Vejledning til sagsbehandlere om pseudonymiserede og anonymiserede oplysninger i sundhedsforskningsprojekter

Indhold

Udarbejdet af Den Juridiske Arbejdsgruppe for Sundhedsforskning, den 31. august 2023.

1. Indledning

Vejledningen er udarbejdet af den Juridiske Arbejdsgruppe for Sundhedsforskning (LMS), der refererer til sundhedsdirektørerne for de deltagende regioner samt til sundhedsdekanerne for de fire deltagende sundhedsvidenskabelige fakulteter på henholdsvis Københavns Universitet, Syddansk Universitet, Aalborg Universitet og Aarhus Universitet. Vejledningen finder således alene anvendelse på klinisk sundhedsforskning for regionerne og for de fire førnævnte sundhedsfakulteter.

Denne vejledning er målrettet de juridiske rådgivere og sagsbehandlere, som rådgiver om juridiske spørgsmål inden for sundhedsforskning, og den omhandler de juridiske krav i relation til pseudonymiserede og anonymiserede personoplysninger i forskningsprojekter.

Det er i den forbindelse vigtigt indledningsvist at være opmærksom på, at der ikke er entydige juridiske svar, der kan afgøre/verificere, om en personoplysning er anonym eller ej. Det vil være en vurdering baseret på både de videnskabelige metoder, som forskerne anvender, og de databeskyttelsesretlige krav hertil, som juristerne kan rådgive om. Det er således en samlet vurdering af mere end bare juraen, der i øvrigt også udvikler sig løbende.

Selvom den juridiske arbejdsgruppe tilstræber at holde vejledningen ajour i forhold til gældende lov og retspraksis, så skal vejledningen til enhver tid sammenholdes med gældende ret på det pågældende tidspunkt og kan ikke stå alene.

Det er indledningsvist også vigtigt at være opmærksom på, at der er snævre grænser for at anse personoplysninger for anonyme i Danmark, hvilket uddybes nedenfor.

Som udgangspunkt kan personoplysninger være vanskelige at anonymisere. Det er ofte, at der i praksis bruges lang tid på at vurdere, om datasæt kan anonymiseres, for så at konkludere, at oplysningerne alene kan pseudonymiseres.

I denne vejledning gennemgås først begreberne ”pseudonyme personoplysninger” og ”anonyme oplysninger”, herunder de juridiske krav. Dernæst gennemgås en række eksempler fra praksis, der er fremkommet fra forskellige institutioner i regionerne og de deltagende sundhedsfakulteter i Den Juridiske arbejdsgruppe for sundhedsforskning. Målet med gennemgangen af disse eksempler er at bibringe læseren en metode til gennemgang og analyse i

rådgivningen af forskerne om sondringen mellem pseudonymisering og anonymisering således, at der bedre kan bygges bro mellem de videnskabelige metoder, forskerne bruger, samt de juridiske rammer og krav, som juristerne rådgiver om.

Henvisninger til præambelbetragtninger og artikler uden nærmere præcisering er til præambelbetragtninger og artikler i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse - herefter databeskyttelsesforordningen).

2. Begreber og regler

2.1 Hvad er pseudonyme personoplysninger?

Begrebet "pseudonymisering" er defineret i artikel 4, nr. 5, hvoraf det fremgår: "behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person"

Pseudonymisering er således en teknisk foranstaltning, som fx kan bestå i, at personnavne, personnumre, adresser og andre personoplysninger, der kan anvendes til at identificere enkeltpersoner, udskilles til et særskilt dokument. De udskilte oplysninger kan herefter erstattes i deres oprindelige sammenhæng af koder. Det er således inden for rammerne af pseudonymisering, at der kan oppebæres et unikt løbenummer. Løbenummeret vil – med en tilhørende separat 'nøglefil' – muliggøre, at der entydigt kan findes tilbage til den oprindelige fysiske person.

Det skal dog altid vurderes i det konkrete tilfælde, hvad der udgør en effektiv pseudonymisering. Effektiviteten vil afhænge af typen af oplysninger, sammensætningen i datasættet, mængden/antallet af oplysninger, den valgte metode osv. En pseudonymisering er i praksis kun effektiv, hvis de "supplerende oplysninger" fx den separate nøglefil opbevares separat fra øvrige oplysninger og er underlagt tekniske og organisatoriske foranstaltninger.

