II

(Meddelelser)

MEDDELELSER FRA DEN EUROPÆISKE UNIONS INSTITUTIONER, ORGANER, KONTORER OG AGENTURER

EUROPA-KOMMISSIONEN

MEDDELELSE FRA KOMMISSIONEN

Vejledning om apps til støtte for bekæmpelse af covid-19-pandemien i forbindelse med databeskyttelse

(2020/C 124 I/01)

1 BAGGRUND

Covid-19-pandemien har skabt en hidtil uset udfordring for Unionen og medlemsstaterne, deres sundhedssystemer, livsstil, økonomiske stabilitet og værdier. Digitale teknikker og data spiller en værdifuld rolle i bekæmpelsen af covid-19-krisen. Mobilapplikationer, der typisk installeres på smartphones (apps), kan hjælpe de offentlige sundhedsmyndigheder på nationalt plan og EU-plan med at overvåge og inddæmme covid-19-pandemien og er særlig relevante i fasen med fjernelse af inddæmningsforanstaltningerne. De kan vejlede borgerne direkte og støtte kontaktopsporingsindsatsen. I en række lande, både inden for EU og globalt, har myndigheder og udviklere på nationalt eller regionalt plan annonceret lanceringen af apps med forskellige funktioner med henblik på at støtte bekæmpelsen af virussen.

Den 8. april 2020 vedtog Kommissionen en henstilling om en fælles EU-værktøjskasse med henblik på at udnytte teknologi og data til at bekæmpe og overvinde covid-19-krisen, navnlig hvad angår mobilapplikationer og anvendelse af anonymiserede mobilitetsdata ("henstillingen") [1]. Formålet med henstillingen er bl.a. at udvikle en fælles europæisk tilgang ("værktøjskasse") for anvendelse af mobilapplikationer, koordineret på EU-niveau, som skal gøre borgerne i stand til at træffe effektive foranstaltninger til at distancere sig socialt, og som skal advare, forebygge og spore kontakter for at bidrage til at begrænse spredningen af covid-19. I henstillingen fastsættes de generelle principper, der bør ligge til grund for udviklingen af en sådan værktøjskasse, og det fastsættes heri, at Kommissionen vil offentliggøre yderligere retningslinjer, herunder om følgerne for databeskyttelse og beskyttelse af privatlivets fred af anvendelse af applikationer på dette område.

Med den fælles europæiske køreplan for ophævelse af foranstaltningerne til inddæmning af covid-19 opstillede Kommissionen i samarbejde med formanden for Det Europæiske Råd en række principper, der skal være retningsgivende for udfasningen af foranstaltningerne til inddæmning af covid-19-udbruddet. Mobilapplikationer, herunder kontaktopsporingsfunktioner, kan spille en vigtig rolle i denne sammenhæng. Afhængigt af funktionerne i disse apps, og i hvilket omfang befolkningen bruger dem, kan de have en betydelig indvirkning på sygdomsdiagnosticering, behandling og håndtering af covid-19 i og uden for hospitalsmiljøet. De er særlig relevante, når inddæmningsforanstaltningerne ophæves, og risikoen for smitte vokser, i takt med at flere mennesker kommer i kontakt med hinanden. Disse applikationer kan bidrage til at afbryde smittekæder hurtigere og mere effektivt end generelle inddæmningsforanstaltninger og kan mindske risikoen for en betydelig spredning af virussen. De bør derfor være et vigtigt element i genåbningsstrategien og skal supplere andre foranstaltninger såsom øget testkapacitet [2]. En vigtig forudsætning for udvikling, accept og udbredelse af sådanne apps blandt brugerne er tillid. Folk skal have sikkerhed for, at overholdelsen af de grundlæggende rettigheder sikres, og at disse apps kun vil blive anvendt til de specifikt definerede formål, at de ikke vil blive anvendt til

[1] Henstilling C(2020) 2296 final af 8. april 2020. https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.
[2] https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

masseovervågning, og at brugerne fortsat bevarer fuld kontrol over deres egne data. Dette er grundlaget for nøjagtigheden og effektiviteten af sådanne apps, når det gælder om at inddæmme spredningen af virusset. Det er derfor vigtigt at finde løsninger, som er så lidt indgribende som muligt og fuldt ud opfylder kravene til beskyttelse af personoplysninger og privatlivets fred som fastsat i EU-lovgivningen. Derudover bør disse apps senest deaktiveres, når pandemien erklæres under kontrol. Appsene bør også omfatte de mest avancerede informationssikkerhedsforanstaltninger.

Denne vejledning tager hensyn til bidraget fra Det Europæiske Databeskyttelsesråd (EDPB) ([3]) og drøftelser inden for e-sundhedsnetværket. EDPB planlægger at offentliggøre retningslinjer i de kommende dage om geolokalisering og andre opsporingsværktøjer i forbindelse med covid-19-udbruddet.

