Notat om hjemmelsgrundlag for behandling af oplysninger i app til smitteopsporing til COVID-19-bekæmpelse – 1. udkast

1. FORMÅL OG KONKLUSION

Sundheds- og Ældreministeriet har anmodet om en vurdering af, om Styrelsen for Patientsikkerhed har hjemmel til som dataansvarlig at etablere og behandle personoplysninger i en app til mobile enheder til brug for COVID-19-bekæmpelse. Ministeriet har i et tværgående samarbejde påbegyndt udviklingen af appen, der vil blive udviklet i 3 faser (releases). Det er ambitionen, at appen skal downloades og anvendes af langt størstedelen af Danmarks befolkning, og appen vil bl.a. indebære behandling af oplysninger om helbredsforhold og geolokation på brugerne.

Det er aftalt med ministeriet, at vurderingen foretages ud fra de gældende regler i epidemiloven, databeskyttelsesforordningen og -loven samt e-databeskyttelsesreglerne. Sundheds- og Ældreministeriet foretager selv i samarbejde med Styrelsen for Patientsikkerhed en vurdering af eventuelle begrænsninger i muligheden for anvendelse af data efter den øvrige sundhedslovgivning, herunder sundhedsloven. Det er en del af vurderingen, om det er retligt nødvendigt eller hensigtsmæssigt at vedtage ny lovgivning for at sikre det fornødne og hensigtsmæssige hjemmelsgrundlag for løsningen.

Som nærmere begrundet nedenfor i afsnit 4 kan mine konklusioner og anbefalinger sammenfattes som følger:

- Styrelsen for Patientsikkerhed vil kunne etablere og anvende app'en samt behandle de dermed forbundne personoplysninger i fase 1-3 ud fra en model 1 ved indhentelse af samtykke fra de registrerede efter cookiebekendtgørelsens § 3 og databeskyttelsesforordningens artikel 6, stk. 1, litra a, og artikel 9, stk. 2, litra a. Dette synes også bedst i overensstemmelse med ministeriets og styrelsens forudsætning om frivillighed. For så vidt angår fase 3, kan det dog overvejes at regulere dataindsamlingen henset til den meget omfattende indsamling af geolokationsoplysninger, om end der ikke vil være pligt hertil. En nærmere regulering vil kunne ske ved lov eller i bekendtgørelsesform med hjemmel i epidemilovens bemyndigelsesbestemmelser, smh. databeskyttelseslovens § 7, stk. 5.
- Man skal være opmærksom på, at modellen indebærer, *at* Styrelsen for Patientsikkerhed skal kunne dokumentere samtykkerne, deres indhold og tidspunktet for dem, og *at* borgerne løbende skal give samtykke i takt med fase 1-3, *at* borgerne har ret til at trække deres samtykke tilbage, hvorefter behandlingen af oplysninger i personhenførbar form skal stoppe. Det sidstnævnte vil indebære, at oplysnin-

gerne om kontaktregistreringerne, helbredsforhold, geolokation m.v. skal slettes i appen samt i den bagvedliggende database, idet der dog kan være pligt til at opretholde opbevaringen af data i henhold til arkivlovgivningen, i hvilket tilfælde der vil skulle ske begrænsning af brugen af dataene. Modellen indebærer tillige, *at* samtykket vil skulle opdateres, hvis der i øvrigt sker væsentlige ændringer i behandlingen undervejs, samt *at* der vil være ret til dataportabilitet af dataene, hvilket skal bygges ind i løsningen.

- Som et alternativ til samtykke kan styrelsen vælge en model 2, hvorefter løsningen baseres helt eller delvist på øvrige grundlag end samtykke, dvs. hvor behandlingen helt eller delvist baserer sig på eksisterende eller ny regulering. Det kan her bl.a. overvejes, om epidemiloven og bekendtgørelser udstedt i medfør deraf kan udgøre et grundlag for visse behandlinger, evt. sammenholdt med bemyndigelsesbestemmelsen i databeskyttelseslovens § 7, stk. 5.
- Hvis der ikke anvendes samtykke til behandlingen af personhenførbare geolokationsdata, kan det give anledning til principielle spørgsmål om dataminimering, opbevaringsbegrænsning og behovet for at sikre et sikkert hjemmelsgrundlag, som man i givet fald må genbesøge inden påbegyndelsen af fase 3. Under alle omstændigheder er det vigtigt at være opmærksom på, at lagring af eller adgang til oplysninger på borgernes mobile enheder vil kræve et samtykke efter cookiebekendtgørelsens § 3, jf. e-databeskyttelsesdirektivets artikel 5, stk. 3. En fravigelse heraf vil kræve national regulering, jf. e-databeskyttelsesdirektivets artikel 15.

2. BEHANDLING AF OPLYSNINGER I SPORINGSAPPEN

Til brug for min undersøgelse har jeg modtaget en række forskelligt materiale og beskrivelser af sporingsappens udvikling. Nærværende notat tager udgangspunkt i beskrivelsen af appens udviklingsfaser og behandling af oplysninger i Styrelsen for Patientsikkerheds notat af 7. april 2020 vedrørende databeskyttelsesretlige overvejelser i forbindelse med introduktion af app til smitteopsporing samt yderligere oplysninger modtaget fra Styrelsen fra Patientsikkerhed den 8. april 2020.

Det fremgår af det modtagne materiale, at regeringen har besluttet at iværksætte udviklingen af en app til smitteopsporing til brug for genåbningen af Danmark i forbindelse med den igangværende Corona/COVID-19-epidemi, og at appen er tænkt udviklet i tre faser (releases):

- Fase 1: Kontaktregistrering (planlagt release den 22. april 2020)
- Fase 2: Smitteoplysning (planlagt release den 5. maj 2020)
- Fase 3: Geolokation (planlagt release den 29. maj 2020)

De overordnede formål med appen er *at* give den enkelte borger indsigt i egne kontaktmønstre – dvs. hvor mange kontakter vedkommende har på en dag – *at* give den enkelte borger mulighed for at træffe relevante foranstaltninger, når vedkommende er blevet udsat for smitte, samt *at* give myndighederne mulighed for at monitorere kontaktmønstre i Danmark med henblik på at understøtte genåbningen af samfundet.

Det er Digitaliseringsstyrelsen, der er udviklingsleverandør af appen. Netcompany er underleverandør på appen i forhold til udvikling og drift. Det er endnu ikke afklaret, om Netcompany anvender underleverandører, herunder om lagringen af data vil basere sig på en cloudløsning. Det er Styrelsen for Patientsikkerhed, der skal være dataansvarlig for appen og den dermed forbundne behandling af oplysninger. Det er oplyst, at oplysningerne, der indsamles via appen hos borgerne, lagres lokalt på brugernes mobile enheder samt i et centralt repository (database).

Appen til digital kontaktsporing bygger på følgende forudsætninger:

1. Frivillighed: En app til digital kontaktopsporing i Danmark vil basere sig på frivillighed, dvs. at borgere kan vælge at downloade appen og opsamle oplysninger om kontakter og lokationer. Borgeren vil derudover tage stilling til, om borgeren ønsker at dele oplysninger om kontakter og lokationer med myndighederne, hvis pågældende bliver konstateret smittet, og om pågældende ønsker at dele oplysningen om smitte med kontakterne. Princippet om frivillighed betyder, at oplysninger i appen ikke vil blive brugt som kontrol af borgernes bevægelse rundt i landet, som tilsvarende apps er blevet benyttet i f.eks. Kina.
2. Pseudonymiserede og aggregerede data: Et andet princip er, at når myndighederne anvender data fra appen på at følge op på smitteudbredelsen, sker det udelukkende med data på pseudonymiseret og aggregeret niveau. Data kan anvendes til at vurdere, om det giver anledning til at åbne nogle områder hurtigere end andre eller rådgive enkeltinstitutioner om hensigtsmæssig adfærd for at reducere smittet.
3. Ingen restriktioner for borgerne: Myndighederne vil ikke bruge data til på individniveau at pålægge enkelte borgere restriktioner, hvis de ikke opfylder karantænekrav og har for mange kontakter, efter de er konstateret smitte.
4. Ikke en klinisk app: Appen tjener ikke et klinisk formål og skal ikke indeholde selvrapportering af symptomer til brug for selvvurdering af egen sygdom eller lignende. Det vil udgøre en patientrisiko og kan give fejlkilder, både hvor folk over- eller underrapporterer egne symptomer. Oplysninger om smitte i appen baseres på certificerede myndighedstest, og dermed data som allerede ligger hos sundhedsmyndighederne.
5. Appen anvendes kun i forbindelse med COVID-19: Appen forventes kun at skulle anvendes, så længe det er relevant, f.eks. i resten af 2020.

2.1 Fase 1 – Kontaktregistrering (planlagt release den 22. april 2020)

I fase 1 vil der efter det oplyste indsamles oplysninger om, hvor mange kontakter en borger, der har downloadet appen, har haft i løbet af en dag med andre personer, der har downloadet appen. Der indsamles og registreres ikke oplysninger om lokationen og hvem, borgeren har haft kontakt med. Der vil endvidere ikke være oplysninger om, hvorvidt dem, som borgerne har været i kontakt med, er smittet eller har antistoffer.

Oplysninger om borgerens kontakter med andre borgere indsamles via Bluetooth/Beacon-teknologi, dvs. de pågældende mobile enheders fysiske afstand til hinanden, varigheden af kontakten og eventuelt tidsstempel for kontakten.

Der sondres mellem, om borgeren har været "tæt på", "i nærheden af" og "langt fra". "Tæt på" defineres som enten en person, man har været meget fysisk tæt på (håndtryk, kys, selfie mv.), eller en person, som man har befundet sig i samme lokale med i mindre end 2 meters afstand i mere end sammenlagt 15 minutter. Borgeren skal således have været "tæt på" en anden i en kortere tidsmæssig udstrækning for at tælle som en kontakt, "hvor i nærheden af" skal tælle op til 15 minutter.

Borgeren vil på sin app kunne se, hvor mange kontakter borgeren har haft i dag, evt. fordelt over dagen. Der vil evt. udvikles en funktionalitet, der gør det muligt for borgeren at sammenligne med de foregående dage/uger, f.eks. "i dag ligger du højere end dit gennemsnitlige niveau for de seneste 7 dage". Og der vil evt. udvikles funktionalitet, der gør, at borgeren kan sammenligne med gennemsnittet for samtlige app-brugere.

Myndighederne kan i fase 1 få opgørelser af antal kontakter med potentiel smitterisiko fordelt på antal app-brugere, og evt. fordelt over tid på dagen.