Det afgørende for, at pseudonymisering kan anses for sket, er, at den registrerede ikke længere kan identificeres umiddelbart og direkte af modtageren. Så længe de supplerende oplysninger eksisterer til at "låse" disse

informationer op, da er der stadig tale om personoplysninger, jf. artikel 4, nr. 1.

Det fremgår af præambelbetragtning nr. 28, at pseudonymisering af personoplysninger kan mindske risikoen for de registrerede. I præambelbetragtning nr. 156 angives pseudonymisering som et eksempel på "fornødne garantier". På den baggrund må pseudonymisering af personoplysninger endvidere anses som en væsentlig teknisk foranstaltning.

2.2 Hvad er anonyme oplysninger?

Databeskyttelsesforordningen gælder ikke for anonyme oplysninger. Det fremgår således af præambelbetragtning nr. 26, at:

"*Principperne for databeskyttelse bør gælde for enhver information om en identificeret eller identificerbar fysisk person. Personoplysninger, der har været genstand for pseudonymisering, og som kan henføres til en fysisk person ved brug af supplerende oplysninger, bør anses for at være oplysninger om en identificerbar fysisk person. For at afgøre, om en fysisk person er identificerbar, bør alle midler tages i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende. For at fastslå, om midler med rimelighed kan tænkes bragt i anvendelse til at identificere en fysisk person, bør alle objektive forhold tages i betragtning, såsom omkostninger ved og tid der er nødvendig til identifikation, under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling. Databeskyttelsesprincipperne bør derfor ikke gælde for anonyme oplysninger, dvs. oplysninger, der ikke vedrører en identificeret eller identificerbar fysisk person, eller for personoplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke eller ikke længere kan identificeres. Denne forordning vedrører derfor ikke behandling af sådanne anonyme oplysninger, herunder til statistiske eller forskningsmæssige formål*"

Databeskyttelsesforordningen gælder dermed ikke for oplysninger, som er fyldestgørende anonymiseret. Det er derfor centralt, hvad der forstås ved anonyme oplysninger. For at oplysninger kan betragtes som værende anonyme, må det hverken være muligt at identificere enkeltpersoner ud fra oplysningerne alene eller i kombination med anden information.

Det bør derfor overvejes, om andre kan have adgang til information, der i samspil med de anonyme oplysninger muliggør, at der – helt eller delvist – kan findes tilbage til den oprindelige personidentifikation. Anonymiseringen skal efter Datatilsynets praksis være uigenkaldelig, jf. nærmere pkt. 2.3.

Ved en umiddelbar læsning af præambelbetragtning 26, er anonymitet ikke et absolut "enten/eller"-begreb. Det første fremhævede afsnit angiver, at det ud fra en rimelighedsbetragtning skal vurderes, om der er midler som direkte og indirekte kan medvirke til identifikation af en fysisk person.

I vurderingen af, hvorvidt noget er anonymiseret, skal alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den dataansvarlige eller af enhver anden person, tages i betragtning. I praksis vil det fx betyde, at man i vurderingen af, om data er anonymiseret, er nødsaget til at vægte hvorvidt nogle andre parter har data som kan supplere de personoplysninger, som den dataansvarlige er i besiddelse af, således at den fysiske person kan identificeres.

Dette er også understøttet af retspraksis fra EU Domstolen i fx Breyer-dommen (C-582/14,), der dog blev afsagt i 2016 og altså før databeskyttelsesforordningen trådte i kraft.

I afgørelsen bemærkede Domstolen, at der godt kan foreligge momenter, der taler for at anse oplysninger som anonymiserede, selvom der objektivt set ikke er tale om anonyme oplysninger. Se præmisserne 42-45, der lyder:

”*42. Det er desuden anført i 26. betragtning til direktiv 95/46, at der for at afgøre, om en person er identificerbar, tages alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person, i betragtning.*

43. For så vidt som der i denne betragtning henvises til hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse, både af den registeransvarlige og af »enhver anden person«, synes det at følge af dens ordlyd, at det, for at en oplysning kan kvalificeres som »personoplysning« som omhandlet i nævnte direktivs artikel 2, litra a), ikke er påkrævet, at alle de oplysninger, der gør det muligt at identificere den registrerede, skal befinde sig hos en enkelt person.