Vejledningens anvendelsesområde

For at sikre en sammenhængende tilgang i hele EU og yde vejledning til medlemsstaterne og app-udviklere beskriver dette dokument, hvilke funktioner og krav disse apps bør opfylde for at sikre overholdelse af EU-lovgivningen om databeskyttelse og beskyttelse af privatlivets fred, navnlig den generelle forordning om databeskyttelse ([4]) (GDPR) og e-databeskyttelsesdirektivet ([5]). Denne vejledning omhandler ikke yderligere betingelser, herunder begrænsninger, som medlemsstaterne kan have medtaget i deres nationale lovgivning for så vidt angår behandlingen af helbredsoplysninger.

Vejledningen er ikke juridisk bindende. Den berører ikke EU-Domstolens rolle, som er den eneste institution, der kan foretage en autoritativ fortolkning af EU-retten.

Denne vejledning omhandler kun frivillige apps til støtte for bekæmpelse af covid-19-pandemien (apps, der downloades, installeres og anvendes på frivillig basis af brugerne) med en eller flere af følgende funktioner:

— leverer nøjagtige oplysninger til brugerne om covid-19-pandemien

— tilvejebringer spørgeskemaer til selvevaluering og vejledning for den enkelte (funktion til symptomverifikation) ([6])

— advarer personer, der i en vis periode har været i nærheden af en smittet person, for bl.a. at oplyse om, hvorvidt de bør gå i karantæne, og hvor de kan blive testet (kontaktopsporing og advarselsfunktion)

— fungerer som et kommunikationsforum mellem patienter og læger i situationer med isolation eller for yderligere diagnosticerings- og behandlingsrådgivning (øget brug af telemedicin).

I henhold til e-databeskyttelsesdirektivet er det kun muligt at indføre obligatorisk brug af en app, der omfatter retten til kommunikationshemmelighed som omhandlet i artikel 5, via lovgivning, som er nødvendig, passende og forholdsmæssig med henblik på at beskytte visse specifikke mål. I betragtning af den store grad af indgriben, der er forbundet med en sådan tilgang, og de udfordringer, der er forbundet hermed, herunder indførelsen af passende sikkerhedsforanstaltninger, er der ifølge Kommissionen behov for en omhyggelig analyse, inden denne mulighed anvendes. Af disse grunde anbefaler Kommissionen, at der anvendes frivillige apps.

Denne vejledning omhandler ikke apps, der har til formål at håndhæve karantænekrav (herunder obligatoriske krav).

2 BIDRAG FRA APPS TIL BEKÆMPELSE AF COVID-19

Funktionen til symptomverifikation er et værktøj, som kan benyttes af de offentlige sundhedsmyndigheder til at vejlede borgerne om testning for covid-19 og oplyse om isolation, om hvordan man undgår at smitte andre, og hvordan man søger sundhedsbehandling. Den kan også supplere overvågningen i den primære sundhedspleje og bruges til bedre oplysning om covid-19-infektionsraten i befolkningen.

([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

([4]) 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) (EUT L 119 af 4.5.2016, s. 1).

([5]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

([6]) Hvis disse apps leverer oplysninger om diagnosticering, forebyggelse, overvågning, forudsigelse eller prognose, bør de vurderes med hensyn til deres potentielle karakter af medicinsk udstyr i henhold til den lovgivningsmæssige ramme for medicinsk udstyr. For så vidt angår disse rammer, se Rådets direktiv 93/42/EØF af 14. juni 1993 om medicinsk udstyr (EFT L 169 af 12.7.1993, s. 1) og Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr (EUT L 117 af 5.5.2017, s. 1).

Kontaktopsporings- og advarselsfunktioner er værktøjer til at identificere personer, der har været i kontakt med en person, der er smittet med covid-19, og til at underrette vedkommende om, hvilke næste skridt der vil være hensigtsmæssige, såsom karantæne, testning eller rådgivning om, hvad der skal gøres i tilfælde af symptomer. Denne funktion er derfor nyttig både for den enkelte borger og de offentlige sundhedsmyndigheder. Den kan også spille en vigtig rolle i forvaltningen af inddæmningsforanstaltninger i forbindelse med genåbningsscenarier. Dens virkning kan forstærkes med en strategi, der understøtter en mere omfattende testning af personer med milde symptomer.

Begge funktioner kan også være en relevant datakilde for de offentlige sundhedsmyndigheder og lette overførslen af sådanne data til de nationale epidemiologiske myndigheder og til Det Europæiske Center for Forebyggelse af og Kontrol med Sygdomme (ECDC). Dette vil bidrage til at forstå smittemønstre og — i kombination med testresultater — anslå den positive prognoseværdi af luftvejssymptomer i et givet samfund og dermed tilvejebringe oplysninger om omfanget af virus i omløb.

