# Konsekvensanalyse vedr. databeskyttelse

## Smittestop-app til kontaktregistrering og smitteopsporing i forbindelse med genåbning af Danmark i den igangværende COVID-19-pandemi

Dataansvarlig: Styrelsen for Patientsikkerhed

Dato: 17. juni 2020

Ansvarlig kontaktperson: Birgitte Drewes, enhedschef, Styrelsen for Patientsikkerhed

Databeskyttelsesrådgiver (DPO): Helle Ginnerup-Nielsen

| Version | Kommentar |
|---|---|
| 1.1 (19.06.20) | Opdateret for at afspejle de seneste mitigerende foranstaltninger |
| 1.0 (17.06.20) | Mindre grammatiske rettelser. |
| 0.9 (16.06.20) | Faktatjekket, verificeret m. teknikere og mod løsning. |
| 0.2 (02.06.20) | Andet udkast, opdateret på baggrund af ændringer i design af løsning. |
| 0.1 (30.04.20) | Første udkast. |

# Indhold

## 1. SAMMENFATNING

Denne konsekvensanalyse vedrørende databeskyttelse er gennemført af Styrelsen for Patientsikkerhed i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 35.

De væsentligste risici i løsningen er, at borgerne ikke kan overskue konsekvenserne af deres accept af frivilligt at dele information om smittestatus med andre (smittenotifikation). Derudover vil borgerne i forbindelse med en smittenotifikation i meget sjældne tilfælde kunne identificere den smittede, der har valgt at notificere sine kontakter herom. Det gælder i de tilfælde, hvor en borger, der modtager en smittenotifikation i appen, alene har haft én enkelt elektronisk kontakt (med den smittede) i løbet af en periode på 14 dage. En yderligere risiko er risikoen for manglende eller tab af pseudonymisering af personoplysninger i løsningen, således at borgerne vil kunne identificeres af uvedkommende. Derudover er der risiko for, at appen enten ikke er effektiv henset formålet, eller at for få brugeren anvender den.

Styrelsen for Patientsikkerhed vurderer dog, at disse risici – såvel som øvrige identificerede risici vedrørende appen – gennem fornødne tekniske og organisatoriske foranstaltninger, herunder sikkerhedsforanstaltninger samt udførlig information af brugerne af appen, kan nedbringes til et passende niveau forud for de behandlinger af personoplysninger, der er forbundet med appen, således at behandlingen ikke vil føre til en høj risiko for de registreredes rettigheder og frihedsrettigheder. Det er derfor også styrelsens vurdering, at styrelsen ikke har pligt til at foretage en høring af Datatilsynet forud for behandlingen af personoplysningerne i løsningen, idet der ikke foreligger en høj risiko for de registrerede efter reducering af risiciene gennem de nævnte foranstaltninger.

Styrelsen har herved lagt betydelig vægt på, at brug af appen er frivillig, at der i - og i forbindelse med - appen vil blive givet en udførlig information til brugerne om appens funktioner og begrænsninger, før brugerne vælger at benytte løsningen og dens funktionalitet i form af smittenotifikation. Brugerne vil blive informeret om den (begrænsede) risiko for, at en bruger, der er smittet med virussen, i meget sjældne tilfælde vil kunne blive identificeret som smittet af de personer, som den pågældende smittede bruger har været i elektronisk kontakt med, hvis den smittede bruger vælger frivilligt at notificere sine kontakter om, at brugeren er smittet.

Det bemærkes, at hele løsningen er baseret på en underliggende teknisk snitflade (API) udviklet af Google og Apple til brug på brugernes udstyr (devices). API'et er udviklet med det formål at sikre mest mulig privatlivsbeskyttelse og beskyttelse af brugerdata. Dette sikres blandt andet ved, at der kun registreres oplysninger om brugernes kontakter på brugernes telefon[1] og at det ikke er muligt for andre,

[1] Den såkaldte "decentrale model"

herunder STPS, at tilgå disse oplysninger. Der overføres heller ikke personoplysninger til Google eller Apple.