44. Det forhold, at den yderligere viden, som kræves for at identificere brugeren af en internetside, indehaves, ikke af udbyderen af online-medietjenester, men af denne brugers internetudbyder, synes således ikke at kunne udelukke, at de dynamiske ip-adresser, der er registreret af udbyderen af online-medietjenester, for denne udgør personoplysninger som omhandlet i artikel 2, litra a), i direktiv 95/46.

45. Det skal imidlertid afgøres, om muligheden for at kombinere en dynamisk ip-adresse med den nævnte yderligere viden, som denne internetudbyder har, udgør et hjælpemiddel, der med rimelighed kan tænkes bragt i anvendelse for at identificere den registrerede.”

Domstolen åbner således op for, at der skal anlægges en rimelighedsbetragtning, når det vurderes, hvilke hjælpemidler der kan tages i brug for at kunne identificere fysiske personer. Det er vigtigt at være opmærksom på, at Breyer-dommens præmisser vedrører betragtning 26 i Direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (”databeskyttelsesdirektivet”). Når det er sagt, er de to betragtninger nr. 26 i hhv. databeskyttelsesforordningen og databeskyttelsesdirektivet dog stort set enslydende. I Danmark anlægger

Datatilsynet dog en strengere fortolkning, der er baseret på Artikel 29-gruppen, jf. nærmere afsnit 2.3.

Eksistensen af et oprindeligt datasæt hos en anden part, vil gøre det yderst vanskeligt at anonymisere den kopi af personoplysninger, som ønskes anvendt til forskningsformål. Eksempelvis i tilfælde, hvor man prøver at anonymisere personoplysninger, der er modtaget fra patientjournaler i medfør af en af sundhedslovens regler, mens de oprindelige personoplysninger fortsat er tilgængelige i patientjournalerne. Det afhænger selvsagt af konteksten, typen af oplysninger, antallet af registrerede i datasættet mv., og de foranstaltninger der træffes med henblik på anonymisering. Men findes det oprindelige datasæt, skal man nok være varsom med at konkludere data som værende anonyme, navnlig henset til kravene om iagttagelse af den teknologiske udvikling mv., jf. præambelbetragtning nr. 26.

Hvis der skal forsøges at opstille nogle minimumskrav for at anse data som anonymiseret, bør disse fire som minimum være opfyldt:

- Fjern alle eksterne/unikke identifikatorer - også løbenumre.
- Datoer og klokkeslæt skal enten
    - Fjernes,
    - Erstattes med beregnede afstande, fx kan ”indlæggelse 16/6 2019 - genindlæggelse 27/8 2019” ændres til ”indlæggelse - genindlæggelse: 73 dage” eller,
    - tilføres et 'slør' ved parallelforskydning med et tilfældigt antal dage fx +/- til 10 dage på individniveau, fx 'indlæggelse 16/6 2019' ændres til 'indlæggelse 11/6 2019' og ’genindlæggelse 27/8 2019' ændres til 'genindlæggelse 22/8 2019'.
- Fjern alle tekstfelter - erstat fx med kategorier, samt
- Reducér til absolut færrest mulige datafelter/variabler.

EU’s General Court har den 26. april 2023 afsagt dom i sagen T-557/20, hvori domstolen fastlægger, at der i vurderingen af, om der er tale om personhenførbare oplysninger, skal lægges vægt på, om modtageren af et datasæt kan identificere konkrete personer eller om en genidentifikation med rimelighed er mulig.

I overensstemmelse med Breyer-dommen fremgår det endvidere, at det må vurderes, om et modtaget datasæts kombination med et andet datasæt konkret er et middel, som med rimelighed kan anvendes til genidentifikation.

Eftersom det i sagen ikke var blevet undersøgt, om modtager af et datasæt rådede over midler, som i praksis kunne give adgang til de yderligere

oplysninger, der var nødvendige for genidentifikation, kunne det ikke konkluderes, at det modtagne datasæt var personoplysninger.

Dommen kan muligt være udtryk for en lempet praksis i forhold til hvornår et datasæt vurderes som værende anonymiseret og ikke alene pseudonymiseret. I så fald åbner det for en række spørgsmål, fx rækkevidden af afsenderens forpligtelser i relation til forudgående undersøgelser og efterfølgende kontrol. Det vurderes, at Datatilsynets stillingtagen til dommens rækkevidde må foreligge, førend eventuel praksisændring kan ske.