Skønnenes pålidelighed er direkte forbundet med antallet og pålideligheden af de indberettede data.

Kombineret med passende teststrategier kan både symptomverifikations- og kontaktopsporingsfunktionerne derfor tilvejebringe oplysninger om omfanget af virus i omløb og hjælpe med at vurdere virkningen af social distancering og isolationsforanstaltninger. Som anført i henstillingen bør der sikres interoperabilitet mellem IT-løsninger i de forskellige medlemsstater for at muliggøre grænseoverskridende samarbejde og sikre kontaktopsporing mellem brugere af forskellige apps (især vigtig, når borgerne krydser grænser). Hvis en smittet person kommer i kontakt med en bruger af en app fra en anden medlemsstat, bør det være muligt at videregive personoplysninger om denne bruger på tværs af grænserne til sundhedsmyndighederne i den pågældende medlemsstat, i det omfang det er strengt nødvendigt. Arbejdet med dette spørgsmål vil finde sted som en del af den værktøjskasse, der er meddelt i henstillingen. Der bør sikres interoperabilitet både ved hjælp af tekniske krav og ved at forbedre kommunikationen og samarbejdet mellem de nationale sundhedsmyndigheder. Der kan også anvendes en model for et bestemt samarbejde ([7]) som en styringsmodel for kontaktopsporingsapps under covid-19-pandemien.

3 ELEMENTER TIL AT SIKRE TILLIDSFULD OG ANSVARLIG BRUG AF APPS

De funktioner, der indgår i disse apps, kan have forskellig indvirkning på en lang række rettigheder, som er nedfældet i EU's charter om grundlæggende rettigheder, såsom menneskelig værdighed, respekt for privatliv og familieliv, beskyttelse af personoplysninger, fri bevægelighed, ikke-forskelsbehandling, frihed til at oprette og drive egen virksomhed samt forsamlings- og foreningsfrihed. Denne indgriben i privatlivets fred og retten til beskyttelse af personoplysninger kan være særlig betydelig, da nogle af funktionerne er baseret på en dataintensiv model.

Formålet med de elementer, der præsenteres nedenfor, er at vejlede om, hvordan app-funktionernes indgribende karakter kan begrænses for at sikre overholdelse af EU's lovgivning om beskyttelse af personoplysninger og privatlivets fred.

3.1 Nationale sundhedsmyndigheder (eller organer, der varetager opgaver af offentlig interesse på sundhedsområdet) som dataansvarlig

Identificeringen af, hvem der tager stilling til formålet med, og de midler der benyttes til, databehandlingen (den dataansvarlige) er afgørende for at fastslå, hvem der er ansvarlig for overholdelsen af EU's regler om beskyttelse af personoplysninger, og navnlig: hvem der skal oplyse de personer, der downloader appen, om, hvad der skal ske med deres personoplysninger (allerede eksisterende eller dem, der skal genereres gennem enheden, f.eks. en smartphone, hvorpå appen installeres), hvad er deres rettigheder er, hvem der er ansvarlig i tilfælde af brud på datasikkerheden osv.

I betragtning af de foreliggende personoplysningers følsomhed og formålet med databehandlingen som beskrevet nedenfor er Kommissionen af den opfattelse, at disse apps bør udformes således, at de nationale sundhedsmyndigheder (eller organer, der varetager opgaver af offentlig interesse på sundhedsområdet) fungerer som dataansvarlige ([8]). De dataansvarlige er ansvarlige for at sikre overholdelse af GDPR (princippet om ansvarlighed). Omfanget af en sådan adgang bør begrænses ud fra de principper, der er beskrevet i afsnit 3.5 nedenfor.

([7]) Et sådant samarbejde finder allerede sted i forbindelse med projektet MyHealth@EU om udveksling af patientjournaler og e-recepter. Se også artikel 5, stk. 5, og betragtning 17 i Kommissionens gennemførelsesafgørelse 2019/1765.

([8]) Se betragtning 45 i GDPR.

Dette vil også bidrage til en højere tillid i befolkningen og således accept af disse apps (og de underliggende smittekædere-laterede informationssystemer) og vil sikre, at de opfylder det tilsigtede mål om at beskytte folkesundheden. De underliggende politikker, krav og kontroller bør samordnes og gennemføres på en koordineret måde af de ansvarlige nationale sundhedsmyndigheder.