Statens Serum Institut (SSI) har et ønske om, at der allerede i fase 1 indsamles oplysninger om køn og alder. Dette ønsker SSI, da det kan give viden om, hvilke befolkningsgrupper fordelt på køn og alder, der er gode til at holde afstand og hvilke der er mindre gode til det. Disse oplysninger kan indsamles og registreres, hvis appen i fase 1 lanceres med NemID-login. Alternativt kan der indbygges en funktionalitet, hvor borgerne selv indtaster denne information.

Appen er tænkt designet således, at første gang brugeren downloader appen, og denne kontakter serveren, kreerer og giver serveren hver bruger et ID, som gemmes på telefonen. Dette ID mappes ikke til telefonens MAC-adresse, og serveren gemmer ikke telefonernes MAC-adresser. ID'er bruges kun til, at telefonerne kan fortælle serveren, hvilket andet anonymt ID, telefonerne har registreret et møde med, når telefonerne kommer tæt på hinanden. Når MAC-adressen er slettet, er der således ikke en kobling mellem appen og den fysiske telefon, ligesom der ikke er en registrering af kobling mellem telefon og borgeren.

2.2 Fase 2 – Smitteoplysning (planlagt release den 5. maj 2020)

I fase 2 vil appen løbende tjekke op mod registrerede smittetilfælde via opslag i MiBA (Mikrobiologisk Bank). Borgeren kan i fase 2 således gennem integrationen til MiBA på sin app få besked, hvis borgeren er smittet med COVID-19, samt vælge at give besked til de kontakter, der har downloadet appen og potentielt har været udsat for smitterisiko, hvis borgeren er smittet.

Fase 2 forudsætter, at borgeren logger ind med NemID for at sikre den fornødne sikre identifikation af borgeren, samt at der videregives data fra MiBA til appen. Det er Statens Serum Institut, der driver og er dataansvarlig for MiBA, og der vil som led i fase 2 således ske en videregivelse af personhenførbare oplysninger om smittestatus og immunitetsstatus fra Statens Serum Institut til Styrelsen for Patientsikkerhed. Denne videregivelse vil ske gennem Sundhedsstyrelsen, der vil stå for integrationen mellem MiBA og appen. Det konkrete dataflow og setup skal afklares yderligere.

Den enkelte borger kan endvidere på sin app vælge at få besked, hvis en af de kontakter, borgeren har haft, og som har downloadet appen, er blevet smittet med COVID-19 og dermed kan have udgjort en smitterisiko for borgeren. Det er endnu ikke afklaret, hvor mange informationer der vil blive givet til borgeren om, hvornår borgeren er blevet udsat for smitterisiko, herunder om borgeren skal have det konkrete kontakttidspunkt at vide. Viden om det konkrete tidspunkt for kontakten med en anden smittet borger vil således efter omstændighederne potentielt give borgeren mulighed for at kunne udlede identiteten på den anden smittede borger (hvis man f.eks. har haft et 1:1 møde), hvorved der således potentielt vil ske en videregivelse af en helbredsoplysning.

Myndighederne kan i fase 2 få opgørelser af antal kontakter med potentiel smitterisiko fordelt på køn og alder, samt få opgørelser af antal kontakter koblet til faktisk smittede.

Telefonens MAC-adressen vil i fase 2 fortsat udskiftes med et ID, men der vil være en nøgle, der kan koble borgerens NemID og dette ID. Nøglen vil blive opbevaret hos Netcompany.

2.3 Fase 3 – Geolokation (planlagt release den 29. maj 2020)

Fase 3 vil indebære, at der sker en geografisk placering af samtlige de borgere – dvs. smittede såvel som ikke-smittede – der har downloadet appen baseret på GPS.

Fase 3 vil gøre det muligt for borgeren på sin app at se, hvilke områder borgeren normalt færdes i, hvor der er ekstra stor risiko for at opleve kontakter med potentiel smitterisiko. Fase 3 vil endvidere gøre det muligt at få opgørelser af antal kontakter med potentiel smitterisiko fordelt på geografiske lokationer.

En række forhold vedrørende fase 3 er endnu uafklaret, herunder hvor mange informationer der vil blive givet til borgeren om, hvornår borgeren er blevet udsat for smitterisiko, da det i fase 3 også vil være muligt at give oplysninger om sted for smitterisiko. Hvis der gives informationer om både tid og sted for smitterisiko til borgeren, vil dette potentielt give borgeren mulighed for at kunne udlede identiteten på den anden smittede borger, hvorefter der således potentielt vil ske en videregivelse af en helbredsoplysning.

Det skal endvidere afklares, hvad myndighedernes reaktionsmuligheder er på baggrund af de informationer, som der indsamles om potentiel smitterisiko fordelt på geografiske lokationer. Det er som anført ovenfor en forudsætning, at oplysningerne ikke vil blive anvendt til at indføre restriktioner eller sanktioner over for den enkelte borger. Men det er fortsat uafklaret, hvor små geografiske områder myndigheder skal have mulighed for at indføre restriktioner i relation til, f.eks. om myndighederne på baggrund af de informationer, som de får via appen, skal kunne lukke en bestemt børnehave eller strand, hvor der er konstateret mange smittede borgere. Det skal ses i lyset af, at det kan være vanskeligt for myndighederne at have viden om konkret stor smitterisiko et bestemt sted uden at reagere på det med konkrete tiltag for at begrænse smitten.

3. RETSGRUNDLAGET

3.1 Epidemiloven

Det følger af § 21 a i lov om foranstaltninger mod smitsomme og andre overførbare sygdomme (epide-miloven)[1], at sundheds- og ældreministeren kan fastsætte regler om fysiske og juridiske personers samt myndigheders oplysningsforpligtelser for at hindre udbredelse og smitte af en bestemt sygdom omfattet af lovens § 2. Endvidere følger det af lovens § 21 b, at sundheds- og ældreministeren kan fastsætte regler om, at personoplysninger kan behandles, hvis behandlingen er nødvendig for at hindre udbredelsen og smitte af en bestemt sygdom omfattet af lovens § 2.

Bestemmelserne i §§ 21 a og 21 b blev indsat ved lov nr. 208 af 17. marts 2020 om ændring af lov om foranstaltninger mod smitsomme og andre overførbare sygdomme (Udvidelse af foranstaltninger til at forebygge og inddæmme smitte samt sikring af kapacitetsmæssige ressourcer m.v.).

Det fremgår om § 21 a af lovforslagets bemærkninger, at bestemmelsen vil kunne tænkes anvendt til at fastsætte regler om, at personer, der har opholdt sig i zoner, hvor sundhedsmyndighederne har fundet, at der er stor risiko for smittespredning, skal afgive oplysninger herom. Desuden fremgår det, at bestemmelsen ligeledes vil kunne tænkes anvendt til at fastsætte regler om, at f.eks. virksomheder skal afgive betalingsoplysninger eller lignende med henblik på kontaktopsporing med henblik på at sikre mulighed for at målrette information om risiko for smitte af en bestemt sygdom, der er omfattet af lovens § 2. Endelig fremgår det, at der vil kunne ske en behandling af personoplysninger i medfør af de regler, som fastsættes efter bestemmelsen, og at databeskyttelsesforordningen og databeskyttelsesloven i den forbindelse vil skulle iagttages, med mindre behandlingen falder uden for forordningens anvendelsesområde.

For så vidt angår § 21 b, fremgår det af lovforslagets bemærkninger, at formålet med bestemmelsen er at sikre, at der hurtigt kan fastsættes regler om, at personoplysninger kan behandles, hvis der er behov for det, eksempelvis som led i smittespredning af en bestemt sygdom. Det fremgår, at der vil kunne fastsættes regler, som giver mulighed for at både private og offentlige aktører kan behandle personoplysninger. Fastsættelse af sådanne regler vil kunne være relevant, hvis der er behov for, at der hurtigt tilvejebringes hjemmel til, at private aktører kan videregive personoplysninger til offentlige myndigheder med henblik på bl.a. at inddæmme smittespredning. Bestemmelsen ændrer ikke ved den adgang, som private og offentlige aktører har efter gældende databeskyttelsesretlige regler til at behandle, herunder videregive, oplysninger. Endelig fremgår det, at databeskyttelsesforordningen og databeskyttelsesloven vil skulle iagttages i forbindelse med den behandling af personoplysninger, som vil finde sted i medfør af regler fastsat efter bemyndigelsesbestemmelsen, og at Datatilsynet forudsættes at blive hørt over regler, som udstedes i medfør af bestemmelsen, jf. databeskyttelseslovens § 28.

Der er udstedt to bekendtgørelser med hjemmel i §§ 21 a og 21 b – bekendtgørelse nr. 216 af 17. marts 2020 og bekendtgørelse nr. 347 af 30. marts 2020. Bekendtgørelserne hedder begge bekendtgørelse om oplysningsforpligtelser samt behandling af personoplysninger med henblik på at hindre udbredelse og smitte i forbindelse med håndtering af Coro-

[1] Lovbekendtgørelse nr. 1026 af 1. oktober 2019, som ændret ved lov nr. 208 af 17. marts 2020 og lov nr. 359 af 4. april 2020.

navirussygdom 2019 (COVID-19), og de har samme indhold (om end lidt formuleringsmæssige forskelle), bortset fra, at nr. 216 trådte i kraft den 18. marts 2020, mens nr. 347 trådte i kraft den 4. april 2020. Begge bekendtgørelser ophæves den 1. juni 2020. Det er uklart, hvorfor der er udstedt to bekendtgørelser med samme indhold.

Efter begge bekendtgørelsers § 1 er juridiske personer forpligtet til efter anmodning fra Styrelsen for Patientsikkerhed eller politiet at afgive relevante oplysninger, når det er nødvendigt med henblik på at hindre udbredelsen af Coronavirussygdom 2019 (COVID-19). I bekendtgørelse nr. 216 nævnes som eksempler oplysninger om navn og adresse på betalingskortindehaver, tid og sted for betalingstransak-tioner samt oplysninger, der kan tjene til at stedfæste en slutbruger i forbindelse med dennes anven-delse af elektroniske kommunikationsnet eller -tjenester. Det anføres i § 1 i begge bekendtgørelser, at der i den forbindelse kan behandles personoplysninger omfattet af artiklerne 6 og 9 i databeskyttelsesforordningen.

