvor resultatet må være i anonymisert form.

Av MSIS-forskriften § 7-1 fremgår det at hregl. § 25 stiller krav til retting ved uriktige opplysninger i tråd med GDPR art. 16 og 17. Folkehelseinstituttet skal sørge for at feil ikke skal få betydning for den registrerte dersom det er mulig. Behandlingsprosessen virker tilsynelatende å ivareta prinsippet om riktighet så langt det lar seg gjøre i den faktiske behandlingen av helseopplysninger i MSIS.

Helseopplysninger kan i utgangspunktet oppbevares i MSIS i ubegrenset tid, jf. MSIS-forskriften § 7-1. Etter hregl. § 25 kan derimot den registreres kreve retting eller sletting av helseopplysningene, jf. GDPR art. 16 og 17. Bestemmelsen inneholder en begrensning ved at opplysningene kan slettes dersom behandlingen av helseopplysningene må føles «sterkt belastende» for den registrerte og det må ikke foreligge «sterke allmenne hensyn» for at de ikke skal slettes, se hregl. § 25. Ordlyden tilsier at den registrertes rett til sletting innskrenkes ettersom «sterkt» belastende taler for at det skal en del til før helseopplysningene kan slettes. Prinsippet om lagringsbegrensning anses dermed svekket.

I følge MSIS-forskriften § 5-1 til § 5-4 stilles det like krav til taushetsplikt, informasjonssikkerhet og internkontroll, og det må således sørges for at prinsippet om integritet og konfidensialitet ivaretas. Dersom det fremgikk av ordlyden i MSIS-forskriften §§ 5-2 og 5-3 hvilke tekniske og organisatoriske tiltak som må gjennomføres for å oppnå tilstrekkelig sikkerhet ville det vist mer forutberegnelighet for Folkehelseinstuttet. Enkelte tiltak følger imidlertid av merknadene til § 5-2 i MSIS-forskriften.

Dersom prinsippene om personvern etter GDPR art. 5 ikke ivaretas i tilstrekkelig grad kan det føre til store økonomiske konsekvenser for Folkehelseinstituttet. Det er av betydning at norsk rett harmoniseres med EU-rett etter personvernforordningen for å redusere smitten ved å ha tilsvarende likebehandling av helseopplysninger om smittsomme sykdommer.[151]

[150] GDPR fortalepunkt 53.

[151] GDPR fortalepunkt 10.

For å unngå uautorisert bruk eller ulovlig behandling av helsepersonell eller hackerangrep bør Folkehelseinstituttet ta ansvar for å gjennomføre risikovurderinger etter GDPR art. 32, jf. art. 24. Det blir for generelt å vise til informasjonssikkerhetskrav i hregl. § 21 idet sikkerhetsnivå og tiltak i MSIS må baseres på en konkret risikovurdering.

I vurderingen ble det tatt stilling til hvordan grunnprinsippene etter GDPR art. 5 blir oppfylt ved behandling av helseopplysninger i MSIS. Dersom det foretas personvernkonsekvensutredning før helseopplysninger lagres i MSIS og underveis vil det bidra til å ivareta den registrertes rettigheter ved å oppfylle prinsippene etter GDPR art. 5.

6.5.2 Hjerte- og karregisteret

I analysen vurderes hvorvidt grunnprinsippene etter GDPR art. 5 blir oppfylt ved behandling av helseopplysninger i hjerte- og karregisteret. Ved behandling av hjerte- og karlidelser i registeret har Folkehelseinstituttet ansvar for å sørge for at pliktene etter GDPR art. 5 blir oppfylt, jf. GDPR art. 5 nr. 2.