Styrelsen har endelig lagt vægt på, at der i løsningen er anvendt en pseudonymiseringsteknik, der sikrer, at det er meget vanskeligt at koble de oplysninger, der behandles, med de enkelte brugere. Dette gøres blandt andet gennem tilfældigt genererede rullende ID'er, der opdateres hver 10.-20. minut og ved at alle registreringer af kontakter kun lagres på brugerens telefon. Pseudonymiseringsteknikken er udviklet af Google og Apple som del af API'et.

Løsningen er endvidere udarbejdet efter reglerne om indbygget databeskyttelse (privacy by design) og databeskyttelse som standardindstillinger (privacy by default) under inddragelse af retningslinjer fra Det Europæiske Databeskyttelsesråd og vejledning fra EU-Kommissionen om apps til støtte for bekæmpelse af COVID-19-pandemien i forbindelse med databeskyttelse.

Dokumentation for begge API'er og den underliggende pseudonymiseringsteknik har været offentliggjort. Dette sikrer, at alle med interesse har mulighed for at se, præcist hvordan koden fungerer.

Sundheds- og Ældreministeriets databeskyttelsesrådgiver har været inddraget i udarbejdelsen af konsekvensanalysen og har fremført en række bemærkninger, som Styrelsen for Patientsikkerhed har forholdt sig til.

På denne baggrund kan ledelsen godkende konsekvensanalysen.

Der vil løbende ske en evaluering af løsningen og ajourføringer af denne konsekvensanalyse.

Denne DPIA offentliggøres.

## 2. BAGGRUND OG FORMÅL

### 2.1 Baggrund

Den igangværende COVID-19-pandemi har skabt en udfordring for Danmark og den øvrige verden, herunder det danske sundhedssystem, vores livsstil, økonomiske stabilitet og værdier. I den nuværende strategi om en gradvis genåbning af Danmark er det efter Styrelsen for Patientsikkerheds vurdering af afgørende betydning, at genåbningen og bekæmpelsen af virussen kan foregå kontrolleret og med understøttelse af relevante digitale teknikker og data.

Styrelsen for Patientsikkerhed (STPS) indgår i det operationelle beredskab med smitsomme sygdomme, og yder rådgivning og bistand til regeringen i forbindelse med den aktuelle pandemi. Som en del af denne opgave har STPS ansvaret for kontaktopsporing.

Styrelsen har i samarbejde med Sundheds- og Ældreministeriets departement og Digitaliseringsstyrelsen udviklet en app – kaldet "Smittestop" – og stiller den til rådighed for danske borgere til brug for kontaktregistrering og smitteopsporing i forbindelse med genåbningen af Danmark og bekæmpelsen af virussen. Styrelsen er samtidig dataansvarlig for den behandling af personoplysninger, der foregår i appen. Tanken er, at bevidsthed hos borgerne om kontakt samt smittekontakt kan gøre afværgeforanstaltninger og sporing mere effektiv. Dataansvaret for appen følger af § 1, stk. 1 i bekendtgørelse nr. 896 af 17. juni 2020 om behandling af oplysninger om elektronisk registrerede kontakter med henblik på at forebygge og inddæmme udbredelsen af Coronavirussygdom 2019 (COVID-19) (herefter "Smittestop-bekendtgørelsen").

Smittestop-appen kan – afhængigt af i hvilket omfang borgerne bruger den – bidrage til at afbryde smittekæder hurtigere og mere effektivt end generelle inddæmningsforanstaltninger og kan mindske risikoen for en betydelig spredning af virussen. Appen kan også bidrage til relevant vejledning af borgerne, om hvordan de skal forholde sig, hvis de er blevet smittet med virussen eller har været i kontakt med smittede.

Smittestop-appen er særlig relevant, når inddæmningsforanstaltningerne ophæves (forsamlingsforbud, nedlukning af institutioner og arbejdspladser m.v.), og risikoen for smitte vokser i takt med, at flere mennesker kommer i kontakt med hinanden i genåbningens faser. Appen er således tænkt som et vigtigt element i genåbningsstrategien og skal supplere andre foranstaltninger såsom manuel kontaktopsporing, øget testkapacitet, informationskampagner m.v.