Efter begge bekendtgørelsers § 2 er fysiske personer forpligtet til efter anmodning fra Styrelsen fra Patientsikkerhed eller politiet at afgive oplysninger om personens forudgående opholdssted i ind- eller udland samt oplysninger om, hvem personen har været i kontakt med under opholdet. Der kan efter bestemmelserne i den forbindelse behandles personoplysninger omfattet af artiklerne 6 og 9 i databeskyttelsesforordningen. Endvidere fremgår det af bestemmelserne, at Styrelsen for Patientsikkerhed og politiet kun kan anmode om oplysningerne, når det er nødvendigt med henblik på at hindre udbredelse og smitte af Coronavirussygdom 2019 (COVID-19).

Efter begge bekendtgørelsers § 4 videregiver Statens Serum Institut efter anmodning fra Styrelsen for Patientsikkerhed personoplysninger, som Statens Serum Institut har modtaget i henhold til § 1 i Sundhedsstyrelsens bekendtgørelse nr. 198 af 13. marts 2020, til Styrelsen for Patientsikkerhed til brug for styrelsens beslutning om påbud i medfør af § 5, stk. 1, i epidemiloven. Styrelsen kan kun anmode om oplysningerne, når det er nødvendigt med henblik på at hindre udbredelsen og smitte af Co-ronavirussygdom 2019 (COVID-19). Epidemilovens § 5, stk. 1, giver sundheds- og ældreministeren mulighed for at give påbud om undersøgelse, indlæggelse eller isolation til enhver, der lider af en alment farlig sygdom, eller som formodes at kunne være smittet med en sådan.

3.2 Databeskyttelsesforordningen og -loven

3.2.1 Personoplysninger, anonymisering og pseudonymisering

Databeskyttelsesforordningen[2] og databeskyttelsesloven[3] indeholder en generel regulering af behandling af personoplysninger.

[2] 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).

[3] Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Personoplysninger er defineret som enhver form for information om en identificeret eller identificerbar fysisk person ("den registrerede"); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet, jf. forordningens artikel 4, nr. 1.

Ved fastlæggelsen af, hvad der nærmere ligger i begrebet, kan der ifølge betænkning 1565, s. 58 f, også lægges vægt på forordningens præambelbetragtning nr. 26, hvoraf det fremgår, at principperne for databeskyttelse bør gælde for enhver information om en identificeret eller identificerbar fysisk person. Det fremgår endvidere af betragtningen, at 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. Det fremgår desuden, at 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. Herudover fremgår det af betragtningen, at 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. Det fremgår endvidere af betragtningen, at databeskyttelsesprincipperne derfor ikke bør 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. Endelig fremgår det af betragtningen, at forordningen derfor ikke vedrører behandling af sådanne anonyme oplysninger, herunder til statistiske eller forskningsmæssige formål.

Det fremgår endvidere af præambelbetragtning nr. 30, at fysiske personer kan tilknyttes onlineidentifikatorer, som tilvejebringes af deres enheder, applikationer, værktøjer og protokoller, såsom IP-adresser og cookieidentifikatorer, eller andre identifikatorer, såsom radiofrekvensidentifikationsmærker. Det fremgår desuden af betragtningen, at dette kan efterlade spor, der, navnlig når de kombineres med unikke identifikatorer og andre oplysninger, som serverne modtager, kan bruges til at oprette profiler om fysiske personer og identificere dem.

I praksis må det antages, at både dynamiske og statiske IP-adresser udgør personoplysninger omfattet af databeskyttelsesforordningen, jf. EU-Domstolens domme i henholdsvis sag C-582/14, Breyer og sag C-70/10, Scarlet Extended, jf. herved også Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udg., 2020, DJØF, s. 247.

Den såkaldte Artikel 29-Gruppe (nu Det Europæiske Databeskyttelsesråd) har i udtalelse nr. 02/2013 af 27. februar 2013 udtalt sig om databeskyttelse i apps i intelligente enheder (WP 202), herunder databeskyttelsesreglernes overholdelse i relation til apps. Det fremgår heraf på s. 8 bl.a., at mange af de typer oplysninger, der lagres på eller genereres af intelligente enheder, er personoplysninger, herunder position, kontakter, unik enheds- og kundeidentifikatorer (f.eks. IMEI13, IMSI14, UDID15 og mobiltelefonnummer), den registreredes identitet, telefonens identitet, kreditkort- og betalingsdata, opkaldsregistrering, SMS eller instant messaging, browsinghistorik, e-mail, informationssamfundstjenesters autentifice-

ringsoplysninger (herunder især tjenester med sociale funktioner), billeder og video samt biometri (f.eks. ansigtsgenkendelse og fingeraftryksskabeloner).

Tilsvarende har Artikel 29-Gruppen forholdt sig til geolokaliseringstjenester i intelligente mobile enheder i udtalelse nr. 13/2011 af 16. maj 2011 (WP 185), hvor gruppen forholder sig til de særlige databeskyttelsesretlige risici, der opstår i forbindelse med behandling af lokaliseringsdata, samt foretaget en gennemgang af reglerne om bl.a. samtykke, information, de registreredes rettigheder, opbevaringsperioder m.v.

I udtalelsen anfører gruppen på s. 7 bl.a., at en intelligent mobil enhed er meget tæt knyttet til en specifik person og indeholder en række meget personlige oplysninger. Dette gør det muligt for udbydere af geolokaliseringsbaserede tjenester at få et detaljeret overblik over vaner og mønstre hos ejeren af en sådan enhed og at opbygge omfattende profiler. Ud fra et inaktivitetsmønster om natten kan en persons sovested udledes, og ud fra et regelmæssigt transportmønster om morgenen kan en arbejdsgivers placering udledes. Mønstret kan også omfatte data udledt fra venners bevægelsesmønstre. Et adfærdsmønster kan også omfatte særlige kategorier af data, hvis de f.eks. viser besøg på hospitaler og religiøse steder, tilstedeværelse ved politiske demonstrationer eller på andre specifikke steder, som afslører data om f.eks. sexliv.

I udtalelsens s. 10 f anfører Artikel 29-Gruppen endvidere bl.a., at intelligente mobile enheder er uløseligt knyttet til fysiske personer, og at der som regel er direkte og indirekte identificerbarhed. Ifølge udtalelsen kan den direkte identificerbarhed bl.a. ske derved, at den telekommunikationsoperatør, som leverer GSM- og mobil internetadgang, som regel har et register med hver kundes navn, adresse og bankoplysninger i kombination med flere unikke numre for enheden som f.eks. IMEI og IMSI. Indirekte identificerbarhed kan ifølge udtalelsen opnås via kombinationen af enhedens unikke nummer og en eller flere beregnede positioner. I udtalelsen henvises herved til, at alle intelligente mobile enheder har mindst én unik identifikator, nemlig MACadressen. En enhed kan have andre unikke identifikationsnumre, som tilføjes af udvikleren af styresystemet. Disse identifikatorer kan overføres og behandles yderligere i forbindelse med geolokaliseringstjenester. Det anføres, at det er et faktum, at positionen af en bestemt enhed kan beregnes meget nøjagtigt, især når de forskellige infrastrukturer for geolokalisering kombineres. En sådan position kan pege på et hus eller en arbejdsgiver. Ved gentagne observationer er det især muligt at identificere ejeren af enheden. Tilsvarende anføres det i udtalelsen, at den indirekte identificerbarhed også gælder for WiFi-adgangspunkter. MACadressen for et WiFi-adgangspunkt er i kombination med sin beregnede position uløseligt knyttet til positionen for ejeren af adgangspunktet. Det faktum, at det i visse tilfælde ikke aktuelt er muligt at identificere ejeren af enheden uden en urimelig indsats, står ifølge udtalelsen ikke til hinder for den generelle konklusion, at kombinationen af en MAC-adresse for et WiFi-adgangspunkt og dens beregnede position skal behandles som personoplysninger.

Ved pseudonymisering forstås 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, jf. databeskyttelsesforordningens artikel 4, nr. 5. Forskellen mellem anonymiserede data og pseudonymiserede personoplysninger er med andre ord, at alene sidstnævnte ikke (længere) udgør personoplysninger omfattet af databeskyttelsesreglerne, forudsat at anonymiseringen er sket på en effek-

tiv og uigenkaldelig måde. For så vidt angår effektiv anonymisering kan der hentes vejledning i Artikel 29-Gruppens udtalelse nr. 05/2014 om anonymiseringsteknikker af 10. april 2014 (WP 216).

Det anføres af Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udg., 2020, DJØF, s. 253, at behandlingsbegrebet dog i nogle situationer bør fortolkes og anvendes med nogen smidighed for, at forordningen i praksis kan blive velfungerende. Der henvises til Peter Blume, Personoplysningsloven, side 44, hvor der argumenteres for, at den tilsvarende definition af behandlingsbegrebet i den tidligere persondatalov ikke burde omfatte det forhold, at der sker anonymisering. Anonymisering sker netop med det formål for øje, at der ikke længere skal være tale om en behandling af personoplysninger, som er omfattet af forordningens anvendelsesområde, jf. artikel 2, stk. 1, sammenholdt med artikel 4, nr. 1, og betragtning 26.

Følsomme personoplysninger er de oplysningstyper, der udtømmende er opregnet i forordningens artikel 9, stk. 1, og omfatter således bl.a. behandling af genetiske data og biometriske data med det formål entydigt at identificere en fysisk person samt helbredsoplysninger. Øvrige personoplysninger, der ikke er opregnet i artikel 9, udgør almindelige, ikke-følsomme personoplysninger omfattet af artikel 6. Helbredsoplysninger er personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand, jf. forordningens artikel 4, nr. 15, og præambelbetragtning nr. 35.

3.2.2 Grundlæggende principper og behandlingshjemmel

Den udbyder af en applikation, som er i stand til at behandle personoplysninger, herunder geolokaliseringsdata, er dataansvarlig i forbindelse med den behandling af personoplysninger, som følger af installationen og brugen af applikationen, smh. s. 12 i Artikel 29-Gruppens udtalelse nr. 13/2011 af 16. maj 2011 (WP 185) om geolokaliseringstjenester i intelligente mobile enheder.

Reglerne om dataansvarliges hjemmel til lovlig behandling af personoplysninger findes bl.a. i databeskyttelsesforordningens artikel 6 og artikel 9 om behandling af henholdsvis almindelige, ikke-følsomme personoplysninger og følsomme personoplysninger. Behandlingen af følsomme personoplysninger kræver, at der kan identificeres en behandlingshjemmel i databeskyttelsesforordningens artikel 9, stk. 2, eller bestemmelser, der gennemfører forordningens artikel 9. Behandlingen af følsomme personoplysninger skal efter en nylig ændring af Datatilsynets praksis tillige have et lovligt grundlag for denne behandling i forordningens artikel 6, jf. herved Datatilsynets nyhed af 7. november 2019.