3. Forskellige tilsynsholdninger i EU-landene

Datatilsynets vurdering af, om personoplysninger kan anses for anonyme følger den tidligere "artikel 29"-gruppe. "Artikel 29"-gruppen bestod af repræsentanter fra alle de europæiske datatilsyn og er i dag erstattet af Det europæiske Databeskyttelsesråd.

"Artikel 29"-gruppen har i Opinion 05/2014 tilkendegivet, at data skal være anonymiseret på "uigenkaldelig" vis. Der er derfor umiddelbart en forskel til fortolkningen af den margin, som præambelbetragtning 26 i databeskyttelsesforordningen efterlader, som er gengivet ovenfor. "Artikel 29"-gruppens fortolkning må siges at være strengere end præambelbetragtning 26, idet ordet "uigenkaldelighed" i sig selv signalerer noget definitivt, mens præambelbetragtning 26 direkte i sin ordlyd rummer en vis adgang til ud fra objektive forhold at foretage en vurdering af rimelighedsbetragtningen.

Det vil alt andet lige være vanskeligere at anonymisere en personoplysning i Danmark fremfor i lande, hvor man fortsat anvender analoge registre, og hvor der er færre databaser at sammenkoble data med.

Efter "artikel 29"-gruppens henstillinger Opinion 05/2014 kræves yderligere, at en dataansvarlig løbende skal vurdere, om den teknologiske udvikling gør, at et datasæt ikke længere kan anses for anonymt. Det er imidlertid uklart, hvor vidtgående denne forpligtelse er til løbende at overvåge/gennemskue fremtidige muligheder, som følge af den teknologiske udvikling (eller om dette overhovedet er muligt i praksis). Det er derimod et opmærksomhedspunkt, som sagsbehandleren bør rådgive forskerne om, så det står klart, at vurderingen om anonymitet er dynamisk. I regionerne og på universiteterne kan det overvejes, om det på en eller anden måde kan dokumenteres, at det løbende er vurderet, om der er sket ændringer i teknologierne med henblik på vedvarende at sikre, at der ikke sker overtrædelse af databeskyttelsesreglerne.

4. Særligt om tredjelandsoverførsler

Der gælder særlige krav til overførsel af personhenførbare oplysninger til tredjelande og yderligere restriktive krav til overførsel til usikre tredjelande. Det er derfor altid relevant at tage stilling til, hvorvidt personoplysninger, der skal overføres fra Danmark til tredjelande, er pseudonymiserede eller anonymiserede, idet databeskyttelsesforordningens regler fortsat finder anvendelse på pseudonyme oplysninger.

Ved modtagelse af personoplysninger fra et tredjeland er det ligeledes nødvendigt, at den dataansvarlige foretager en vurdering på grundlag af dansk ret af, hvorvidt der er tale om anonymiserede oplysninger i henhold til databeskyttelsesforordningen, uanset om en udenlandsk samarbejdspart fra et tredjeland anser oplysningerne for anonyme efter den lokale ret, da databeskyttelsesforordningens anvendelsesområde gælder for personoplysninger, der behandles i Danmark. Dette gælder uanset om de er modtaget fra et tredjeland, hvor de er efter lokal ret kan være anset for værende anonyme data.

5. Konkrete datatyper og eksempler på vurderinger

5.1 Biologisk materiale

Biologisk materiale vil fx være blod, afføringsprøver, organer, mv. Udgangspunktet er, at biologisk materiale er at anse som personhenførbare oplysninger.

Der bør udvises tilbageholdenhed med at anse biologiske prøver for anonymiserede uanset metoden herfor. Uanset at en blodprøve ikke er forsynet med mærkat, navn, kode eller lignende , er det fortsat muligt at udlede en DNA-profil på en bestemt fysisk person. Den teknologiske udvikling på DNA sekvensering må på nuværende tidspunkt anses for et ”rimeligt hjælpemiddel” som skal tages i betragtning, jf. databeskyttelsesforordningens præambelbetragtning 26, så der kun er tale om indirekte personhenførbare oplysninger, selv om prøven ikke medfølges af yderligere oplysninger.