3.2 **Sikring af, at den enkelte borger bevarer kontrollen**

En afgørende faktor for, at de enkelte borgere kan have tillid til applikationerne, er at man er i stand til at påvise, at de bevarer kontrollen over deres personoplysninger. Kommissionen er med henblik på dette af den opfattelse, at navnlig følgende betingelser skal være opfyldt:

— Installation af applikationen på deres enhed bør være frivillig, og det må ikke have negative konsekvenser for den enkelte bruger, som beslutter ikke at downloade eller bruge applikationen;

— forskellige applikationsfunktioner (f.eks. informations-, symptomverifikations-, kontaktopsporings- og advarsels-funktioner) bør ikke bundtes, således at brugeren kan give sit samtykke til hver funktion. Dette bør ikke forhindre brugeren i at kombinere forskellige applikationsfunktioner, hvis udbyderen tilbyder dem som option.

— Hvis der anvendes nærhedsdata (data genereret ved udveksling af Bluetooth Labit Energy (BLE) signaler mellem enheder inden for en epidemiologisk relevant afstand og i en epidemiologisk relevant periode), skal de opbevares på brugerens enhed. Hvis disse data skal deles med sundhedsmyndighederne, bør de kun deles, efter at det er blevet bekræftet, at den pågældende bruger er smittet med covid-19, og på den betingelse, at vedkommende vælger at gøre det;

— sundhedsmyndighederne bør give de enkelte brugere alle nødvendige oplysninger vedrørende behandlingen af deres personoplysninger (jf. artikel 12 og 13 i GDPR og artikel 5 i e-databeskyttelsesdirektivet).

— Brugeren bør kunne udøve sine rettigheder i henhold til GDPR (navnlig adgang, berigtigelse og sletning). Enhver begrænsning af de rettigheder, der følger af GDPR og e-databeskyttelsesdirektivet, bør være i overensstemmelse med disse retsakter og være nødvendig, proportionel og fastsat i lovgivningen.

— Applikationerne bør senest deaktiveres, når pandemien erklæres under kontrol. Deaktiveringen bør ikke afhænge af, at brugeren foretager afinstallering.

3.3 **Retsgrundlag for behandling**

Installation af applikationer og lagring af oplysninger på brugerens enhed

Som nævnt ovenfor er det i henhold til e-databeskyttelsesdirektivet (artikel 5) kun tilladt at lagre oplysninger om brugerens enhed eller at få adgang til de allerede lagrede oplysninger, i) hvis brugeren har givet sit samtykke, eller ii) hvis lagringen og/eller adgangen er strengt nødvendig for den informationssamfundstjeneste (f.eks. applikationen), som brugeren udtrykkeligt har anmodet om (dvs. installeret og aktiveret).

Lagring af oplysninger på brugerens enhed og adgang til oplysninger, der allerede er lagret på denne enhed, er normalt nødvendig for, at applikationerne fungerer. Desuden kræver kontaktopsporings- og advarselsfunktionen andre oplysninger (f.eks. midlertidige, periodisk ændrede aliasser for brugere af denne funktion i nærheden), der skal lagres på brugerens enhed. Desuden vil denne funktion kræve, at (den smittede eller sandsynligt smittede) bruger uploader nærhedsdata. Et sådant upload er som sådan ikke nødvendig for, at applikationen fungerer. Kravene under option ii), som er nævnt i forrige afsnit, er derfor ikke opfyldt, og optionen med samtykke (option i) ovenfor) er således det mest passende grundlag for de pågældende aktiviteter. Dette samtykke bør være "frit givet", "specifikt", "eksplicit" og "informeret" i henhold til GDPR. Det bør udtrykkes gennem en klar bekræftelse fra brugeren, hvilket udelukker stiltiende samtykke (f.eks. tavshed, inaktivitet) ([9]).

([9]) Se retningslinjerne fra Det Europæiske Databeskyttelsesråd om samtykke: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Retsgrundlag for nationale sundhedsmyndigheders behandling — EU-lovgivning eller medlemsstatslovgivning

De nationale sundhedsmyndigheder behandler typisk personoplysninger, når der foreligger en retlig forpligtelse i henhold til EU-lovgivningen eller medlemsstaternes nationale lovgivning, der foreskriver en sådan behandling og opfylder betingelserne i artikel 6, stk. 1, litra c), og artikel 9, stk. 2, litra i), i GDPR, eller når en sådan behandling er nødvendig for udførelsen af en opgave i almenhedens interesse, som er anerkendt i EU-lovgivningen eller medlemsstaternes nationale lovgivning ([10]).

Enhver national lovgivning skal indeholde specifikke og passende foranstaltninger til beskyttelse af registreredes rettigheder og frihedsrettigheder. En generel regel er, at jo større indvirkning på de registreredes frihedsrettigheder, jo stærkere skal de tilsvarende beskyttelsesforanstaltninger, der bør fastsættes i den relevante lovgivning, være.