Det er samtidig en forudsætning for lovlig behandling af personoplysninger, at principperne i forordningens artikel 5 overholdes. Det gælder herunder princippet om dataminimering, hvorefter personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra c, samt princippet om opbevaringsbegrænsning (sletning) i artikel 5, stk. 1, litra e. Disse principper kan ikke fraviges ved den registreredes samtykke.

Det er væsentligt at være opmærksom på, at regler om behandling af personoplysninger i anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, går forud for reg-

lerne i databeskyttelsesloven, jf. lovens § 1, stk. 3. Det gælder f.eks. regler i sundhedslovgivningen, der måtte give de registrerede en bedre beskyttelse end efter databeskyttelsesloven. Tilsvarende gælder efter omstændighederne reglerne i e-databeskyttelsesdirektivet (dvs. den danske telelovgivning), jf. databeskyttelsesforordningens artikel 95 og nærmere ndf. afsnit 3.3.3.

3.2.2.1 Samtykke

Det følger af forordningens artikel 6, stk. 1, litra a, at behandling af almindelige, ikke-følsomme personoplysninger er lovlig, hvis den registrerede har givet samtykke til behandlingen. Tilsvarende kan behandling af følsomme personoplysninger baseres på et udtrykkeligt samtykke til et eller flere formål efter databeskyttelsesforordningens artikel 9, stk. 2, litra a. Det gælder dog ikke, hvis det i EU-retten eller medlemsstaternes nationale ret er fastsat, at det i stk. 1 omhandlede forbud med behandling af følsomme personoplysninger ikke kan hæves ved den registreredes samtykke.

Et samtykke fra den registrerede udgør enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling, jf. databeskyttelsesforordningens artikel 4, nr. 11.

Der er fastsat betingelser for samtykke i forordningens artikel 7. Det fremgår af stk. 1, at hvis behandling er baseret på samtykke, skal den dataansvarlige kunne påvise, at den registrerede har givet samtykke til behandling af sine personoplysninger.

Det fremgår af artikel 7, stk. 2, at hvis den registreredes samtykke gives i en skriftlig erklæring, der også vedrører andre forhold, skal en anmodning om samtykke forelægges på en måde, som klart kan skelnes fra de andre forhold, i en letforståelig og lettilgængelig form og i et klart og enkelt sprog.

Efter artikel 7, stk. 3, har den registrerede til enhver tid ret til at trække sit samtykke tilbage. Tilbagetrækning af samtykke berører ikke lovligheden af den behandling, der er baseret på samtykke inden tilbagetrækningen. Inden der gives samtykke, skal den registrerede oplyses om, at samtykket kan trækkes tilbage. Det skal være lige så let at trække sit samtykke tilbage som at give det.

Endelig fremgår det af artikel 7, stk. 4, at der ved vurdering af, om samtykke er givet frit, skal tages størst muligt hensyn til, bl.a. om opfyldelse af en kontrakt, herunder om en tjenesteydelse, er gjort betinget af samtykke til behandling af personoplysninger, som ikke er nødvendig for opfyldelse af denne kontrakt.

Det fremgår af præambelbetragtning 43 til databeskyttelsesforordningen, at, med henblik på at sikre, at der frivilligt er givet samtykke, bør samtykke ikke udgøre et gyldigt retsgrundlag for behandling af personoplysninger i et specifikt tilfælde, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige, navnlig hvis den dataansvarlige er en offentlig myndighed, og det derfor er usandsynligt, at samtykket er givet frivilligt under hensyntagen til alle de omstændigheder, der kendetegner den specifikke situation.

Om offentlige myndigheders anvendelse af samtykke som hjemmelsgrundlag – herunder kravet om et frivilligt samtykke – kan henvises til Justitsministeriets betænkning 1565/2017, bd. 1, s. 182 f. Her anføres det bl.a., at når offentlige myndigheder behandler personoplysninger med hjemmel i forordningens artikel 6, stk. 1, litra a, og artikel 9, stk. 2, litra a, bør samtykket efter præambelbetragtning nr. 43, sammenholdt med artikel 7, stk. 4, ikke udgøre et gyldigt retsgrundlag for behandlingen, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige. En sådan skævhed må eksempelvis antages at kunne foreligge i de tilfælde, hvor den registrerede ønsker at ansøge om en ydelse fra en offentlig myndighed, idet der netop i sådanne tilfælde må antages at være en klar skævhed. Præambelbetragtning nr. 43 vedrører således særligt den situation, hvor en borger har en ret til eksempelvis en ydelse. Det anføres videre, at reglerne dog ikke kan antages at være til hinder for, at myndigheden anvender samtykke, hvis myndigheden har brug for personoplysningerne for at kunne behandle den pågældende registreredes sag, dvs. hvor myndigheden som følge af indretningen af lovgivningen ikke kan indhente de relevante oplysninger på anden måde.

Datatilsynets vejledning om samtykke, september 2019, s. 6, er på linje hermed. Det anføres bl.a., at i situationer, hvor den registrerede ansøger om en ydelse, vil den registrerede oftest ikke have andre alternativer end at give samtykke til behandlingen, hvis borgeren vil have ydelsen. En offentlig myndighed vil derfor ofte ikke kunne behandle personoplysninger på baggrund af et samtykke, og offentlige myndigheder bør af denne grund nøje overveje anvendelsen af samtykke som behandlingsgrundlag. Det anføres videre, at i visse situationer, hvor den registreredes afvisning af at give samtykke er uden betydning for myndighedens sagsbehandling af en ydelse eller tilladelse til den registrerede, vil behandling imidlertid kunne ske på grundlag af samtykke. Det kan eksempelvis gælde, hvis en borger ønsker at acceptere kommunens tilbud om at modtage oplysninger på e-mail eller SMS om afhentning af storskrald eller oplysning om forsinkede anlægsarbejder i lokalområdet.

Om samtykke som behandlingsgrundlag kan endvidere henvises til Artikel 29-Gruppens (nu Det Europæiske Databeskyttelsesråd) "Retningslinjer vedrørende samtykke i henhold til forordning 2016/679" (WP 259 rev. 01), s. 6 f, hvor det bl.a. anføres, at elementet "frit" indebærer, at de registrerede har et reelt valg og kontrol. Generelt fastslås det i databeskyttelsesforordningen, at et samtykke er ugyldigt, hvis ikke den registrerede er i stand til at foretage et reelt valg, hvis han/hun føler sig tvunget til at give sit samtykke, eller hvis det vil få negative konsekvenser, hvis han/hun ikke samtykker. Der kan endvidere henvises til udtalelse 15/2011 om definitionen af samtykke (WP 187), s. 18.

Om samtykke i relation til behandling af personoplysninger i apps kan henvises til Artikel 29-Gruppens udtalelse nr. 02/2013 af 27. februar 2013 vedrørende databeskyttelse i apps i intelligente enheder (WP 202), s. 13 f, der indeholder detaljerede retningslinjer om samtykkets form, indhold, granularitet, tidspunkt for indhentelse m.v.

3.2.2.2 Alternative hjemmelsgrundlag til samtykke

Som et alternativ til samtykke vil den offentlige myndighed i tvivlstilfælde kunne overveje andre behandlingshjemler – såsom artikel 6, stk. 1, litra e – om behandling, der er nødvendig af hensyn til udførelse af en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, eller artikel 9, stk. 2, litra g, smh. databeskyttelseslovens § 7, stk. 4, 1. pkt., om væsentlige samfundsinteresser, jf. herved også Justitsministeriets betænkning 1565/2017, s. 183. Kernen for bestemmelsen er offentlig myndighedsudøvelse i form af udstedelse af

forvaltningsakter, men bestemmelsen omfatter efter omstændighederne også udførelse af opgaver, som sædvanligvis karakteriseres som faktisk forvaltningsvirksomhed, jf. betænkning 1565/2017, s. 121. Brugen af artikel 6, stk. 1, litra e, som behandlingsgrundlag forudsætter således ikke en national, implementerende hjemmelslovgivning om selve behandlingen af personoplysninger i forbindelse med udførelse af opgaver i samfundets interesse eller som led i offentlig myndighedsudøvelse. Det anføres videre, at brugen af artikel 6, stk. 1, litra e, heller ikke nødvendigvis kræver, at opgaven, som kræver behandling af personoplysninger, udtrykkeligt i lovgivningen er pålagt myndigheden.

Endvidere kan der for så vidt angår behandling af følsomme personoplysninger, herunder navnlig helbredsoplysninger, henvises til databeskyttelsesforordningens artikel 9, stk. 2, litra g, om væsentlige samfundsinteresser, smh. databeskyttelseslovens § 7, stk. 4, 1. pkt., om væsentlige samfundsinteresser, jf. herved også Justitsministeriets betænkning 1565/2017, s. 183.

Derudover kan der henvises til databeskyttelseslovens § 7, stk. 3, hvorefter behandling af oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, kan ske, hvis behandling af oplysninger er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra h. Bestemmelsen giver også hjemmel til at foretage behandling i medfør af databeskyttelsesforordningens artikel 9, stk. 2, litra i, om behandling af hensyn til samfundsinteresser på folkesundhedsområdet, f.eks. beskyttelse mod alvorlige grænseoverskridende sundhedsrisici m.v.

3.2.3 Krav om særlig regulering?

Det tidligere Registertilsyn og Datatilsynet i en række sager har udtalt, at der ud fra overordnede og retspolitiske betragtninger bør tilvejebringes en direkte lovhjemmel i forbindelse med iværksættelsen af registreringsaktiviteter, selvom behandlingen i sig selv har tilstrækkelig hjemmel i den dagældende persondatalov.

Efter lovgivningspraksis etableres der ofte særskilt og klar lovhjemmel i særlovgivningen til oprettelse og udvikling af digitale løsninger, der involverer omfattende behandlinger af personoplysninger, smh. Hanne Marie Motzfeldt og Azad Taheri Abkenar, Digital forvaltning – udvikling af sagsbehandlende løsninger, 1. udg., 2019, DJØF, s. 135 f. Sådanne lovbestemmelser vil ofte regulere behandlingen af personoplysninger, herunder hjemmel, formålsbestemthed m.v. Det gælder f.eks. etableringen af ejendomsvurderingssystemet, jf. lov nr. 654 af 8. juni 2017 (med senere ændringer), etableringen af Erhvervsstyrelsens snydbekæmpelsessystem, jf. lov nr. 438 af 8. maj 2018 om Erhvervsstyrelsens behandling af data, etableringen af Rigspolitiets efterretningssystem (POL-INTEL), jf. lov nr. 671 af 8. juni 2017 om ændring af lov om politiets virksomhed og toldloven, samt etableringen af Arbejdstilsynets system for risikobaseret tilsyn med arbejdsmiljølovgivningen, jf. lov nr. 1554 af 27. december 2019 om ændring af lov om arbejdsmiljø og lov om arbejdsskadesikring.