Synspunktet er også støttet af Datatilsynets bidrag til Justitsministeriets nationale evaluering af databeskyttelsesreglerne fra april 2021 , hvor Datatilsynet side 46, under høringen anfører følgende om biologisk materiale:

”Det er endvidere Datatilsynets forståelse, at der på nuværende tidspunkt ikke er påvist en kombination af teknologiske og organisatoriske midler, som effektivt kan anvendes for at udelukke biologisk materiale fra databeskyttelsesforordningens anvendelsesområde.”

Det kan ikke afvises, at der kan være undtagelser, ligesom det ikke er defineret, hvad Datatilsynet mener med "biologisk materiale". Fx kan det antages, at en plasmaprøve er så forvansket, at der ikke kan udtrækkes entydigt personhenførbare oplysninger ud af prøven i form af DNA. Dette skal dog ses i lyset af den teknologiske udvikling.

Under alle omstændigheder, må der i lyset af Datatilsynets udtalelse udvises påpasselighed med at konkludere at biologisk materiale er anonymt.

5.2 Røntgen- og scanningsbilleder

Et røntgenbillede og et scanningsbillede (fx CT-scanning, PET-scanning, MR-scanning, ultralydsscanning) af en person, et organ, en knogle mv. er som udgangspunkt at anse for en personhenførbar oplysning.

Spørgsmålet er, om det pågældende billede i sig selv kan identificere personen (direkte personhenførbart), og/eller om billedet først bliver personhenførbart, når det kobles sammen med en anden kilde (indirekte personhenførbart).

Såfremt et scanningsbillede viser fx en unik detalje om en person, så personen kan genkendes umiddelbart, er billedet i sig selv personhenførbart.

Viser scanningsbilledet i stedet alene et organ, fx hjertet, men har billedet i øvrigt ikke andre personhenførbare oplysninger ud over et ID-nummer, der er linket til patientjournalen, vil scanningsbilledet umiddelbart være at anse for pseudonymt – efter omstændighederne endda måske direkte personhenførbart.

Hvis ID-nummeret og øvrige metadata er slettet fra scanningsbilledet af hjertet, da vil scanningsbilledet ikke længere direkte kunne henføres til en bestemt person. Det kan imidlertid ikke udelukkes at man med det pågældende scanningsbillede kombineret med muligheden for at gennemsøge regionens database/patientjournaler vil kunne finde et match med det konkrete hjerte, hvis vedkommende fx har været scannet før. Det kan også være, at billedet er så unikt, at personen alligevel kan genkendes ud fra scanningsbilledet.

I sådan en situation bliver det en afvejning af, hvad der må betragtes som et "rimeligt hjælpemiddel", jf. databeskyttelsesforordningens præambelbetragtning 26, hvorefter det vil være en konkret vurdering, idet der er tale om en gråzone.

Det skal holdes for øje, at sådanne scanningsbilleder typisk vil være kildedata, hvor det vil være teknisk muligt, at tilbageføre oplysningerne til de originale data i kildesystemet. Det er heller ikke utænkeligt, at der kan ske identifikation

af en person på et ellers anonymiseret billede på et senere tidspunkt som følge af den teknologiske udvikling.

Skal der i forbindelse med et forskningsprojekt ske publikation, kan der udover databeskyttelsesretlige regler, ligeledes gælder etiske standarder for dokumentation, opbevaring af data mv. Det er derfor altid en supplerende overvejelse i rådgivningen, om forskeren overhovedet kan "nøjes" med anonyme data.

Nedenfor gives tre konkrete eksempler på juridiske vurderinger i forhold til eventuel anonymisering af scanningsbilleder:

Ex 1 - scanningsbilleder af ryghvirvler

I konkret sag henvendte en forsker sig for at høre, hvorvidt han måtte dele/videregive en stor mængde scanningsbilleder af ryghvirvler (ca. 30.000 billeder) med en privat virksomhed. Billederne var trukket ud af PACS på baggrund af en tilladelse.

Virksomheden skulle træne en AI-løsning (virksomhedens formål). Forsker mente at der var tale om anonyme oplysninger.