EU's og medlemsstaternes lovgivning, der eksisterede forud for covid-19-udbruddet, og den, som medlemsstaterne har vedtaget specifikt for at bekæmpe spredning af epidemier, kan i princippet anvendes som retsgrundlag for behandling af personoplysninger, hvis det sker i forbindelse med foranstaltninger, der muliggør overvågning af epidemier, og hvis denne lovgivning opfylder yderligere krav i artikel 6, stk. 3, i GDPR.

I betragtning af de pågældende personoplysningers karakter (navnlig helbredsoplysninger som særlige kategorier af personoplysninger) samt omstændighederne i forbindelse med den nuværende covid-19-pandemi, vil en henvisning til lovgivningen som retsgrundlag bidrage til retssikkerheden, da den i) på detaljeret vis foreskriver behandlingen af specifikke sundhedsoplysninger og klart angiver formålene med behandlingen; ii) præciserer, hvem der er den dataansvarlige, dvs. den enhed, der behandler oplysningerne, og hvem der ud over den dataansvarlige kan få adgang til sådanne data; iii) udelukker muligheden for at behandle sådanne oplysninger til andre formål end dem, der er anført i lovgivningen; og iv) giver specifikke garantier. For ikke at underminere offentlighedens nytte og accept af applikationerne bør den nationale lovgiver være særlig opmærksom på at gøre den valgte løsning så inklusiv som muligt.

Behandling foretaget af sundhedsmyndighederne på grundlag af lovgivningen ændrer ikke ved, at den enkelte borger frit kan vælge at installere eller ikke installere applikationen og dele deres data med sundhedsmyndighederne. Det bør således ikke have negative konsekvenser for brugere, når applikationen afinstalleres.

Kontaktopsporings- og advarselsapplikationer giver mulighed for at advare enkeltpersoner. Når denne advarsel kommer direkte fra applikationen, henleder Kommissionen opmærksomheden på forbuddet mod at pålægge enkeltpersoner en afgørelse, der udelukkende er baseret på automatisk behandling, og som har retsvirkning eller på tilsvarende vis påvirker de pågældende (artikel 22 i GDPR).

3.4 **Dataminimering**

De data, der er genereret via enheder, og som allerede tidligere er blevet oplagret i disse enheder, er beskyttet som følger:

— De er som "personoplysninger", dvs. oplysninger om en identificeret eller identificerbar fysisk person (artikel 4, stk. 1, i GDPR), beskyttet i henhold til GDPR. Helbredsoplysninger er omfattet af yderligere beskyttelse (artikel 9 i GDPR).

— De er som "lokaliseringsdata", dvs. data, der behandles i et elektronisk kommunikationsnet eller en elektronisk kommunikationstjeneste og angiver den geografiske position af brugerens terminaludstyr, beskyttet i henhold til e-databeskyttelsesdirektivet (artikel 5, stk. 1, og artikel 6 og 9) ([11])

— Alle oplysninger, der lagres i og tilgås fra brugerens terminaludstyr, er beskyttet i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet.

Andre data end personoplysninger (f.eks. uigenkaldeligt anonymiserede data) er ikke beskyttet i henhold til GDPR.

Kommissionen henviser til, at man i henhold til princippet om dataminimering kun skal behandle de personoplysninger, der er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til formålet ([12]). En vurdering af nødvendigheden af at behandle personoplysningerne og relevansen af sådanne personoplysninger bør foretages i lyset af det eller de formål, der forfølges.

Kommissionen bemærker, at hvis formålet med funktionen f.eks. er symptomverifikation eller telemedicin, kræver sådanne formål ikke adgang til enhedsejerens kontaktliste.

([10]) Artikel 6, stk. 1, litra e), i GDPR.

([11]) Ifølge den europæiske kodeks for elektronisk kommunikation er tjenester, som rent funktionelt svarer til elektroniske kommunikationstjenester, også omfattet.

([12]) Princippet om dataminimering.

Generering og behandling af færre data begrænser sikkerhedsrisiciene. Ved at overholde princippet om dataminimering opnås der samtidig en række garantier.

— Informationsfunktion:

En applikation, der udelukkende indeholder denne funktion, vil ikke skulle behandle helbredsoplysninger om enkeltpersoner. Den vil blot give dem oplysninger. For at opfylde dette mål må der ikke ske behandling af oplysninger, som lagres i og tilgås fra terminaludstyret, ud over hvad der er nødvendigt for at give oplysninger.

— Symptomverifikations- og telemedicinfunktioner:

Hvis applikationen indeholder en eller to af disse funktioner, behandler den personlige sundhedsoplysninger. Derfor bør en liste over oplysninger, der kan behandles, specificeres i den lovgivning, der ligger til grund for sundhedsmyndighedernes virke.