Reglene for lovlig behandling i hjerte og karregisteret følger av de samme bestemmelsene i personvernforordningen som behandlet etter MSIS. Det rettslige grunnlaget for behandling av personopplysninger i hjerte- og karregisteret er dermed GDPR art. 6 nr. 1 bokstav e, jf. art. 9 nr. 2 bokstav h og g. Det er i allmennhetens interesse å gjenbruke helseopplysninger om hjerte- og karlidelser for å analysere og forske på forbedring av kvalitet på helsehjelp, forebyggende arbeid og helseforskning av disse sykdommene. Det forutsettes at behandlingen har et supplerende rettsgrunnlag i nasjonal rett.[152] Prinsippet om lovlighet blir ivaretatt i hjerte- og karregisteret ved at registeret er et lovbestemt sentralt helseregister, jf. hregl. § 11 bokstav h, i samsvar med § 8. Det gjelder ingen reservasjonsrett for hjerte- og karregisteret.[153]

Prinsippet om rettferdig behandling anses for å bli ivaretatt ved at det er en rimelig sammenheng mellom innsamling av helseopplysninger i hjerte- og karregisteret og formålet de skal brukes til. I likhet med MSIS er formålet med hjerte- og karregisteret generelt utformet, se hjerte- og karregisterforskriften § 1-2. Det må med andre ord mye til for at behandlingen er utenfor rekkevidden av formålet. Prinsippet om åpenhet ivaretas ved at den registrerte har rett til informasjon og innsyn, jf. GDPR art. 5 nr. 1 bokstav a og hjerte- og karregisterforskriften § § 4-2.

Prinsippet om formålsbegrensning ivaretas gjennom hjerte- og karregisterforskriften § 1-2. Det fremgår av ordlyden til bestemmelsen at formålet går ut på å forbedre kvalitet på helsehjelpen til

[152] Skullerud (2018) s. 111.

[153] Søvig (2016) note 42.

personer med hjerte- og karsykdommer. Formålet legger til rette for gjenbruk av helseopplysninger for å fremme helse, forebygge sykdom og gi bedre helse- og omsorgstjenester. Behandlingen kan gjøres så lenge den utføres på en etisk forsvarlig måte, ivaretar den enkeltes personvern og brukes til individets og samfunnets beste og er innenfor formålets rekkevidde.[154] Formålet er bredt og sier ingenting om individbehandling, men helsehjelp til en gruppe mennesker med hjerte- og karsykdommer. Ved å ha et vidt formål til å forbedre helse relatert til hjerte- og karsykdommer kan behandling etter GDPR art. 6 nr. 1 bokstav e, jf. art. 9 nr. 2 bokstav g i allmennhetens interesse anses for å være innenfor rekkevidden.

For å oppfylle prinsippet om dataminimering må sammenstillingen av helseopplysninger i helseregisteret ligge innenfor rammene av behandlingens formål, jf. hjerte- og karregisterforskriften § 1-4. Sammenstilling med opplysninger i andre registre for uttrykkelig angitte formål legges til rette etter hjerte- og karregisterforskriften § 3-2, for eksempel befolkningsbaserte helseundersøkelser. Ved behandling må det tas stilling til om formålet kan oppnås med færre personopplysninger eller om personopplysningene kan anonymiseres.[155] Ut fra ordlyden som til hjerte- og karregisterforskriften § 1-2 vurderes det som lite sannsynlig at det er nødvendig med direkte identifiserbare opplysninger for å oppnå formålet om forbedring av helsehjelp. De mest sensitive og identifiserbare opplysninger bør være mulig å fjerne for å oppnå den samme behandlingen.

For å oppfylle kravet om riktighet kan håndtering av massedata i helsetjenesten gjøres ved bruk av IKT-systemer. IKT-systemer skal kommunisere helseopplysninger på en effektiv og sikker måte i samsvar med prinsippet om riktighet. Slik kan pasienter og helsepersonell stole på at opplysningene i hjerte- og karregisteret er korrekte, oppdaterte og tilgjengelige for databehandlere og pasientene selv. Systemene må ha høy sikkerhet for å sørge at opplysningene ikke kommer på avveie.