Det må anses for uafklaret, om denne lovgivningspraksis er udtryk for et behov for at sætte klare rammer for bl.a. dataanvendelse eller dækker over et ønske om lovgivningsmagtens accept af igangsættelse af i hvert fald mere omfattende og potentielt kontroversielle projekter, der kan få ikke ubetydelige økonomiske konsekvenser samt påvirke arbejdsgange, or-

ganisatoriske forhold m.v. i større omfang, jf. Hanne Marie Motzfeldt og Azad Taheri Abkenar, ovf. anf. st., s. 135 f. Lovgivningspraksissen har dog ikke vedrører tilfælde som i nærværende sag, hvor behandlingsgrundlaget udgøres af et samtykke, men har derimod handlet om behandling af personoplysninger på baggrund af myndighedsudøvelse m.v.

Det så vidt ses seneste eksempel fra administrativ praksis udgøres af Datatilsynets udtalelse til Rigspolitiet i den såkaldte ANPG-sag vedrørende politiets påtænkte anvendelse af automatisk nummerpladegenkendelse (ANPG), jf. Datatilsynets j.nr. 2014-082-0114.

Fastsættelse af dansk særregulering skal ske inden for rammerne af databeskyttelsesforordningen, jf. om det nationale råderum herfor s. 141 ff og s. 223-233 i betænkning 1565.

I databeskyttelsesloven er der mulighed for, at vedkommende minister efter forhandling med justitsministeren og inden for databeskyttelsesforordningens rammer kan fastsætte nærmere regler om behandling af personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, jf. lovens § 7, stk. 5. Ifølge de specielle bemærkninger til bestemmelsen i lovforslaget er bestemmelsen begrundet i, at det kan være vanskeligt på forhånd fuldstændigt at forudse behovet for at kunne behandle personoplysninger omfattet af forordningens artikel 9, stk. 1.

3.3 E-databeskyttelsesreglerne

E-databeskyttelsesdirektivet[4] indeholder regler for alle, der ønsker at lagre eller få adgang til oplysninger, der er lagret på enheder tilhørende brugere i Det Europæiske Økonomiske Samarbejdsområde (EØS).

Det følger af direktivets artikel 5, stk. 3, at medlemsstaterne sikrer, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har givet sit samtykke hertil efter i overensstemmelse med direktiv 95/46/EF at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen. Dette er ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at sætte udbyderen af en informationssamfundstjeneste, som abonnenten eller brugeren udtrykkelig har anmodet om, i stand til at levere denne tjeneste.

Samtykkekravet i artikel 5, stk. 3, finder anvendelse på alle oplysninger uden hensyn til arten af de oplysninger, der lagres eller skaffes adgang til. Det er ikke begrænset til personoplysninger, men kan være en hvilken som helst type oplysninger, der er lagret på enheden. Et samtykke givet af bruger eller abonnent svarer til den registreredes samtykke i data-

[4] Europa-Parlamentets og Rådets direktiv af 2002-07-12 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (2002/58) som ændret ved EP/Rdir 2006/24 og EP/Rdir 2009/136. Kommissionen har den 10. januar 2017 fremsat forslag til revision af e-databeskyttelsesdirektivet (2002/58/EF) om behandling af persondata og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor) (KOM (2017). Formålet med forslaget er at opdatere reglerne i forhold til den teknologiske og markedsmæssige udvikling samt tilpasse regelsættet til de generelle regler i databeskyttelsesforordningen. Det vides endnu ikke, hvornår denne retsakt forventes vedtaget, og forslaget behandles ikke yderligere her.

beskyttelsesdirektivet (direktiv 95/46/EF), jf. e-databeskyttelsesdirektivets artikel 2, litra f. Definitionen af samtykke i e-databeskyttelsesdirektivet svarer således til definitionen af samtykke i databeskyttelsesforordningen, jf. forordningens artikel 94, stk. 2, 1. pkt., hvorefter henvisninger til det ophævede databeskyttelsesdirektiv (direktiv 95/46/EF) gælder som henvisninger til databeskyttelsesforordningen. I EU-Domstolens dom af 1. oktober 2019 i sag C-673/17, *Planet 49*, slog EU-Domstolen fast, at samtykket efter e-databeskyttelsesdirektivets artikel 5, stk. 3, svarer til samtykket i databeskyttelsesforordningens artikel 4, nr. 11, jf. præmis 62-65. Dette gælder i øvrigt uanset, om de lagrede eller konsulterede oplysninger i brugeren af et internetwebsteds terminaludstyr udgør personoplysninger som omhandlet i direktiv 95/46 og forordning 2016/679 eller ej, jf. præmis 71.

E-databeskyttelsesdirektivets artikel 5, stk. 3, er implementeret i dansk ret i § 3 i den såkaldte cookiebekendtgørelse[5]. Det følger af stk. 1, at fysiske eller juridiske personer ikke må lagre oplysninger eller opnå adgang til oplysninger, der allerede er lagret, i en slutbrugers terminaludstyr eller lade tredjepart lagre oplysninger eller opnå adgang til oplysninger, hvis slutbrugeren ikke giver samtykke hertil efter at have modtaget fyldestgørende information om lagringen af eller adgangen til oplysningerne. Der er i stk. 2 fastsat en række minimumskrav til indholdet af den information, som brugerne skal have efter stk. 1.

Som terminaludstyr forstås et produkt eller en relevant komponent heri, der muliggør kommunikation, og som er beregnet til at blive direkte eller indirekte tilsluttet nettermineringspunkter i offentlige elektroniske kommunikationsnet, jf. cookiebekendtgørelsens § 2, nr. 1.

Pligten til samtykke efter e-databeskyttelsesdirektivets artikel 5, stk. 3, og dermed cookiebekendtgørelsens § 3, omfatter også lagring af eller adgang til oplysninger, herunder personoplysninger, der sker i apps i mobile enheder, jf. Artikel 29-Gruppen udtalelse nr. 02/2013 af 27. februar 2013 om databeskyttelse i apps i intelligente enheder (WP 202), s. 13 ff.

Forholdet mellem e-databeskyttelsesdirektivet og databeskyttelsesforordningen er reguleret i databeskyttelsesforordningens artikel 95. Det fremgår af bestemmelsen, at forordningen ikke indfører yderligere forpligtelser for fysiske eller juridiske personer for så vidt angår behandling i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet i Unionen for så vidt angår spørgsmål, hvor de er underlagt specifikke forpligtelser med samme formål som det, der er fastsat i direktiv 2002/58/EF. I det omfang der er overlap mellem de to regelsæt, går e-databeskyttelsesdirektivet forud, således at det pågældende spørgsmål skal afgøres ud fra direktivets regler, og ikke databeskyttelsesforordningens regler, jf. Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udg., 2020, DJØF, s. 954. E-databeskyttelsesdirektivet må således anses for lex specialis, jf. herved også Christopher Kuner m.fl. (ed.), The EU Generel Data Protection Regulation (GDPR) – A Commentary, 1. udg., 2020, Oxford University Press, s. 1297.

[5] Bekendtgørelse nr. 1148 af 9. december 2011 om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugeres terminaludstyr

Det Europæiske Databeskyttelsesråd har i en udtalelse af 12. marts 2019[6] forholdt sig til samspillet mellem de to regelsæt. På s. 14, punkt 40, i udtalelsen anføres det bl.a., at i det omfang, at informationen, der opbevares i slutbrugerens terminaludstyr, udgør personoplysninger, har e-databeskyttelsesdirektivets artikel 5, stk. 3, forrang for databeskyttelsesforordningens artikel 6 for så vidt angår den behandling, der består i lagring af eller adgang til denne information. Det anføres, at når kravet om samtykke i e-databeskyttelsesdirektivets artikel 5, stk. 3, finder anvendelse, kan den dataansvarlige ikke anvende de øvrige mulige hjemmelsgrundlag i databeskyttelsesforordningens artikel 6. Noget tilsvarende må ud fra samme betragtning antages at gælde for så vidt angår databeskyttelsesforordningens artikel 9.

Om samspillet mellem det databeskyttelsesretlige samtykke og det e-databeskyttelsesretlige samtykke i relation til behandling af personoplysninger i apps, anfører Artikel 29-Gruppen bl.a. følgende på s. 13ff i udtalelse nr. 02/2013 af 27. februar 2013 om databeskyttelse i apps i intelligente enheder (WP 202):

> *"**3.4.1 Samtykke før installation og behandling af personoplysninger***
>
> *I forbindelse med apps er det vigtigste retlige grundlag samtykke. Når en app installeres, placeres der oplysninger på slutbrugerens enhed. Mange apps har også adgang til oplysninger, der er lagret på enheden, kontakter i adressebogen, billeder, videoer og andre personlige dokumenter. I alle disse tilfælde kræver e-data-direktivets artikel 5, stk. 3, samtykke fra brugeren, som har modtaget klare og fyldestgørende oplysninger, før der placeres oplysninger på enheden eller hentes oplysninger på den.*
>
> *Det er vigtigt at bemærke sondringen mellem det samtykke, der kræves for at placere oplysninger på og aflæse oplysninger fra enheden, og det samtykke, der er nødvendigt for at have et retligt grundlag for behandling af forskellige typer personoplysninger. Begge samtykkekrav finder anvendelse sideløbende, baseret på hver deres retsgrundlag, men de er begge underlagt betingelser om, at de skal være frivillige, specifikke og informerede (som defineret i databeskyttelsesdirektivets artikel 2, litra h) [nu databeskyttelsesforordningens artikel 4, nr. 11]). Derfor kan de to typer samtykke i princippet kombineres, enten under installationen eller før appen begynder at indsamle personoplysninger fra enheden, forudsat at brugeren bliver utvetydigt oplyst om, hvad han giver samtykke til.*
>
> *[…]*
>
> ***3.4.2 Retlige grundlag for databehandling under brug af appen***
> *Som forklaret ovenfor udgør samtykke det nødvendige retlige grundlag for at give app-udvikleren tilladelse til at læse og/eller skrive oplysninger og dermed behandle personoplysninger lovligt. Efterfølgende under brug af appen kan app-udvikleren anvende andre retlige grundlag til andre typer databehandling, så længe det ikke omfatter behandling af følsomme personoplysninger. […]"*

[6] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities

Der er i e-databeskyttelsesdirektivets artikel 15 givet mulighed for, at medlemsstaterne kan fravige samtykkekravene i bl.a. artikel 5, stk. 3, om samtykke til lagring eller adgang til oplysninger på brugernes terminaludstyr.