Hertil kommer, at sundhedsmyndighederne kan have brug for telefonnumre til de personer, der har anvendt symptomverifikation og uploadet resultaterne. Oplysninger, der lagres i og tilgås fra terminaludstyr, må kun behandles i det omfang, det er nødvendigt for, at applikationen kan opfylde sit formål og fungere.

— Kontaktopsporings- og advarselsfunktioner:

Et flertal af covid-19-smittetilfælde opstår via dråber, der bevæger sig over en begrænset afstand. For at afbryde smittekæden er det således af afgørende betydning hurtigst muligt at identificere personer, der har været i nærheden af en smittet person. Bestemmelsen af, hvorvidt en sådan nærhed har fundet sted, afhænger af afstanden og varigheden af en kontakt, og bør konstateres på et epidemiologisk grundlag. Afbrydelsen af smittekæden er særlig relevant for at undgå genopblussen af smittetilfælde i genåbningsfasen.

Der kan til dette formål være behov for nærhedsdata. For at måle afstand og nærkontakt synes Bluetooth Low Energy (BLE) kommunikation mellem enheder at være mere præcist og derfor mere hensigtsmæssigt end brugen af geolokaliseringsdata (GNSS/GPS eller data for mobillokaliseringsdata). BLE gør det muligt at undgå sporing (i modsætning til geolokaliseringsdata). Kommissionen anbefaler derfor anvendelsen af BLE-kommunikationsdata (eller data genereret med tilsvarende teknologi) med henblik på at fastslå nærkontakt.

Lokaliseringsdata er ikke nødvendige med henblik på kontaktopsporingsfunktioner, da de ikke har som formål at følge enkeltpersoners bevægelser eller håndhæve forbud. Desuden vil det være vanskeligt at begrunde behandlingen af lokaliseringsdata i forbindelse med kontaktopsporing i forhold til princippet om dataminimering, og det kan skabe problemer med hensyn til sikkerhed og privatlivets fred. Derfor anbefaler Kommissionen ikke at anvende lokaliseringsdata i denne kontekst.

Uanset de tekniske midler, der anvendes til at fastslå nærkontakten, forekommer det ikke nødvendigt at gemme det nøjagtige tidspunkt for kontakten eller stedet (hvis det er tilgængeligt). Det kan dog være nyttigt at lagre datoen for kontakten for at afdække, om kontakten fandt sted, da den pågældende udviklede symptomer (eller 48 timer før ([13])), og udforme den opfølgende meddelelse med rådgivning om, hvor længe der skal ske selvkarantæne.

Nærhedsdata bør kun genereres og behandles, hvis der er en reel risiko for smitte (afhængigt af kontaktens nærhed og varighed).

Det skal bemærkes, at dataindsamlingens nødvendighed og proportionalitet således vil afhænge af faktorer som f.eks. i hvilket omfang der er adgang til testudstyr, navnlig når der allerede er truffet afgørelse om foranstaltninger som f.eks. karantæne. Personer, der har været i nærkontakt med en smittet person, kan advares på to måder:

Med den første metode leveres en advarsel automatisk via applikationen til de personer, hvormed brugeren har været i nærkontakt, når brugeren meddeler applikationen — med sundhedsmyndighedens godkendelse eller bekræftelse, f.eks. via en QR-kode eller TAN-kode — at han eller hun er blevet testet positiv (decentraliseret behandling). Indholdet af advarselsmeddelelsen bør helst fastsættes af sundhedsmyndighederne. Med den anden metode lagres de vilkårlige midlertidige identifikatorer på en backend-server, som styres af sundhedsmyndigheden (backend-server-løsning). Brugerne kan ikke identificeres direkte på grundlag af disse data. Brugere, som har været i nærkontakt med en bruger, der er testet positiv, vil med hjælp af identifikatorer modtage en advarsel på deres enhed. Hvis sundhedsmyndighederne ønsker at kontakte de brugere, der har været i nærkontakt med en smittet person, også via telefon eller SMS, har de brug for disse brugeres samtykke til at opnå deres telefonnumre.

([13]) Den smittede person er smitsom 48 timer før symptomernes start.

3.5 **Begrænsning af videregivelse af/adgang til data**

— Informationsfunktion:

Oplysninger, der lagres i og tilgås fra terminaludstyr, må kun deles med sundhedsmyndighederne i det omfang, det er nødvendigt for at benytte informationsfunktionen. Da denne funktion kun udgør kommunikationskanalen, får sundhedsmyndighederne ikke adgang til andre data.

— Symptomverifikations- og telemedicinfunktioner:

Funktionen til symptomverifkation kan være nyttig for medlemsstaterne med henblik på at vejlede borgerne om, hvorvidt de bør testes, give oplysninger om isolation og om adgang til sundhedsydelser, især for risikogrupper. Denne funktion kan også supplere overvågningen i den primære sundhedspleje og bidrage til at give et billede af covid-19-smitteraten i befolkningen. Det besluttes måske derfor, at de ansvarlige sundhedsmyndigheder og nationale epidemimyndigheder bør have adgang til de oplysninger, patienten har afgivet. ECDC kan modtage aggregerede data fra de nationale myndigheder med ansvar for epidemiovervågning.