Regionens juridiske vurdering var, at som udgangspunkt var scanningsbillederne ikke anonyme. Man måtte formode, at for at træne en AI-løsning, måtte der nødvendigvis være forskel på billederne, særligt hvis AI-løsningen skulle genkende en abnormalitet. I vurderingen heraf indgik tillige om der var en mulighed for, at en radiolog eller læge ville kunne huske eller genkende tidligere kendetegn, operationer, abnormaliteter eller andet. Som led i den juridiske vurdering inddrog man forskernes knowhow. De deltagende forskere kunne afkræfte dette set fra et forskningsmæssigt perspektiv. Herefter blev den juridiske konklusion, at oplysningerne kunne anonymiseres. Regionen fremsendte herefter oplysningerne til virksomheden.

Ex 2- pseudonymiserede data

I forbindelse med et projekt om udvikling af nye metoder til at analysere medicinske billeddata af personer skulle en udenlandsk samarbejdspartner (inden for EU) modtage billeddata fra en dansk forskningsinstitution (PET og CT billeder). Billederne dækkede reelt set hele "kroppen".

I første omgang blev behandlings- og overførselsgrundlag undersøgt. De oprindelige billeder var indhentet på baggrund af samtykke, i hvilken sammenhæng det var oplyst for patienterne, at billederne kun ville blive anvendt til et forskningsprojekt i DK. Der skulle derfor indhentes nyt samtykke til videregivelse af billederne og til den nye behandlingsaktivitet. Derfor opstod spørgsmålet om anonymisering idet billederne i så fald ville kunne deles med samarbejdsparten uden iagttagelse af de databeskyttelsesretlige regler.

Vurderingen var, at scanningsbillederne som udgangspunkt var pseudonymiserede personoplysninger. Forskeren (regionen) blev gjort udtrykkeligt opmærksom på, at anonymitet i databeskyttelsesretlig forstand indebærer, at billederne på "uigenkaldelig" vis blev gjort både direkte og indirekte ikke-personhenførbare. Der var herefter dialog, hvorvidt dette kunne lade sig gøre. Fx ved at slette alle navne, tal, numre, osv. fra billederne. Men der var enighed om, at så omfattende billeder ikke kunne anonymiseres, da dette ikke kunne anses for at være en uigenkaldelig foranstaltning, således at personerne bag billederne ikke længere kunne

identificeres. Den danske institution ville stadig være i stand til at kunne sammenholde billederne med andre indikatorer og identificere personerne. Billederne blev derfor pseudonymiseret, og der blev udarbejdet og indhentet nyt samtykke med henblik på videregivelse under iagttagelse af de databeskyttelsesretlige krav hertil.

Ex 3 - anonyme data

Et dansk hospital skulle foretage nogle scanningsbilleder af i alt ca. 100-150 patienters ene organ. Efter scanningen skulle "billederne" bearbejdes yderligere, så der kom en slags visuel model af et organ ud af det. Dvs. det var ikke et egentlig scanningsbillede af et organ men et visuel kodet modelbillede i farver og tal. Farverne og tallene ville variere alt efter patientens helbredstilstand, alder mv. Billederne gengav ikke den faktiske fysiske form af organet.

Modelbilledet kunne i sig selv ikke identificere personerne. Dette ville kræve, at en "trænet" forsker fik et almindeligt scanningsbillede af organet at sammenholde modelbilledet med.

Modelbilledet skulle efter den interne færdiggørelse deles med en udenlandsk forskningsinstitution (uden for EU) med henblik på analyse og fælles publikation.

Det blev oplyst fra forskerens (regionens) side, at det var uden betydning for forskningsprojektet, om man kendte identiteten på personerne bag modelbillederne, og derfor gjorde man alt for at anonymisere data, så de lettere kunne deles med samarbejdsparten. Blandt andet slettede man på hospitalet samtlige scanningsbilleder og indikatorer til genkendelse af patienten i de interne fortegnelser og systemer, når modelbilledet var udarbejdet for den enkelte patient (Dette havde forskerne endvidere vurderet var overensstemmende med gældende code of conduct-regler). Man sendte endvidere først modelbillederne til samarbejdsparten, når der var mindst 10 stk. Dvs. på afsendelsestidspunktet var det eneste tilbage på hospitalet alene modelbilledet.