Det Europæiske Databeskyttelsesråd har i en udtalelse af 19. marts 2020[7] forholdt sig til spørgsmålet om databeskyttelse i lyset af COVID-19 pandemien, herunder særligt brug af lokaliseringsdata omfattet af e-databeskyttelsesdirektivet. Her anføres det overordnet, at lokaliseringsoplysninger omfattet af e-databeskyttelsesdirektivet alene kan anvendes i anonym form eller som følge af samtykke, ligesom rammerne for brug af muligheden for at fravige e-databeskyttelsesdirektivet i national lovgivning via direktivets artikel 15 behandles. Det Europæiske Databeskyttelsesråd har endvidere i en pressemeddelelse af 7. april 2020[8] anført, at rådet har påbegyndt et arbejde med at udarbejde vejledninger om adskillige aspekter af behandling af data i bekæmpelsen af COVID-19. Det drejer sig om en vejledning om geolokalisering og andre sporingsværktøjer til bekæmpelse af COVID-19 samt en vejledning om behandling af helbredsoplysninger til forskningsformål i samme øjemed. Førstnævnte vejledning vedrørende geolokalisering vil bl.a. omhandle emner såsom brug af aggregerede/anonymiserede lokaliseringsdata (f.eks. leveret af teleudbydere eller udbydere af informationssamfundstjenester), anvendelsen af de grundlæggende principper i databeskyttelsesforordningens artikel 5 om bl.a. dataminimering m.v., en generel juridisk analyse af brugen af apps og indsamling og behandling af personoplysninger via apps til brug for inddæmning af smittespredning, samt sikkerhed og opbevaringsperiode m.v. Det er uvist, hvornår disse vejledninger vil blive offentliggjort af rådet.

4. VURDERING

4.1 Forudsætninger for min vurdering

Jeg lægger efter det oplyste til grund for min vurdering, at Styrelsen for Patientsikkerhed som udbyder af appen – i det omfang der behandles personoplysninger i appen – er dataansvarlig for denne databehandling.

Spørgsmålet er, om Styrelsen for Patientsikkerhed har hjemmel til som dataansvarlig at etablere og behandle personoplysninger i appen med det formål at understøtte COVID-19-bekæmpelse og information til borgerne om smitterisiko. Jeg foretager vurderingen ud fra de gældende regler i epidemiloven, databeskyttelsesforordningen og -loven samt e-databeskyttelsesreglerne. Det er aftalt, at Sundheds- og Ældreministeriet i samarbejde med Styrelsen for Patientsikkerhed selv vurderer eventuelle begrænsninger i muligheden for anvendelse af data efter den øvrige sundhedslovgivning, herunder sundhedsloven.

Det er en del af vurderingen, om det er retligt nødvendigt eller hensigtsmæssigt at vedtage ny lovgivning for at sikre det fornødne og hensigtsmæssige hjemmelsgrundlag for løsningen.

[7] Statement on the processing of personal data in the context of the COVID-19 outbreak, tilgængelig her: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[8] Pressemeddelelsen er tilgængelig her: https://edpb.europa.eu/news/news_da

Ved min vurdering lægger jeg følgende til grund som forudsætninger for min vurdering, jf. nærmere ovenfor afsnit 2: (1) *At* appen baserer sig på frivillighed, (2) *at* der udelukkende sker behandling af pseudonymiserede og aggregerede data, (3) *at* myndighederne ikke vil bruge data på individniveau til at pålægge enkelte borgere restriktioner (ingen restriktioner for borgerne), (4) at appen ikke udgør en klinisk app og altså ikke tjener et klinisk formål og ikke skal indeholde selvrapportering af symptomer til brug for selvvurdering af egen sygdom eller lignende, samt (5) at appen kun anvendes i forbindelse med COVID-19.

4.2 To grundlæggende modeller

Grundlæggende kan der for så vidt angår hjemmelsgrundlaget for behandlingen af personoplysninger i app-løsningen opereres med to forskellige modeller: (1) Løsningen baseres på et samtykke efter databeskyttelsesforordningens regler og uden brug af ny regulering, eller (2) løsningen baseres delvist på øvrige grundlag end samtykke, dvs. de øvrige bestemmelser i databeskyttelsesforordningen og -loven, epidemiloven og bestemmelser fastsat i medfør heraf samt eventuelt tillige øvrig særlig regulering, dvs. regler baseret på myndighedsudøvelse og bredere samfundsmæssige interesser.

Der er i notatet taget udgangspunkt i en virkeliggørelse af appen ved brug af samtykke (model 1), da dette er i overensstemmelse med forudsætningen om frivillighed. Man skal i den forbindelse bl.a. være opmærksom på, at modellen indebærer, *at* Styrelsen for Patientsikkerhed skal kunne dokumentere samtykkerne, deres indhold og tidspunktet for dem, og *at* borgerne løbende skal give samtykke i takt med fase 1-3, *at* borgerne har ret til at trække deres samtykke tilbage, hvorefter behandlingen af oplysninger i personhenførbar form skal stoppe. Det sidstnævnte vil indebære, at oplysningerne om kontaktregistreringerne, helbredsforhold, geolokation m.v. skal slettes i appen samt i den bagvedliggende database, idet der dog kan være pligt til at opretholde opbevaringen af data i henhold til arkivlovgivningen, i hvilket tilfælde der vil skulle ske begrænsning af brugen af dataene. Modellen indebærer tillige, *at* samtykket vil skulle opdateres, hvis der i øvrigt sker væsentlige ændringer i behandlingen undervejs, samt *at* der vil være ret til dataportabilitet af dataene, hvilket skal bygges ind i løsningen.

Det er en forudsætning for brug af model 1, at samtykket opfylder betingelserne i definitionen i artikel 4, nr. 11, og artikel 7, herunder at samtykket skal være frivilligt. Jeg har i den forbindelse overvejet, om Styrelsen for Patientsikkerhed kan indhente et frivilligt samtykke, henset til at der er tale om en relation mellem en borger og en offentlig myndighed, og hvor samtykke ikke bør udgøre et gyldigt retsgrundlag for behandlingen, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige, idet offentlige myndigheders brug af samtykke dog ikke er udelukket.

Efter min opfattelse vil samtykket i nærværende tilfælde reelt være frivilligt, og dermed leve op til betingelsen herom. Jeg har lagt vægt på, *at* der er en realitet bag frivilligheden, idet borgerne har et reelt valg, om de vil downloade og bruge appen eller ej, ligesom de har kontrol over, hvilke oplysninger de vil modtage og dele under brug af appen, idet det vil ikke være forbundet med negative konsekvenser for borgeren, hvis borgeren ikke samtykker. Der må også lægges vægt på, at der ikke er tale om levering af en offentlig ydelse efter ansøgning, men at appens funktion snarere har karakter af faktisk forvaltningsvirksomhed, hvor borgeren har mulighed for at tilvælge eller fravælge en service. Jeg lægger til grund, at download og brug af appen ikke er en forudsætning for at modtage information om, hvorvidt man er smittet med COVID-19 eller ej. Det vil endvidere styrke vurderingen af appen som en frivillig service, såfremt borgerne får mulighe-

den for at opnå yderligere information, som gives i appen, ad anden vej, f.eks. derved at der på styrelsens hjemmeside offentliggøres anonymiserede/aggregerede "coronakort" over, i hvilke dele af landet der er særlig risiko for smitte.

Selvom model 1 om brug af samtykke anvendes, kan en nærmere regulering overvejes, jf. nærmere ndf. afsnit 4.6, inden påbegyndelsen af fase 3 og den deri indeholdte omfattende behandling af geolokationsdata, om end det efter min vurdering ikke vil være et retligt krav.

Hvis behandlingen af personoplysninger i sporingsappen ikke fuldt ud skal baseres på samtykke, kan model 2 overvejes, dvs. hvor behandlingen delvist baserer sig på eksisterende eller ny regulering. Det kan her bl.a. overvejes, om epidemiloven og bekendtgørelser udstedt i medfør deraf kan udgøre et grundlag for visse behandlinger.

Hvad angår de to gældende bekendtgørelser, bemærkes det, at de ikke efter deres nuværende ordlyd fuldt ud dækker de behandlinger, herunder videregivelser, af personoplysninger, som vil være omfattet af ordningen, f.eks. vil videregivelse af oplysninger fra MiBA om smittede – fra Statens Serum Institut til Styrelsen for Patientsikkerhed – ikke være dækket af bekendtgørelsens § 4, da den henviser til tilfælde, hvor Styrelsen for Patientsikkerhed skal vurdere, om der er grundlag for påbud efter epidemilovens § 5.

For så vidt angår muligheden for administrativt at fastsætte bestemmelser med hjemmel i epidemilovens §§ 21 a og 21 b, bemærkes det, at bestemmelserne er meget bredt formuleret. § 21 a giver mulighed for at fastsætte regler om fysiske og juridiske personers samt myndigheders oplysningsforpligtelser for at hindre udbredelse og smitte af en sygdom omfattet af lovens § 2, og § 21 giver mulighed for at fastsætte regler om, at personoplysninger kan behandles, hvis behandlingen er nødvendig for at hindre udbredelsen og smitte af en bestemt sygdom omfattet af lovens § 2.

Sidstnævnte bestemmelse forudsætter en vurdering af reglernes nødvendighed, hvilket skal ses i lyset af, at reglerne skal kunne rummes inden for de muligheder, som databeskyttelsesforordningen giver for at fastsætte nationale særregler, og at der heraf må antages også at følge et krav om nødvendighed. Epidemilovens §§ 21 a og 21 b giver med andre ord hjemmel til at fastsætte regler om oplysningspligter og behandling af personoplysninger med henblik på bekæmpelse af Coronavirussygdom 2019 (COVID-19), i det omfang Danmarks internationale forpligtelser tillader det.

Hvis ordningen ikke baseres på samtykke – dvs. model 2 vælges – og der er et ønske om at udstede regler med hjemmel i epidemilovens §§ 21 a og 21 b, vil der i givet fald skulle foretages en vurdering af reglernes nødvendighed, og den skal bl.a. foretages i lyset af, at der er tale om en app, som borgeren frivilligt downloader. Hvis der ikke anvendes samtykke til behandlingen af personhenførbare geolokationsdata, kan det give anledning til principielle spørgsmål om dataminimering, opbevaringsbegrænsning og behovet for at sikre et sikkert hjemmelsgrundlag, som man i givet fald må genbesøge inden påbegyndelsen af fase 3.