Appen skal ses som et supplement til den manuelle kontaktopsporing, da appen ikke kan identificere alle typer af kontakter, f.eks. kortvarig fysisk kontakt. Kontaktopsporing gennem elektroniske løsninger har dog en række fordele, som ikke findes ved den manuelle kontaktopsporing:

- Det er muligt at notificere kontakter, som brugeren ikke kender.
- Den kan notificere kontakter, som brugeren kender, men ikke umiddelbart husker.
- Processen er hurtigere, da notifikationen kan ske direkte fra den smittede til kontakterne uden anden menneskelig indblanding.

Hvor den manuelle kontaktopsporing fra sundhedsmyndighedernes side er en koncentreret og målrettet indsats, er appen en bredere indsats, som varetages af borgerne selv.

Regeringen, Venstre, Radikale Venstre, Socialistisk Folkeparti, Enhedslisten, Det Konservative Folkeparti, Liberal Alliance, Alternativet og Susanne Zimmer (UFG) har den 15. maj 2020 indgået en aftale om principper, formål og teknologisk løsning for den danske smitteopsporingsapp.[2]

Sundheds- og Ældreministeriets departement, Digitaliseringsstyrelsen og Styrelsen for Patientsikkerhed har i et tværgående samarbejde påbegyndt udviklingen af appen, der foreløbigt vil blive udviklet til brug for kontaktnotifikation i overensstemmelse med principperne i den ovennævnte politiske aftale. Det er ambitionen, at appen frivilligt vil blive downloadet og anvendt af en stor del af Danmarks befolkning.

Sundheds- og Ældreministeriet og Digitaliseringsstyrelsen har i samarbejde i forbindelse med udvikling af appen nedsat et Advisory Board[3]. Advisory Board'et har bidraget med viden, råd, vurderinger og erfaringer angående udviklingen og ibrugtagning af appen, herunder:

- Sikkerheden i opbevaring og behandling af data
- Beskyttelse af brugernes rettigheder til privatliv
- Teknologiske valg, der bedst muligt understøtter appens formål
- Internationale løsninger og anbefalinger

Advisory Boardet består af fem repræsentanter:

- Camilla Gregersen, formand for Dansk Magisterforening, medlem af Dataetisk Råd
- Christiane Vejlø, CEO Elektronista Media, medlem af Dataetisk Råd
- Sune Lehmann, professor på Institut for Matematik og Computerscience, DTU
- Mikkel Thorup, professor på Institut for Datalogi, KU
- Jacob Herbst, Chief Technical Officer i Dubex, medlem af Cybersikkerhedsrådet

[2] Aftale om frivillig smittesporingsapp for COVID-19, offentliggjort på Sundheds- og Ældreministeriets hjemmeside, www.sum.dk, den 15. maj 2020, https://www.sum.dk/Aktuelt/Nyheder/Coronavirus/2020/Maj/~/media/Filer%20-%20dokumenter/01-corona/App/Politisk-aftale-om-smittessporingsappen.pdf

[3] Bilag 5 – Kommissorium for Advisory Board

Der har løbende under udviklingen af appen været afholdt møder med boardet, hvor væsentlige designbeslutninger er blevet forelagt. Boardets kommentarer til disse beslutninger er indgået løbende i udviklingen af appen og denne DPIA. Der har herudover været afholdt møder med Dataetisk Råd og Cybersikkerhedsrådet om appen.

Når appen tages i brug, skal effekten af den som et værktøj til kontaktopsporing løbende evalueres.

### 2.2 Formålet med konsekvensanalysen

En væsentlig forudsætning for udvikling, accept og udbredelse af Smittestop-appen blandt borgerne er tillid. Borgerne skal have sikkerhed for, at appen overholder de gældende regler om databeskyttelse ved behandling af personoplysninger. Det er derfor vigtigt, at løsningen lever op til et højt informations- og persondatasikkerhedsniveau, og at den involverede behandling af personoplysninger begrænses til det nødvendige. Det skal bl.a. sikres, at appen udelukkende anvendes til specifikke formål, og ikke anvendes til andre formål, herunder f.eks. overvågning. Det skal endvidere sikres, at borgerne bevarer kontrollen over deres egne oplysninger.