Hvis det besluttes at tillade kontakt med sundhedspersonale i stedet for kun gennem appen, er det også nødvendigt at oplyse applikationsbrugernes telefonnumre til de nationale sundhedsmyndigheder.

— Kontaktopsporings- og advarselsfunktioner:

— Den smittede persons oplysninger

Applikationerne genererer pseudo-vilkårlige efemeriske identifikatorer for de telefoner, som brugeren er i kontakt med. En mulighed er, at identifikatorer lagres på brugerens enhed (”decentraliseret behandling”). En anden mulighed er, at disse vilkårlige identifikatorer lagres på den server, som sundhedsmyndighederne har adgang til (”backendserverløsning”). Den decentrale løsning er mere i overensstemmelse med minimeringsprincippet. Sundhedsmyndighederne bør kun have adgang til nærhedsdata fra en smittet persons enhed for at kunne kontakte personer, der kan være blevet smittet.

Sådanne data vil først være tilgængelige for sundhedsmyndighederne, når den smittede person (efter at være blevet testet) proaktivt deler disse data med dem.

Den smittede person bør ikke oplyses om identiteten af de personer, som den pågældende har været i potentielt epidemiologisk relevant kontakt med, og som vil blive underrettet.

— Data om de personer, der har været i (epidemiologisk) kontakt med den smittede person

Den smittede persons identitet må ikke videregives til de personer, som den pågældende har været i epidemiologisk kontakt med. Det er tilstrækkeligt at meddele dem, at de har været i epidemiologisk kontakt med en smittet person inden for de sidste 16 dage. Som anført ovenfor bør oplysninger om tid og sted for sådanne kontakter ikke lagres. Det er derfor hverken nødvendigt eller muligt at videregive disse oplysninger.

Med henblik på opsporing af epidemiologiske kontakter for en e-applikationsbruger, der konstateres smittet, bør de nationale sundhedsmyndigheder kun underrettes om identifikatoren for den person, som den smittede person har været i epidemiologisk kontakt med fra 48 timer før symptomernes opståen indtil 14 dage efter symptomernes opståen, på grundlag af nærhed og varighed af kontakten.

ECDC kan modtage aggregerede kontaktopsporingsdata fra de nationale myndigheder med ansvar for epidemiovervågning for indikatorer, der fastlægges i samarbejde med medlemsstaterne.

3.6 **Fastlæggelse af de præcise formål med behandlingen**

Retsgrundlaget (EU-ret eller national ret) bør fastsætte formålet med behandlingen. Formålet skal være specifikt, således at der ikke er tvivl om, hvilken type persondata der er nødvendige for at nå det ønskede mål.

Det eller de præcise formål afhænger af applikationens funktioner. Der kan være flere formål for hver funktion i en applikation. For at give den enkelte borger fuld kontrol over deres data anbefaler Kommissionen ikke at samle forskellige funktioner. Under alle omstændigheder bør den enkelte borger have mulighed for at vælge mellem forskellige funktioner, der har hver sit formål.

Kommissionen fraråder, at data indsamlet på ovenstående betingelser anvendes til andre formål end bekæmpelse af covid-19. Hvis formål som videnskabelig forskning og statistik er nødvendige, bør de medtages i den oprindelige liste over formål og kommunikeres klart til brugerne.

— Informationsfunktion:

Formålet med denne funktion er at tilvejebringe oplysninger, der er relevante for sundhedsmyndighederne i forbindelse med krisen.

— Funktioner til symptomverifikation og telemedicin:

Funktionen til symptomverifikation kan give en indikation af, hvor stor en andel af de personer, der melder om covid-19-kompatible symptomer, der rent faktisk er smittede (f.eks. ved podning og test af alle eller et vilkårligt antal personer med sådanne symptomer, hvis der er kapacitet til det). Denne identifikation af formålet bør gøre det klart, at personlige sundhedsoplysninger vil blive behandlet for i) at give personen mulighed for på grundlag af en række spørgsmål selv at vurdere, om vedkommende har symptomer på covid-19, eller ii) at få lægehjælp, hvis vedkommende har symptomer på covid-19.

— Kontaktopsporings- og advarselsfunktioner:

Den blotte angivelse af et formål om "forebyggelse af yderligere covid-19-smitte" er ikke specifik nok. I dette tilfælde anbefaler Kommissionen yderligere præcisering af formålet/formålene i stil med: "opbevaring af kontakter for de personer, der anvender applikationen, og som kan have været eksponeret for covid-19-smitterisiko, med henblik på at advare personer, der kan være blevet smittet".