Vurderingen var, at modelbillederne blev anset for at være personoplysninger. Men henset til de foranstaltninger, der blev gjort, således at ingen hverken hos afsender eller modtager kunne sammenkoble data og/eller genskabe patienternes identitet, blev konklusionen, at man kunne anse modelbillederne for anonyme oplysninger. Regionen er dog opmærksom på, at der gælder en vedvarende forpligtelse (selvom det er uklart, hvad rækkevidden er, jf. præambelbetragtning 26) til at iagttage den teknologiske udvikling, som muligvis vil indebære, at man i fremtiden kan genskabe identiteten på de deltagende patienter alene ud fra modelbillederne.

5.3 Registerforskningsdata – "tørre" data

Nogle projekter er designet således, at de fra begyndelsen tager højde for et ønske om brug af anonymiseret data, da identiteten på respondenterne ikke er central for forskningsprojektet. Dette ses typisk inden for registerforskning eller andre typer af forskning, hvor det er samlinger af "tørre" data som eksempelvis spørgeskemasvar, interview-svar, observationer mv. Kendetegnet for disse typer indsamlinger er, at data indsamles direkte hos den registrerede, men at den registreredes identitet ikke er relevant. Det er den samlede mængde svar, der har betydning for forskeren.

I disse projekter kan man på grund af mængden af indsamlet data designe studiet således, at man ved indsamlingen har taget højde for, at der ikke bliver registreret personhenførbare oplysninger.

I visse projekter, anvender man "tørre" data udledt af fx biologisk materiale. Det vil afhænge af en konkret vurdering, om sådanne "tørre" data er anonyme, herunder om det tørre datasæt i sig selv indeholder er personhenførbare oplysninger, hvorvidt det biologiske materiale fortsat er tilgængeligt, /eller om man fortsat kan koble de tørre data med andre oplysninger mv. Det vil bero på en konkret vurdering.

Ex 1 – telefoninterviews indsamlet anonymt

I en sag blev et datasæt videregivet fra en telefonhjælpelinje vedrørende ludomani. Datasættet indeholdt blandt andet oplysninger om ca. størrelsen på økonomisk tab, antal tidligere gange vedkommende eventuelt har søgt om hjælp, dato og køn. Der var tale om et datasæt med et højt antal respondenter. Men navn, alder, adresse mv. blev ikke indsamlet; folk ringede ind anonymt, og der var ikke nogen "nøgle", der kunne føre tilbage til personerne.

Vurderingen var, at der var tale om anonyme oplysninger. Telefonhjælpelinjen registrerede som nævnt ikke yderligere oplysninger om den enkelte. Heller ikke telefonopkaldet i sig selv kunne bruges som identifikation, idet der var mange opkald om dagen.

6. Sammenfatning

Begrebet pseudonymisering er i databeskyttelsesforordningen defineret som behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke kan henføres til en identificeret eller identificerbar fysisk person.

Oplysninger, der er gjort anonyme, sådan at ingen fysiske personer kan identificeres ud fra oplysningerne eller i kombination med andre oplysninger, er derimod ikke længere beskyttet af databeskyttelsesreglerne. Det skyldes, at databeskyttelsesreglerne kun finder anvendelse, så længe oplysningerne kan føres tilbage til en identificerbar eller identificeret fysisk person. Det er en betingelse, at anonymiseringen er uigenkaldelig. I vurderingen af om oplysninger er anonymiseret, skal alle hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende person tages i betragtning. Der skal også være øje for, om andre er i besiddelse af oplysninger, der gør det muligt at identificere den enkelte.

Det er en gennemgående konklusion i vejledningen, at det i praksis er vanskeligt at foretage en tilstrækkelig anonymisering - henset til den teknologiske

udvikling og de mange eksisterende datakilder på området for sundhedsforskning, f.eks. patientjournaler, databaser og nationale registre.

Det bemærkes desuden, at en vurdering af om personoplysninger er pseudonymiserede eller anonymiserede altid forudsætter en konkret vurdering. Formålet med denne vejledning er derfor at lette de dataansvarlige myndigheders individuelle juridiske vurderinger ved bl.a. ved at skabe overblik over lovgivningen samt ved hjælp af eksempler fra praksis. Vejledningen kan anvendes, indtil at Datatilsynets kommende vejledning er en realitet, men bidrager ikke med ny praksis på området. Nærværende vejledning vil blive genbesøgt, når Datatilsynets nye vejledning er offentliggjort.