Formålet med denne konsekvensanalyse vedrørende databeskyttelse er at beskrive den behandling af personoplysninger, som STPS vil foretage i forbindelse med udbredelsen af Smittestop-appen, og afdække risici forbundet med denne behandling. Analysen skal endvidere bidrage til at afværge, minimere og håndtere disse risici for fysiske personers rettigheder og frihedsrettigheder, som behandlingen af personoplysninger i løsningen medfører. Det sker ved, at analysen vurderer risiciene og fastlægger de rette foranstaltninger til at afhjælpe dem.

Appen er under udvikling og vil blive udviklet i overensstemmelse med reglerne om indbygget databeskyttelse (privacy by design) og databeskyttelse gennem standardindstillinger (privacy by default), jf. databeskyttelsesforordningens artikel 25. Udviklingen sker under inddragelse af bl.a. retningslinjerne fra Det Europæiske Databeskyttelsesråd (EDPB) vedrørende brug af apps til bekæmpelse af COVID-19[4] samt EU-Kommissionens vejledning om apps til støtte for bekæmpelse af COVID-19-pandemien i forbindelse med databeskyttelse.[5]

[4] Det Europæiske Databeskyttelsesråd: Retningslinjer 04/2020 om brug af lokaliseringsdata og kontaktopsporingsredskaber i forbindelse med covid-19- udbruddet, vedtaget den 21. april 2020, tilgængelig her: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_da.pdf

[5] EU-Kommissionen: Vejledning af den 17. april 2020 om apps til støtte for bekæmpelse af covid-19-pandemien i forbindelse med databeskyttelse, tilgængelig her: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)

Formålet med konsekvensanalysen er på den baggrund også at bidrage til at understøtte, at de nødvendige og relevante databeskyttelsesretlige krav tænkes ind i appen ved dens udvikling.

Konsekvensanalysen skal således samlet set bidrage til at sikre overholdelse af reglerne om databeskyttelse, ligesom den er en væsentlig forudsætning for overholdelse af forordningens grundlæggende princip om ansvarlighed, jf. forordningens artikel 5, stk. 2, og artikel 24. Konsekvensanalysen omfatter endvidere en beskrivelse af overholdelse af reglerne om samtykke til lagring af og adgang til oplysninger på brugernes mobile enheder efter cookiebekendtgørelsens § 3[6], som implementerer e-databeskyttelsesdirektivets[7] artikel 5, stk. 3.

### 2.3 Afgrænsning af konsekvensanalysen

Smittestop-appen vil muligvis blive gjort tilgængelig for borgerne i flere trin (kaldet "releases" i det følgende). Der er foreløbigt planlagt en release, hvori appen kan bidrage til smitteopsporing blandt de borgere, der benytter appen.

Det overvejes, at appens funktioner senere suppleres med en yderligere release 2, hvor borgeren kan vælge frivilligt at videregive oplysninger om kontaktantal til sundhedsmyndighederne i aggregeret form. Release 2 er ikke omfattet af denne konsekvensanalyse, og der vil således ske en forudgående ajourføring af konsekvensanalysen, hvis appen vil blive suppleret med release 2 eller øvrige ændringer.

STPS har vurderet, at STPS som dataansvarlig for Smittestop-appen har pligt til at udarbejde en konsekvensanalyse vedrørende databeskyttelse for release 1 henset navnlig til, at der er tale om ny teknologi, hvor der vil ske behandling af personoplysninger, herunder helbredsoplysninger i form af oplysninger om konstateret smitte med COVID-19, samt det forventede store antal brugere af appen.

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

[7] 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.

## 3. PROCESSEN FOR GENNEMFØRELSEN AF KONSEKVENSANALYSEN

### 3.1 Metode

Databeskyttelsesforordningen fastsætter følgende minimumskrav til konsekvensanalysens indhold, jf. forordningens artikel 35, stk. 7:

a) En systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige.
b) En vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene.
c) En vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder.
d) De foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af databeskyttelsesforordningen, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

Der fremgår endvidere en række kriterier for en acceptabel konsekvensanalyse i bilag 2 til Artikel 29-Gruppens (nu: Det Europæiske Databeskyttelsesråd) vejledning om konsekvensanalyser.[8] Nærværende konsekvensanalyse er udarbejdet i overensstemmelse med disse krav.