I samsvar med prinsippet om lagringsbegrensning kan opplysninger i registeret sammenstilles anonymt i statistisk form og slettes av Folkehelseinstituttet så snart statistikkfremstillingen er ferdig, jf. hjerte- og karregisterforskriften § 3-1 (2) og (4). Det må være klart ut fra etiske hensyn av sammenstillingen må være en sikker behandling, se hjerte- og karregisterforskriften § 3-2 (1) for å hindre at helseopplysninger kommer på avveie.

Folkehelseinstituttet har plikt til å sørge for at behandling av personopplysninger registrert i hjerte- og karregisteret sikrer opplysningenes integritet og behandles konfidensielt. Folkehelseinstituttet kan iverksette tekniske og organisatoriske sikkerhetstiltak for å nå et sikkerhetsnivå som tilsvarer risikoen ved behandlingen, jf. hjerte- og karregisterforskriften § 4-2, se GDPR art. 32 og hregl. § 21. Kryptering ivaretar prinsippet om konfidensialitet og integritet ved at direkte identifiserbare

[154] Prop. 72 L (2013-2014) s. 117.
[155] GDPR fortalepunkt 39.

opplysninger skjules slik det blir vanskeligere å finne sensitive elementer ved opplysningene i helseregisteret, jf. hjerte- og karregisterforskriften § 4-3. På samme måte som at IKT-systemer skal sørge for at opplysninger er korrekte og oppdaterte, må systemet ha høy sikkerhet for å sørge for at opplysningene ikke kommer på avveie.[156]

For å svare på problemstillingen om hvordan behandling etter hjerte- og karregisteret blir oppfylt etter GDPR art. 5 nr. 1 har bestemmelsens naturlige språklige forståelse betydelig vekt. For å sikre og påvise at behandlingen av helseopplysningene utføres i samsvar med prinsippene etter GDPR art. 5 nr. 1 og hregl. § 22 må Folkehelseinstituttet føre internkontroll ved hjelp av tekniske og organisatoriske tiltak, jf. hjerte- og karregisterforskriften § 4-4. Helseforetak som er databehandlere skal behandle helseopplysninger etter rutiner fastsatt av Folkehelseinstituttet, se alternativene i hjerte- og karregisterforskriften § 4-4.

Ved at Folkehelseinstituttet vurderer personvernkonsekvenser som kan oppstå ved behandling av helseopplysninger i registeret kan det bidra til å minske risikoen ved behandling. DPIA er på samme måte som ved behandling i MSIS en god personvernutredning for å ivareta den registrertes rettigheter. Arbeidet med personvern i helseregistre er en kontinuerlig prosess. For å takle nye personvernutfordringer som oppstår er det vesentlig at behandlingsansvarlig tar tak i disse med en gang de inntreffer. Det er spesielt viktig å vise rask handleevne når det oppdages svakheter i de digitale systemene med helseregistre. Dette er som følge av at store mengder helsedata behandles og det kan få konsekvenser for mange pasienters personvern.

[156] Prop. 72 L (2013-2014) s. 55.

7 OPPSUMMERING OG PERSPEKTIVER

Store mengder helsedata har i dag en sentral rolle for kvalitetssikring og helseforskning. Personopplysninger utgjør grunnlaget i digitale helseregistre. Den nye helseanalyseplattformen gjør det enklere å dele og bruke helsedata på tvers av ulike systemer. De automatiske prosessene kan gjøre det vanskeligere å få oversikt over hvilke personopplysninger som blir delt og hvem som får tilgang på opplysningene. Med hensyn til oppgavens første problemstilling er det belyst flere risikoer som potensielt innskrenker den registrertes rettigheter og friheter. Noen av de viktigste risikoene ved behandling av personopplysninger i helseregistre er datasikkerhet, sikkerhetshull i behandlingsruteringer samt brudd på konfidensialitet ved uautorisert tilgang og urettmessige undersøkelser av helsepersonell. Samtidig må disse risikoene måles opp mot hensynet til forbedring av folkehelse og smittevern, helsesikkerhet og effektiv behandling av helsedata til sekundærbruk.