Under alle omstændigheder er det vigtigt at være opmærksom på, at lagring af eller adgang til oplysninger på borgernes mobile enheder vil kræve et samtykke efter cookiebekendtgørelsens § 3, jf. e-databeskyttelsesdirektivets artikel 5, stk. 3. En fravigelse heraf vil kræve særlig national regulering, jf. e-databeskyttelsesdirektivets artikel 15.

4.3 Fase 1 – Kontaktregistrering

4.3.1 Samtykke efter cookiebekendtgørelsen

Når borgerne downloader og installerer appen, sker der en lagring af oplysninger på borgernes mobile enhed, typisk en smartphone. Denne lagring af data samt Styrelsen for Patientsikkerheds efterfølgende adgang til oplysninger i appen, herunder kontaktdata gennem bluetooth-/beaconteknologi, kræver, at styrelsen indhenter et forudgående samtykke fra borgerne, efter borgerne har modtaget fyldestgørende information om lagringen af eller adgangen til oplysningerne, jf. cookiebekendtgørelsens § 3, stk. 1, der bygger på e-databeskyttelsesdirektivets artikel 5, stk. 3, samt s. 13f i Artikel 29-Gruppens udtalelse nr. 02/2013 af 27. februar 2013 om databeskyttelse i apps i intelligente enheder (WP 202). Dette samtykke skal indhentes, *uanset* om der vil ske behandlingen af personoplysninger eller ej.

Samtykket skal overholde betingelserne for et gyldigt samtykke i databeskyttelsesforordningens artikel 4, nr. 11, og skal leve op til en række minimumskrav til fyldestgørende information i cookiebekendtgørelsens § 3, stk. 2. Herefter skal informationen som minimum (1) fremstå i et klart, præcist og letforståeligt sprog eller tilsvarende billedskrift, (2) indeholde oplysning om formål med lagringen af eller adgangen til oplysninger i borgerens terminaludstyr, (3) indeholde oplysninger, der identificerer enhver fysisk eller juridisk person, der foranstalter lagringen af eller adgangen til oplysningerne, (4) indeholde en umiddelbart tilgængelig adgang for slutbrugeren til at afslå samtykke eller tilbagekalde samtykke til lagringen af eller adgangen til oplysninger samt en klar, præcis og letforståelig vejledning om, hvordan slutbrugeren anvender en sådan adgang, og (5) være umiddelbart tilgængelig for slutbrugeren ved samlet og tydeligt at blive meddelt denne. Desuden skal information, når der sker lagring af eller adgang til oplysninger i slutbrugerens terminaludstyr igennem en informations- og indholdstjeneste, være vedvarende tilgængelig for slutbrugeren ved en direkte og tydeligt markeret adgang på den pågældende informations- og indholdstjeneste.

4.3.2 Sker der behandling af personoplysninger i appen?

Spørgsmålet er herefter, om der i fase 1 vil blive behandlet personoplysninger i appen, eller om oplysningerne vil være ikke-personhenførbare, fordi de er effektivt anonymiserede og således ikke (længere) er omfattet af databeskyttelsesforordningen eller -loven. I fase 1 vil der efter det oplyste indsamles oplysninger om, hvor mange kontakter en borger, der har downloadet app'en, har haft i løbet af en dag med andre personer, der har downloadet appen, dvs. de pågældende mobile enheders fysiske afstand til hinanden, varigheden af kontakten og eventuelt tidsstempel for kontakten. Der indsamles og registreres ikke oplysninger om lokationen og hvem, borgeren har haft kontakt med. Der vil endvidere ikke være oplysninger om, hvorvidt dem, som borgerne har været i kontakt med, er smittet eller har antistoffer.

Der lægges op til to forskellige modeller for henholdsvis med og uden brug af NemID til sikker identifikation af borgerne ved borgernes installation af appen.

Hvis modellen *med brug af NemID* som login anvendes, vil der ske en identifikation af den enkelte borger, idet de oplysninger om kontaktregistreringer, der behandles i appen i første fase, kobles til borgerens identitet gennem CPR-nummer. Der vil således uden videre være tale om behandling af personoplysninger, og databeskyttelsesreglerne finder anvendelse,

herunder kravet om hjemmel for behandlingen m.v., jf. nærmere nedenfor afsnit 4.2. Brugen af NemID er begrundet i et ønske om, at der allerede i fase 1 indsamles valide oplysninger om køn og alder, da dette kan give viden om, hvilke befolkningsgrupper fordelt på køn og alder, der er gode til at holde afstand og hvilke der er mindre gode til det.

Hvis modellen *uden brug af NemID* anvendes, vil der ikke ske en umiddelbar identifikation af borgeren og dermed behandling af personoplysninger. Databeskyttelsesreglerne finder ikke anvendelse, hvis oplysningerne, der behandles i app'en, ikke er personhenførbare, fordi de er effektivt, dvs. uigenkaldeligt, anonymiserede.

Efter det oplyste er appen tænkt designet således, at første gang brugeren downloader appen, og denne kontakter serveren, kreerer og giver serveren hver bruger et ID, som gemmes på telefonen. Dette ID henføres ikke til telefonens MAC-adresse, og serveren gemmer ikke telefonernes MAC-adresser. Telefonens MAC-adresse fungerer som en unik identifikator for telefonen, og da telefonen i almindelighed meget ofte er tæt knyttet til en fysisk person, udgør MAC-adressen og den deraf tilknyttede information personhenførbare oplysninger. ID'er bruges kun til, at telefonerne kan fortælle serveren, hvilket andet anonymt ID, telefonerne har registreret et møde med, når telefonerne kommer tæt på hinanden. Når MAC-adressen er slettet, er der således ikke en kobling mellem appen og den fysiske telefon, ligesom der ikke er en registrering af kobling mellem telefon og borgeren.

Jeg må forstå ovennævnte således, at driftsleverandøren Netcompany som databehandler på vegne af Styrelsen for Patientsikkerhed indsamler telefonens MAC-adresse alene med det formål straks at omdanne den til et unikt ID, hvorefter MAC-adressen slettes. Der indsamles og registreres dog (kortvarigt) en MAC-adresse, der kan føres tilbage til en bestemt telefon (og dermed person), og MAC-adressen må derfor som udgangspunkt anses som værende en personhenførbar oplysning, på samme måde som en IP-adresse er en personhenførbar oplysning, om end behandlingen af MAC-adressen er tidsmæssigt begrænset.

Omvendt antages det i Databeskyttelsesforordningen og databeskyttelsesloven, 1. udgave, Kristian Korfits Nielsen and Anders Lotterup, Djøf Forlaget, 2020, side 253 med henvisning til Peter Blume, at behandlingsbegrebet i nogle situationer bør fortolkes og anvendes med nogen smidighed for, at forordningen i praksis kan blive velfungerende. Det anføres, at den tilsvarende definition af behandlingsbegrebet i den tidligere gældende persondatalov ikke bør omfatte det forhold, at der *sker* anonymisering. Anonymisering sker netop med det formål for øje, at der ikke længere skal være tale om en behandling af personoplysninger, som er omfattet af forordningens anvendelsesområde, jf. artikel 2, stk. 1, sammenholdt med artikel 4, nr. 1 og betragtning 26.

Det giver således anledning til tvivl, om behandlingen, dvs. konverteringen af telefonernes MAC-adresser til anonyme, irreversible ID-numre, falder uden for databeskyttelsesforordningens anvendelsesområde, således at databeskyttelsesreglerne ikke finder anvendelse.

Jeg anbefaler derfor en løsning, hvorefter appen behandles, som om der sker behandling af personhenførbare oplysninger, hvorefter der vil skulle sikres et hjemmelsgrundlag for behandlingen, f.eks. i form af samtykke. Dette vil også indebære, at Styrelsen for Patientsikkerhed gennem en databehandleraftale kan styre og stille krav til leverandørernes behandling af det meget omfattende antal MAC-adresser, hvilket må anses for hensigtsmæssigt.

Oplysningerne vil herefter kunne behandles med hjemmel i samtykke efter cookiebekendtgørelsens § 4, stk. 1, jf. e-databeskyttelsesdirektivets artikel 5, stk. 3, og databeskyttelsesforordningens artikel 6, stk. 1, litra a.

4.4 Fase 2 – Smitteoplysning

I fase 2 vil Styrelsen for Patientsikkerhed – i tillæg til oplysningerne nævnt ovenfor i fase 1 – løbende indsamle oplysninger fra MiBA, som SSI er dataansvarlig for, om app-brugernes helbredsforhold i form af oplysning om, hvorvidt de pågældende app-brugere er smittet med COVID-19.

Dette forudsætter, at borgeren logger ind med NemID for at sikre den fornødne sikre identifikation af borgeren og ud fra et hensyn til at sikre validiteten af dataene om smitte- og immunitetsstatus set i forhold til borgernes egen indberetning heraf (datakvalitet).

Identifikationen via NemID medfører, at Styrelsen for Patientsikkerhed nu med sikkerhed behandler personhenførbare data om dels kontaktregistrering, dels ovennævnte oplysninger om smitte- og immunitetsstatus, da borgerens ID-oplysning i appen kan henføres til borgerens NemID.

Adgangen til dataene om kontaktregistreringer på borgernes mobile enheder vil som nævnt kræve et informeret samtykke efter reglerne i cookiebekendtgørelsens § 3. Tilsvarende gælder, hvis oplysningerne om helbredsforhold fra SSI lagres på borgernes mobile enheder, og der opnås adgang til dem herfra.

Derudover skal der i ovennævnte tilfælde være hjemmel til Styrelsen for Patientsikkerheds indsamling af oplysningerne efter databeskyttelsesforordningen, herunder SSI's videregivelse af oplysninger om smitte- og immunitetsstatus. Oplysningerne omfatter dels almindelige ikke-følsomme personoplysninger omfattet af databeskyttelsesforordningens artikel 6 samt oplysninger om helbredsforhold omfattet af forordningens artikel 9.

Denne behandling vil også kunne foretages med samtykke efter cookiebekendtgørelsens § 3 samt databeskyttelsesforordningens artikel 6, stk. 1, litra a, og artikel 9, stk. 2, litra a.