Databeskyttelsesforordningen fastsætter ikke i detaljer, hvilken procedure for udarbejdelse af konsekvensanalysen den dataansvarlige skal følge. Udarbejdelsen af nærværende konsekvensanalyse er navnlig sket under anvendelse af den metode, der fremgår af den internationale standard for udarbejdelse af konsekvensanalyser vedrørende databeskyttelse, ISO/IEC DIS 29134[9], med nødvendige tilpasninger af hensyn til sagens karakter.

I forbindelse med udarbejdelsen af denne konsekvensanalyse har der fra STPS deltaget en række centrale aktører for at sikre den fornødne beskrivelse af behandlingen samt identifikation og håndtering af risici. Det gælder navnlig repræsentanter fra Styrelsen for Patientsikkerhed, Sundheds- og Ældreministeriets departement, systemleverandøren Digitaliseringsstyrelsen samt udviklings- og driftsleverandørerne Netcompany og Trifork:

[8] Artikel 29-Gruppen (nu Det Europæiske Databeskyttelsesråd, herefter forkortet "EDPB"): Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, WP 248, rev. 01, revideret og endeligt vedtaget den 4. oktober 2017

[9] ISO/IEC DIS 29134, "*Information technology – Security techniques – Privacy impact assesment – Guidelines*", first edition 2017-06

- Systemudviklere og driftsleverandører har bistået med tekniske dokumentation samt beskrivelse af dataflows.
- Samtlige aktører har deltaget i møder i forbindelse med input til risikovurderingen.
- Sundheds- og Ældreministeriet har i samarbejde med STPS udarbejdet bekendtgørelsen.
- Sikkerhedsfirmaet FortConsult har foretaget en sikkerhedstest af hele løsningen, og deres fund er indgået i den tekniske risikovurdering.
- Artikler, nyheder og rapporter om andre landes erfaringer har løbende været inddraget.

Derudover har databeskyttelsesrådgiveren været inddraget i processen, ligesom Kammeradvokaten har bistået STPS med udarbejdelsen af konsekvensanalysen. Der har endvidere i forløbet været afholdt møder med Datatilsynet, Dataetisk Råd og Cybersikkerhedsrådet om udviklingen af appen.

### 3.2 Inddragelse af de registrerede og information af offentligheden om appen

STPS har vurderet, at det ikke er relevant at indhente de registreredes eller deres repræsentanters synspunkter vedrørende den planlagte behandling forud for behandlingen, jf. databeskyttelsesforordningens artikel 35, stk. 9.

STPS har herved lagt vægt på, at behandlingen af de omfattede personoplysninger i Smittestop-appen er hastende henset til den vigtige samfundsmæssige interesse i en fortsat genåbning af Danmark. Hertil kommer, at det er frivilligt for borgerne, om de ønsker at downloade Smittestop-appen til deres smartphones. STPS vil endvidere informere borgerne bredt om behandlingen af personoplysningerne i Smittestop-appen, forinden behandling af personoplysningerne finder sted.

Det har dog alligevel være muligt at indhente synspunkter fra en række af de registreredes interessenter. Dette er primært sket gennem nedsættelse af et Advisory Board bestående af medlemmer fra Dataetisk Råd, Cybersikkerhedsrådet, DTU og Københavns Universitet. Der har løbende under udviklingen af appen været afholdt møder med Advisory Boardet, hvor væsentlige designbeslutninger er blevet forelagt. Boardets kommentarer til disse beslutninger er indgået i den videre udvikling.

Derudover har beslutningen om, at der skulle udvikles en app, været kendt af offentligheden siden påbegyndelsen af udviklingen. Dette har betydet, at der har været bred offentlig og politisk interesse for, hvordan den endelige løsning kommer til at se ud. De synspunkter og bekymringer, der har været fremhævet i den offentlige debat, at indgået som en del af overvejelserne i udviklingen.