For å svare på den andre problemstillingen er utgangspunktet for behandling av personopplysninger i helseregistre er GDPR art. 6 nr. 1, jf. art. 9 nr. 1. Det er helseopplysninger sin sensitive karakter som gjør at det er en utsatt kategori av personopplysninger. Dette kommer for eksempel til uttrykk ved behandling av personopplysninger relatert til seksuelt overførbare sykdommer i MSIS. I utgangspunktet kan den registrertes rett til personvern i stor grad ivaretas ved behandling. Særlig gjelder dette dersom databehandler foretar behandling basert på samtykke, tilstrekkelig informasjon og muligheten til innsyn i egne personopplysninger. Pseudonymisering og anonymisering er gode behandlingsformer som kan øke graden av ivaretakelse av retten til personvern.

Derimot med Helse Sør-Øst-hendelsen og Facebook-hendelsen friskt i minne tyder dette på at den registrertes rett til personvern ivaretatt blir i mye mindre grad enn det som følger av lovkravene i personvernforordningen. I tillegg virker det noe tillitsvekkende at det ikke er et krav om samtykke ved behandling av personopplysninger i MSIS og hjerte- og karregisteret. Dette er til tross for at personvernforordningen åpner for behandling uten samtykke, jf. GDPR art. 9 nr. 4. Samtykkekravet er egnet til å ivareta den registrertes rett til selvbestemmelse, styrker rett til informasjon og sikrer personvern som helhet. Rettskildebildet i helseretten viser at det er nødvendig med en forholdsmessighetsvurdering i hvert enkelt tilfelle for å sørge for at den registrertes rett til personvern ivaretas etter beste evne.

Etter den tredje problemstillingen er det en forutsetning for å behandle personopplysninger i helseregistre er at behandlingsprosessen ivaretar grunnprinsippene som følger av GDPR art. 5. Med utvikling i helsetjenesten er det ønske og behov for å opprette flere helseregistre som bidrar til spredning av sensitive personopplysninger. Bakgrunnen for innstramming av personvernregelverket er tendensen til at hensynet til personvern og dens grunnprinsipper blir gradvis tillagt mindre vekt. Det må foretas en konkret vurdering ved for eksempel gjenbruk av helseopplysninger hvorvidt

grunnprinsippene oppfylles i tilstrekkelig grad. Det stilles strenge krav til at behandlingsansvarlig sørger for at grunnprinsippene etterleves. Ansvaret kan utføres ved intern- og etterkontroll av behandling i helseregistre. For at prinsippene om behandling av personopplysninger skal anses oppfylt, bør det tilføres en mer utfyllende vurdering i litteraturen og i høringsnotat til lovforslag om nye helseregistre. I forarbeider om lovforslag er ofte drøftelsene om hvordan personvernet skal veies opp mot andre hensyn korte eller fraværende. Utfordringer ved lovtolkning etter personvernforordningen vil vises ved blant annet hvor mange henvendelser om avvik Datatilsynet må håndtere fremover.

Helseregistrene i oppgaven skal ikke belyse forskjeller og likheter som finnes i det enkelte helseregistre ved behandling av personopplysninger. Behandling i MSIS viser hvordan behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger er essensielt for den registrertes rett til personvern. Behandling av personopplysninger i hjerte- og karregisteret gir uttrykk for hvordan den registrertes rett til personvern ikke gjør seg like gjeldende avveid mot hensyn til å forebygge folkesykdom og fremme helse.