3.7 **Fastsættelse af strenge grænser for lagring af data**

I henhold til princippet om begrænsning af lagring må personoplysninger ikke opbevares længere end nødvendigt. Tidsfrister bør baseres på den medicinske relevans (afhængigt af formålet med applikationen: inkubationstid osv.) og den tid, det forventeligt vil tage at træffe nødvendige administrative foranstaltninger.

— Informationsfunktion:

Hvis der indsamles data, mens denne funktion installeres, skal de straks slettes. Der er ingen begrundelse for at lagre sådanne data.

— Symptomverifikations- og telemedicinfunktioner:

Sådanne data bør slettes af sundhedsmyndighederne efter højst en måned (inkubationstid plus margin), eller efter at personen er blevet testet, og resultatet er negativt. Sundhedsmyndighederne kan opbevare data i længere tid med henblik på overvågningsrapportering og forskning, forudsat at oplysningerne er i anonymiseret form.

— Kontaktopsporings- og advarselsfunktioner:

Nærhedsdata bør slettes, så snart de ikke længere er nødvendige for at advare enkeltpersoner. Det bør være tilfældet efter højst en måned (inkubationstid plus margin), eller efter at personen er blevet testet, og resultatet er negativt. Sundhedsmyndighederne kan opbevare data i længere tid med henblik på overvågningsrapportering og forskning, forudsat at oplysningerne er i anonymiseret form.

Dataene bør lagres på brugerens enhed, og kun data, der er meddelt af brugerne, og som er nødvendige for at opfylde formålet, bør uploades til den server, der er til rådighed for sundhedsmyndighederne, når denne mulighed vælges (dvs. upload kun data til serveren vedrørende "tætte kontakter" for en person, der er blevet testet positiv for smitte med covid-19).

3.8 **Sikring af datasikkerheden**

Kommissionen anbefaler, at dataene lagres på brugerens terminalenhed i krypteret form ved brug af de nyeste krypteringsteknikker. Hvis oplysningerne lagres på en central server, skal adgangen, herunder også administrativ adgang, registreres.

Nærhedsdata bør kun genereres og lagres på brugerens terminalenhed i krypteret og pseudonymiseret format. For at forebygge sporing foretaget af tredjeparter bør det være muligt at aktivere Bluetooth uden at skulle aktivere andre lokaliseringstjenester.

Ved indsamling af nærhedsdata via BLE er det bedre at oprette og lagre midlertidige bruger-ID'er, der ændres regelmæssigt, end at lagre det faktiske enheds-ID. Denne foranstaltning giver yderligere beskyttelse mod aflytning og sporing foretaget af hackere og gør det derfor vanskeligere at identificere enkeltpersoner.

Kommissionen anbefaler, at applikationens kildekode gøres offentlig tilgængelig.

Der kan overvejes yderligere foranstaltninger til sikring af de behandlede data, navnlig automatisk sletning eller anonymisering af dataene efter et bestemt tidspunkt. Generelt bør sikkerhedsgraden svare til mængden og følsomheden af de behandlede personoplysninger.

Alle transmissioner fra den personlige enhed til de nationale sundhedsmyndigheder bør krypteres.

Hvis det i den nationale lovgivning er fastsat, at de indsamlede personoplysninger også kan behandles til videnskabelige forskningsformål, kan der anvendes pseudonymisering.

3.9 **Sikring af datanøjagtigheden**

Sikring af nøjagtigheden af de behandlede personoplysninger er ikke kun en forudsætning for applikationens effektivitet, men er også et krav i lovgivningen om beskyttelse af personoplysninger.

I den forbindelse er det afgørende at sikre nøjagtigheden af oplysningerne om, hvorvidt kontakt med en smittet person (epidemiologisk afstand og varighed) har fundet sted, for at minimere risikoen for falske positiver. Dette bør omfatte scenarier, hvor to brugere af applikationen er i kontakt på gaden, i offentlig transport eller i en bygning. Det er usandsynligt, at anvendelsen af lokaliseringsdata baseret på mobiltelefonnettet er tilstrækkeligt præcis til dette formål.

Det anbefales derfor, at man baserer sig på teknologier, der muliggør en mere præcis vurdering af kontakten (såsom Bluetooth).

3.10 **Inddragelse af databeskyttelsesmyndigheder**

Databeskyttelsesmyndighederne bør inddrages fuldt ud og høres i forbindelse med udviklingen af applikationen samt løbende holde øje med udrulningen. Da databehandlingen i forbindelse med applikationen betragtes som en behandling i stort omfang af særlige kategorier af data (helbredsoplysninger), henleder Kommissionen opmærksomheden på artikel 35 i GDPR.