Til understøttelse af den løbende evaluering af appen vil STPS inddrage faglig ekspertise fra Statens Serum Institut og Sundhedsstyrelsen. Samtidig vil der løbende modtages feedback om de erfaringer, brugerne gør sig gennem App Store/Google Play og gennem den offentlige debat.

I forbindelse med den stigende interesse for brugen af apps til smitteopsporing udgav Det Europæiske Databeskyttelsesråd en række anbefalinger[10]. En af disse anbefalinger er, at kildekoden til appen bør offentliggøres for at sikre gennemsigtighed og tilskynde offentligheden til test og forbedring.

Kildekoden til den del af appen, som STPS har fået udviklet, offentliggøres ikke. Dette skyldes, at STPS vurderer, at der kan være sikkerhedsrisici forbundet med en sådan offentliggørelse. STPS har vurderet, at disse risici vejer tungere end hensynet til offentliggørelse. Dog er dokumentationen for det underliggende API, der bruges til kontaktregistreringen i appen udviklet af Apple og Google, offentliggjort og er tilgængeligt for offentligheden.

## 4. BESKRIVELSE AF DEN PLANLAGTE BEHANDLINGS FORMÅL, KARAKTER, OMFANG OG SAMMENHÆNG

### 4.1 Formål med Smittestop-appen og centrale forudsætninger for dens anvendelse

Løsningens overordnede formål er at forebygge og hindre udbredelse og smitte af Coronavirussygdom 2019 (COVID-19). Løsningen har i den forbindelse til formål at bidrage til at bryde smittekæder ved at give mulighed for, at brugere af løsningen kan få elektronisk meddelelse om, at de har været i elektronisk kontakt med andre brugere af løsningen, der er bekræftet smittet med Coronavirussygdom 2019 (COVID-19), og dermed er i risiko for at være blive smittet med Coronavirussygdom 2019 (COVID-19). Der henvises herved til § 1, stk. 2, i Smittestop-bekendtgørelsen.

Formålet med appen er kontaktopsporing, hvor appen skal fungere som et digitalt supplement til manuel kontaktopsporing. Appen skal give borgeren mulighed for nemt at give besked til personer, som brugeren har været i kontakt med, hvis brugeren får COVID-19. Tilsvarende vil brugeren selv få besked, hvis brugeren har været i kontakt med en person, der konstateres smittet. På den måde kan borgeren hurtigt tage de anbefalede forholdsregler, herunder selvisolation og test, og dermed hjælpe med at mindske smittespredningen og stoppe smittekæder. Til forskel fra manuel smitteopsporing giver appen mulighed for at give besked om risiko for smitte til personer, som en smittet bruger har været tæt på, men som den smittede bruger ikke kender, f.eks. i offentlig transport.[11]

[10] Det Europæiske Databeskyttelsesråd: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, af 21. april 2020, s. 14

[11] Faktaark – appen smitte|stop, offentliggjort på Sundheds- og Ældreministeriets hjemmeside, www.sum.dk, den 15. maj 2020, https://www.sum.dk/Aktuelt/Nyheder/Coronavirus/2020/Maj/~/media/Filer%20-%20dokumenter/01-corona/App/Faktaark-smitte-stop.pdf

Det er derimod ikke formålet med Smittestop-appen, at den skal tjene som en klinisk app til brug for (selv)diagnosticering af smitte, og den skal således ikke indeholde muligheder for selvrapportering af symptomer til brug for selvvurdering af egen sygdom eller lignende. Appen skal heller ikke bruges til telemedicin, dvs. som et kommunikationsforum mellem patienter og læger eller for yderligere diagnosticerings- og behandlingsrådgivning.