Datatrusler mot helseregistre kan opptre i form av dataspionasje eller hackerangrep. Sikkerhetsbrudd skyldes imidlertid ikke bare av eksterne faktorer, men også av interne. Konsekvensen av mangelfulle risikovurderinger gjør virksomhetene sårbare for innbrudd og ulovlig deling av helsedata. Uautorisert tilgang eller avsløring kan for eksempel gjøres ved å sende feil e-post eller at en ansatt sender sensitiv informasjon til feil databehandler. I situasjoner med datatrusler er det ofte brudd på konfidensialitet eller integritet til behandling av personopplysninger som er tilfelle. Personvernforordningen stiller strenge krav til informasjonssikkerhet, men kan ikke garantere absolutt sikkerhet. Den registrerte må akseptere en viss risiko.

Denne oppgaven fremhever utfordringer i interesseavveiningen av behandling av personopplysninger i helseregistre. På den ene siden vil et helsesystem med effektiv administrering og enkel tilgjengelighet være egnet for sekundærbruk. På den andre siden vil økt vektlegging av tillitsforholdet mellom pasient og lege, betydningen av taushetsplikt og personvern kunne føre til et komplisert administrativt helsesystem. Personopplysningsbegrepets store rekkevidde, basert på tolkningsfaktorer fra EU-domstolen og forvaltningspraksis, har betydning for å identifisere risiko for innskrenkning i personvernet ved behandling.

Målet med denne normative analysen har vært å bidra til å styrke balansen mellom ulike hensyn til helse og personvern. Det er uheldig hvis det stadig i interesseavveiingen vises til at den registrertes rett til personvern skal tillegges vesentlig vekt, men ender opp med å sette det til side uten en grundig nok vurdering av alle de sentrale momentene som spiller inn. Nytteverdien med behandlingen må være større enn personvernulempen. Pasienters personopplysninger skal beskyttes, men ikke til enhver pris.

Referanseliste

Litteratur

01248/07/EN	Article 29 Data Protection Working Party. *WP 136 Opinion 4/2007 on the concept of personal data,* Article 29 Data Protection Working Party. Adopted on 20 June 2007.
00323/07/EN	Article 29 Data Protection Working Party. WP *131 Working Document on the processing of personal data relating to health in electronic health records (EHR). Adopted on 15 February 2007.*
Befring (2017)	Befring, Anne Kjersti. *Helse- og omsorgsrett,* Oslo: Cappelen Damm, 2017.
Boe (2012)	Boe, Erik Magnus. *Rettskildelære under debatt,* Oslo: Universitetsforl., 2012.
Blume (2018)	Blume, Peter. *Den nye persondataret, 2. utg.,* København: Jurist- og Økonomforbundet, 2018.
Eckhoff (2001)	Eckhoff, Torstein. *Rettskildelære,* 5. utg. ved Jan E. Helgesen, Oslo: Universitetsforl., 2001.
Engelschiøn (2017)	Engelschiøn, Sverre og Elisabeth Vigerust. (2017) «Helseregisterloven: kommentarutgave» i *Kommentarutgave.no.*
Kierulf (2016)	Kierulf, Anine. (2016) «Kommentar til Grunnloven» i *Norsk lovkommentar, Gyldendal Rettsdata*, 16.11.2016 [Sitert 26.09.18].
Ploem (2006)	Ploem, MC. «Towards an Appropriate Privacy Regime for Medical Data Research», *European Journal of Health Law* Vol. 13(1) (2006), s. 41-63.

Region Sjælland (2018) — Region Sjælland. «Personoplysninger – Sådan gør vi», *Broen til bedre sundhed* (2018).

Schartum (2012) — Schartum, Dag Wiese. (2012) «Kommentar til personopplysningsloven 2000» i *Norsk lovkommentar, Gyldendal Rettsdata,* 18.10.2012 [Sitert 26.09.18].

Schartum (2016) — Schartum, Dag Wiese og Lee Andrew Bygrave. *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger,* 3. utg., Bergen: Fagbokforl., 2016.

Skoghøy (1994) — Skoghøy, Jens Edvin A. «Rett, politikk og moral: om bruk av politiske og etiske argumenter ved rettsanvendelse og juridisk forskning», *Tidsskrift for rettsvitenskap* (1994), s. 837-881.