Databeskyttelsesforordningens artikel 95 medfører, at kravet om samtykke i cookiebekendtgørelsen går forud for databeskyttelsesforordningen, således at Styrelsen for Patientsikkerhed som dataansvarlig skal anvende et samtykke, der lever op til betingelserne i databeskyttelsesforordningens artikel 4, nr. 11, som hjemmelsgrundlag for at kunne lagre og få adgang til oplysningerne på borgernes mobile enheder. Dette lex specialis princip medfører således, at Styrelsen for Patientsikkerhed ikke vil kunne anvende de øvrige mulige hjemmelsgrundlag i databeskyttelsesforordningens artikel 6, jf. herved Det Europæiske Databeskyttelsesråds udtalelse af 12. marts 2019, s. 14, punkt 40. Tilsvarende må ud fra samme betragtning gælde hjemmelsgrundlagene i forordningens artikel 9.

Borgeren kan – hvis borgeren er smittet med COVID-19 – i fase 2 vælge at *give* besked til de af borgerens kontakter, der har downloadet appen og potentielt har været udsat for smitterisiko gennem kontakt med borgeren. Som en refleksvirk-

ning heraf kan den enkelte borger endvidere på sin app vælge at *modtage* besked, hvis en af de kontakter, som borgeren har haft, og som har downloadet appen, er blevet smittet med COVID-19 og dermed kan have udgjort en smitterisiko for borgeren.

Der sker med andre ord en udstillelse af data over for andre brugere af appen, som borgeren har været i kontakt med, om, at borgeren er smittet. Det er endnu ikke afklaret, hvor mange informationer, der vil blive udvekslet mellem borgerne om, hvornår borgeren er blevet udsat for smitterisiko, herunder om borgeren skal have det konkrete kontakttidspunkt at vide. De borgere, som den smittede borger har været i kontakt med, vil ikke direkte få oplysninger om identiteten på den smittede borger. Det kan dog i sagens natur meget vel være tilfældet, at den smittede borger (A), vil kunne blive identificeret af den/de borger(e) (B), som borger A har været i kontakt med, hvis borger B over en begrænset periode alene har været i kontakt med borger A, og borger B får oplysning gennem appen om, at borger B har været i kontakt med en smittet i løbet af en kortere tidsperiode.

Således vil der med andre ord blive videregivet følsomme oplysninger om helbredsforhold i appen. En sådan videregivelse må efter min opfattelse kræve samtykke fra borgerne, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra a, samt artikel 6, stk. 1, litra a. Det må efter min opfattelse anses for sagligt og proportionelt, at der i appen gives en vis tidsmæssig oplysning om kontakten med smittede, da formålet med appen netop er, at personer, der har været i kontakt med en smittet (boger B), vil kunne tage deres forholdsregler og f.eks. opsøge lægehjælp, blive testet eller gå i hjemmekarantæne med henblik på at forhindre yderligere smitte m.v.

Dette betyder, at appen skal designes således, at borgeren i hvert fald har mulighed for selv at kontrollere afgivelse af – og tilbagetrækning heraf – oplysningen om, at borgeren er smittet med COVID-19, og at funktionaliteten i appen som standardindstilling skal være indstillet således, at der ikke sker deling af denne helbredsoplysning, før borgeren selv aktiverer delingen, jf. herved databeskyttelsesforordningens artikel 25, stk. 2, om databeskyttelse gennem standardindstillinger.

Styrelsen for Patientvirksomhed kan i fase 2 videregive opgørelser af antal kontakter med potentiel smitterisiko fordelt på køn og alder, samt opgørelser af antal kontakter koblet til faktisk smittede, hvis oplysningerne anonymiseres og aggregeres, dvs. i ikke-personhenførbar form. En sådan videregivelse falder uden for databeskyttelsesreglerne.

4.5 Fase 3 – Geolokation

Fase 3 vil – i tillæg til oplysningerne omfattet af fase 1 og 2 – indebære, at der sker en geografisk placering af samtlige de borgere – dvs. smittede såvel som ikke-smittede – der har downloadet appen baseret på GPS. Jeg har forstået det således, at formålet med registreringen af borgernes lokation er at give myndighederne mulighed for at monitorere kontaktmønstre i Danmark med henblik på at understøtte genåbningen af samfundet samt at give borgerne mulighed for gennem appen at kunne få overblik over og undgå de steder, hvor der er smittede.

Det er endnu uafklaret, hvor mange informationer der vil blive givet til borgeren om, hvornår borgeren er blevet udsat for smitterisiko, samt lokationen, hvor kontakten med den smittede skete. Hvis der gives informationer om både tid og sted

for kontakten med en smittet til borgeren, vil dette potentielt give borgeren endnu bedre mulighed for at kunne udlede identiteten på den anden smittede borger, hvorefter der i så fald vil ske en videregivelse af en helbredsoplysning, jf. også ovenfor vedrørende fase 2. Jeg skal i den forbindelse gøre opmærksom på, at dataminimeringsprincippet i databeskyttelsesforordningens artikel 5, stk. 1, litra c, ikke kan fraviges ved samtykke.

For så vidt angår hjemmelsgrundlaget, vil der skulle indhentes samtykke fra borgerne efter cookiebekendtgørelsen, hvis der opnås adgang til geolokationsdataene på borgernes mobile enheder.

Den påtænkte etablering og anvendelse af appen indebærer, at der vil blive indsamlet en overordentlig stor mængde personhenførbare oplysninger om lokationen på de smittede og ikke smittede borgere, der har downloadet appen, deres kontakter og færden. Oplysningerne vil blive lagret centralt i en database af Styrelsen for Patientsikkerhed. Det er således efter det oplyste forventningen, at størstedelen af Danmarks befolkning vil downloade og anvende appen. Appen vil med andre ord give et "coronalandkort" over borgernes færden i realtid. Indsamlingen af oplysninger om geolokation vil tillige give mulighed for at identificere følsomme oplysninger om f.eks. religiøse tilhørsforhold (besøg/ophold i religiøse institutioner),.

Omfanget og karakteren af oplysningerne, der vil blive lagret centralt i en database af Styrelsen for Patientsikkerhed – herunder mulighederne for samkøring af oplysningerne – medfører hermed, at der kan blive tale om omfattende overvågning af de omhandlede borgere.

Etableringen af og behandlingen af personoplysninger i appen giver derfor anledning til overvejelser om foreneligheden med de grundlæggende databeskyttelsesprincipper i databeskyttelsesforordningens artikel 5, herunder navnlig dataminimeringsprincippet (proportionalitet) og princippet om opbevaringsbegrænsning, der gælder, selvom der er indhentet samtykke til behandlingen af personoplysninger.

I proportionalitetsvurderingen må det tillægges betydelig vægt, at løsningen varetager et særdeles vægtigt og sagligt samfundsmæssigt formål om bekæmpelse af en dødelig virus, samt at løsningen er baseret på frivillighed (samtykke), således at borgerne har kontrol over, hvorvidt de vil downloade appen samt hvilke oplysninger, de vil dele i appen. Der må også lægges vægt på det oplyste om, at oplysningerne ikke er tiltænkt anvendt til brug for at træffe foranstaltninger over for enkeltindivider. Det bør være en yderligere forudsætning for lovlig etablering og anvendelse af løsningen, at der i videst mulige omfang behandles egentlige anonymiserede/aggregerede oplysninger og pseudonymisering. Det bør endvidere være et krav, at opbevaringsperioden for oplysninger begrænses til det absolut nødvendige i lyset af formålet, således at oplysningerne slettes eller anonymiseres effektivt, når denne periode er udløbet. Der skal fastlægges procedurer for sletning af oplysninger, det konkret viser sig unødvendigt at opbevare i systemet. I øvrigt skal databeskyttelsesforordningens regler overholdes, herunder regler om sikkerhed, de registreredes rettigheder, udarbejdelse af konsekvensanalyse vedrørende databeskyttelse, regler om indbygget databeskyttelse og databeskyttelse gennem standardindstillinger m.v.

Det er vurderingen, at der ved anvendelse af samtykke som behandlingsgrundlag kan etableres en ordning, hvor der sker en geografisk placering af borgere, der har downloadet appen. Der vil dog skulle foretages en endelig vurdering her, når der er taget stilling til den nærmere udformning af ordningen.

4.6 Overvejelser om særlig regulering

På denne baggrund er det min vurdering, at etableringen og anvendelsen af app'en i fase 3 vil kunne ske med borgernes samtykke – hvilket også er i overensstemmelse med forudsætningen om frivillighed – under forudsætning af, at de ovennævnte krav om dataminimering og opbevaringsbegrænsning m.v. overholdes.

Praksis fra Datatilsynet og tidligere Registertilsynet viser dog, at selvom databeskyttelsesforordningen (tidligere persondataloven og registerlovene) måtte udgøre et tilstrækkeligt retsgrundlag for behandlingen af personoplysningerne, vil det efter omstændighederne og ud fra mere overordnede samfunds- og retssikkerhedsmæssige overvejelser kunne være tilrådeligt, at der tilvejebringes en særskilt lovhjemmel eller administrativ regulering i bekendtgørelsesform for registrets oprettelse og førelse. Dette er også kommet til udtryk i legislativ praksis, og i den ovenfor omtalt ANPG-sag blev der fastsat regler om sletning m.v. i bekendtgørelsesform. I forbindelse med denne vurdering indgår overvejelser om bl.a. registrets formål, karakteren og omfanget af de registrerede oplysninger og den tilladte anvendelse af oplysningerne.

Henset til den omfattende mængde af personoplysninger, karakteren af disse samt muligheden og risikoen for gennem samkøring af foretage egentlig overvågning af borgerne, kan det overvejes at tilvejebringe et særskilt lovgrundlag for etableringen og anvendelsen af appen – i hvert fald for fase 3, der indebærer tilknytningen af oplysninger om geolokation. En sådan løsning vil skabe et sikkert grundlag for løsningens lovlighed, idet man vil kunne foretage en nærmere og mere detaljeret regulering af centrale forhold såsom formålene med behandlingen af personoplysningerne i løsningen, slettefrister, sikkerhedsforanstaltninger og begrænsninger af brugen af oplysningerne til foranstaltninger over for enkeltindivider m.v. Her vil man også kunne fastlægge, om dataene må anvendes til f.eks. at kunne lukke en bestemt børnehave eller strand, hvor der er konstateret mange smittede borgere. For at skabe fleksibilitet vil der kunne indarbejdes en bemyndigelsesbestemmelse til at fastsætte nærmere regler indenfor rammerne af databeskyttelsesforordningens rammer. Alternativt kan der tænkes en løsning, hvor ovennævnte forhold reguleres i bekendtgørelsesform med hjemmel i epidemiloven og databeskyttelseslovens § 7, stk. 5.