I henhold til den politiske aftale af 15. maj 2020 skal Smittestop-appen udvikles på grundlag af følgende principper privatlivsbeskyttelse, datasikkerhed og frivillighed m.v.:

1. Appen er baseret på frivillighed
2. Brugervenlighed og værdi for borgerne skal sikre kritisk masse
3. Data om borgeres kontakter skal *alene* opbevares decentralt på borgerens egen mobiltelefon – ikke på central server – og data slettes efter 14 dage
4. Myndighederne har ikke adgang til personhenførbare data om borgerens kontakter
5. Appen følger gældende lovgivning og skal leve op til krav om privacy og sikkerhed
6. Appen lukkes ned og alle data slettes, når appen ikke længere er aktuel at bruge i forbindelse med COVID-19
7. Muligheden for at anvende appen på tværs af grænser undersøges i samarbejde med EU-lande, så appen om muligt kan understøtte interoperabilitet.

Der er i Smittestop-bekendtgørelsens kapitel 1 fastsat regler om formålsbegrænsning og generelle betingelser for brugen af appen.

Anvendelse af løsningen er frivillig, hvorved forstås, *at* den enkelte borger ikke kan pålægges at benytte løsningen, *at* borgere, der vælger ikke at benytte løsningen, ikke af den grund kan udsættes for forskelsbehandling fra myndighedernes side, *at* lagring af oplysninger på brugerens telefon er betinget af samtykke og modtagelse af specifik information om behandlingen af personoplysninger i løsningen, *at* oplysninger om elektroniske kontakter ikke kan tjene som grundlag for påbud overfor registrerede brugere eller andre, samt *at* den enkelte bruger altid har mulighed for at ophøre med at anvende løsningen.

Som beskrevet ovenfor i afsnit 2.3 overvejes det, at appens funktioner senere suppleres med en yderligere release 2, hvor borgeren kan vælge frivilligt at videregive oplysninger om kontaktantal til sundhedsmyndighederne i aggregeret form. Formålet med dette er at give mulighed for bedre at evaluere appens effekt og give sundhedsmyndighederne viden om smittedes kontaktantal til brug for planlægning af testkapacitet og til beslutningsgrundlaget om genåbning af Danmark. Af den politiske aftale af 15. maj 2020 fremgår herom følgende på s. 2:

> *"Kontaktdata til myndighederne som tilvalg*

*Data fra appen kan give vigtig viden om smittespredning til brug for planlægning af testkapacitet og til beslutningsgrundlaget om genåbning af Danmark.*

*Partierne er derfor enige om, at appen udvikles med en tilvalgsmodel, så man som borger i appen kan vælge til, om man ønsker, at kontaktregistreringer alene anonymt og aggregeret kan videregives til at tælle med i datagrundlaget til myndighederne, og appen vil derefter også opfylde dette yderligere formål.*

*Det skal være tydeligt for borgeren i appen, når de benytter tilvalgsmodellen som supplement til smittesporing. Det skal være tydeligt til hvilke formål borgere vælger at dele deres kontaktdata anonymt og aggregeret med myndighederne, og data vil blive opbevaret af myndighederne i kortest mulig tid henset til formålet. Ligeledes skal det være gennemsigtigt for borgerne, hvilke data de deler, og hvem der får adgang til data."*

Denne funktionalitet er dog ikke udviklet på nuværende tidspunkt, ligesom eventuel behandling af personoplysninger forbundet hermed ikke er omfattet af denne konsekvensanalyse.

### 4.2 Dataansvar og behandling af personoplysninger i Smittestop-appen

STPS er i medfør af Smittestop-bekendtgørelsen blevet pålagt at stille Smittestop-appen til rådighed for befolkningen. Det fremgår endvidere af bekendtgørelsens § 1, stk. 1, 2. pkt., at STPS er dataansvarlig for den behandling af personoplysninger, der er beskrevet i bekendtgørelsen. Det er herefter STPS, der træffer beslutning om og er ansvarlig for alle væsentlige forhold i forbindelse med udvikling og drift af appen, herunder dens design, implementering af fornødne sikkerhedsforanstaltninger, og hvordan integrationer til andre registre skal udformes m.v. i overensstemmelse med de grundlæggende behandlingsprincipper og reglerne om indbygget databeskyttelse og databeskyttelse som standardindstillinger, således at reglerne i databeskyttelsesforordningen og -loven samt i Smittestop-bekendtgørelsen overholdes.