Skullerud (2018) — Skullerud, Åste Marie Bergseng, Cecilie Rønnevik og Jørgen Skorstad mfl. *Personvernforordningen (GDPR): Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning),* Oslo: Universitetsforl., 2018.

Søvig (2016) — Søvig, Karl Harald. (2016) «Kommentarer til helseregisterloven» i *Norsk lovkommentar, Gyldendal Rettsdata* [Sitert 28.09.18].

Wessel-Aas (2018) — Wessel-Aas, Jon og Magnus Ødegaard. *Personvern: publisering og behandling av personopplysninger,* Oslo: Gyldendal Norsk Forlag, 2018.

Wierda (2018) — Wierda, Eric, Daniëlle C Eindhoven, Martin Jan Schalij mfl. «Privacy of patient data in quality-of-care registries in cardiology and cardiothoracic surgery: The impact of the new general data protection regulation EU-law», *European Heart Journal. Quality of*

Care & Clinical Outcome, 4(4) (2018), s. 239-245.

Nettsider

Arendt (2018)	Arendt, Torstein og Stian Oddbjørnsen *De første avgjørelsene vedrørende GDPR* (2018), http://www.cw.no/artikkel/it-juss/de-forste-avgjorelsene-vedrorende-gdpr [Sitert 21.11.2018].
Clausen (2018)	Clausen, Vilde Brandtzæg. *Eldre homofile går tilbake i skapet når de møter helsevesenet* (2018), https://www.tv2.no/a/10151483/ [Sitert 21.11.2018].
Datatilsynet (2017)	Datatilsynet. *Ni helseforetak er varslet om gebyr* (2017), https://www.datatilsynet.no/aktuelt/2017/ni-helseforetak-er-varslet-om-gebyr/ [Sitert 21.11.2018].
Helse- og omsorgsdepartementet (2018)	Helse- og omsorgsdepartementet. *Regjeringen tildeler 150 millioner til en nasjonal analyseplattform for helsedata* (2018), https://www.regjeringen.no/no/aktuelt/regjeringen-tildeler-150-millioner-til-en-nasjonal-analyseplattform-for-helsedata/id2594625/ [Sitert 21.11.2018].
Høgseth (2018)	Høgseth, Martin Hagh. *50 millioner Facebook-brukere rammet av sikkerhetsbrist* (2018), https://e24.no/boers-og-finans/facebook/50-millioner-facebook-brukere-rammet-av-sikkerhetsbrist/24452880 [Sitert 21.11.2018].

Norske rettskilder

Lover og forskrifter

1814	Lov 17.mai 1814 Kongeriket Norge Grunnlov.
1992	Lov 27. november 1992 nr. 109 gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) (EØS-loven).
1999	Lov 2. juli 1999 nr. 64 helsepersonell (helsepersonelloven).

2000	Lov 14. april 2000 nr. 31 behandling av personopplysninger (personopplysningsloven) (opphevet).
2003	Forskrift 20. juni 2003 nr. 740 om Meldingssystem for smittsomme sykdommer (MSIS-forskriften).
2008	Lov 20. juni 2008 nr. 44 medisinsk og helsefaglig forskning (helseforskningsloven).
2011	Forskrift 16. desember 2011 nr. 1250 om innsamling og behandling av helseopplysninger i Nasjonalt Register over hjerte- og karlidelser (hjerte- og karregisterforskriften).
2014	Lov 20. juni 2014 nr. 42 behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven).
2014	Lov 20. juni 2014 nr. 43 helseregistre og behandling av helseopplysninger (helseregisterloven).
2018	Lov 15. juni 2018 nr. 38 behandling av personopplysninger (personopplysningsloven).
2018	Forskrift 16. juni 2018 nr. 876 om behandling av personopplysninger (personopplysningsforskriften).

Forarbeider

NOU 1993: 22	*Pseudonyme helseregistre. Et lovutkast om personvern, pasientvern og helsevern.*
Ot.prp. nr. 92 (1998-1999)	*Om lov om behandling av personopplysninger (personopplysningsloven).*
Prop. 23 L (2009-2010)	*Endringer i helseregisterloven og helsepersonelloven (nasjonalt register over hjerte- og karlidelser, adgang til å gi dispensasjon fra taushetsplikt for kvalitetssikring, administrasjon, planlegging og styring av helsetjenesten).*
Prop. 72 L (2013-2014)	*Pasientjournalloven og helseregisterloven.*
Prop. 56 LS (2017-2018)	*Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen.*
Innst.O. nr. 62 (2000-2001)	*Om lov om helseregistre og behandling av helseopplysninger (helseregisterloven).*

Innst. 278 L (2017-2018) *Om lov om behandling av personopplysninger (personopplysningsloven).*

St.meld. nr. 43 (2003-2004) *Datatilsynets og Personvernnemndas årsmeldinger for 2003.*

Pre-2011-12-16-1250 *Forskrift om innsamling og behandling av helseopplysninger i Nasjonalt register over hjerte- og karlidelser (Hjerte- og karregisterforskriften). Kongelig resolusjon.*

Datatilsynet (2018) *Høringsuttalelse - Forslag til endringer i MSIS-forskriften og forskrift om allmennfarlige smittsomme sykdommer*, 22.5.2018.

Høyesterettsavgjørelser

Rt. 2013 s. 143.

Praksis fra Personvernnemnda

PVN-2006-04.

PVN-2013-05.

PVN-2013-08.

PVN-2013-09.

PVN-2013-10.

PVN-2013-11.

PVN-2013-12.

PVN-2013-17.

Annen offentlig praksis

Helse- og omsorgsdepartementet (2017) *Et nytt system for enklere og sikrere tilgang til helsedata – Rapport fra Helsedatautvalget 2016-2017* 30.06.2017. https://www.regjeringen.no/no/dokumenter/et-nytt-system-for-enklere-og-sikrere-tilgang-til-helsedata/id2563907/ [Sitert 26.08.2018].

Internasjonale rettskilder

EMK	Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter, Roma 4. november 1950.
EU-Charteret	Den Europæiske Unions Charter om Grunlæggende Rettigheder. Konsolideret udgave 2016 (2016/C 202/02).
For 679/2016	Personopplysningsforordning (EU) nr. 679/2016 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF.
Dir 95/46 EF	Europaparlamentets- og rådsdirektiv 1995/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger [Personverndirektivet].
Dir 2006/24 EF	Europaparlamentets- og rådsdirektiv 2006/24/EF av 15. mars 2006 om lagring av data fremkommet ved bruk av elektronisk kommunikasjon med endring av direktiv 2002/58/EF.
2018/EØS/46/01	EØS-komiteen. *EØS-komiteens beslutning nr. 154/2018 om endring av EØS-avtalens vedlegg XI*. 6. juli 2018. http://www.efta.int/media/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/2018%20-%20Norwegian/154-2018n.pdf [Sitert 22.11.2018].
Council of Europe (2017)	*Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 01/2017.

Avgjørelser fra EU-domstolen

Sag C-101/01 Sverige mod Lindqvist. .	ECLI:EU:C:2003:596.
Sag C-553/07 College van burgemeester en wethouders van Rotterdam v. M.E.E Rijkeboer	ECLI:EU:C:2009:293.
Samlet sag C-293/12 og C-594/23 Digital Rights Ireland og Seitlinger mfl.	ECLI:EU:C:2014:238.
Sag C-434/16 Nowak mod Data Protection Commissioner.	ECLI:EU:C:2017:994.

Forslag til avgjørelse ved Generaladvokat Kokott i Sag C-434/16 Nowak mod Data Protection Commissioner.	ECLI:C:2017:582.