Det fremgår af Smittestop-bekendtgørelsens § 3, stk. 1, at der registreres oplysninger på den telefon, den enkelte borger har installeret appen på, i form af antal elektroniske kontakter den enkelte borger har haft i de forgangne 14 døgn, og smittenotifikationer modtaget de forgangne 14 døgn. STPS kan alene behandle disse personoplysninger til brug for brugernes egen smitteopsporing, jf. bekendtgørelsens § 1, stk. 4. Smittestop-appen indsamler ikke oplysninger om brugernes lokalitet. Smittestop-appen registrerer kun elektroniske kontakter mellem telefoner, der har appen installeret.

Ved elektroniske kontakter forstås registrerede kontakter på baggrund af Bluetooth-kontakt mellem to telefoner, hvor løsningen er installeret. Kontaktregistreringen indeholder oplysning om kontaktens aktuelle skiftende systemgenererede elektroniske nøgle, signalstyrke, varighed og tidspunkt og opbevares

på brugerens telefon, jf. bekendtgørelsens § 3, stk. 1. Kontaktregistreringen foregår nærmere bestemt via Bluetooth-teknologi. Løsningen registrerer alle kontakter, hvor der mellem to telefoner, hvor løsningen er installeret, er uafbrudt Bluetooth-kontakt over en kort periode. Løsningen registrerer forbindelsesstyrken, varigheden af kontakten og tidsstempel for kontakten.

Personoplysningerne i forbindelse med denne kontaktregistrering lagres alene lokalt på brugerens telefon – STPS lagrer med andre ord ikke oplysningerne på en central server (backend) – og den teknologiske løsning er således baseret på decentral kontaktregistrering, hvor brugerens kontakter kun gemmes på telefonen, og hvor matchingen mellem kontakter og smittede også sker decentralt (på brugerens telefon). Det er ikke muligt for STPS at tilgå oplysningerne på brugernes telefoner, da dette ikke er en funktion, der er indbygget i API'et. Det er muligt for brugeren at afsende, modtage og læse smittenotifikationer.

På telefonen foretages samtidig den beregning af risiko for smitte, som bruges til at give brugeren besked om, at vedkommende har været i kontakt med en smittet. Beregningen foretages ud fra oplysninger om registrerede kontakter (varighed, signalstyrke og tidspunkt samt tidspunktet for, hvornår kontakten fandt sted i relation til, hvornår den smittede havde symptomdebut) sammenholdt med listen over smittede ID'er. Det er muligt for STPS at ændre på kriterierne i beregningen, men det er ikke muligt for STPS at se resultatet af den beregning, der foregår på den enkelte brugers telefon.

Den decentrale løsning rejser nogle udfordringer i forhold til STPS' dataansvar for disse oplysninger i form af kontaktregistreringer på brugernes telefoner, idet STPS ikke kan tilgå oplysningerne. Det er således alene brugeren, der kan give og modtage smittenotifikationer ved kontaktregistreringer, men det er STPS, der beslutter formålet og hjælpemidlerne med behandlingen. Samtidig er sletningen af data på telefonen fastlagt af API'et. Dette fører til en situation, hvor STPS er dataansvarlig for den behandling, der foregår på samtlige brugeres telefoner, men hvor STPS ikke har adgang til oplysningerne. Der kan derfor rejses spørgsmål om rækkevidden af STPS' dataansvar for så vidt angår behandlingen af personoplysninger i appen decentralt på brugernes telefoner. STPS har dog ud fra hensynet til de registrerede valgt at udstrække dataansvaret så langt som muligt.

Det er ikke muligt for STPS at håndtere brugernes eventuelle anmodninger om at udøve deres rettigheder i form af f.eks. anmodninger om indsigt i eller sletning af oplysninger lagret på telefonen. På grund af den måde, API'et er indrettet på, er det heller ikke muligt at give den enkelte bruger indsigt i oplysninger, der lagres på brugerens telefon. Begrundelsen for dette er, at API'et er designet på en måde, der sikrer maksimal privatlivsbeskyttelse, og at det dermed ikke er muligt at få adgang til de data, der ligger på telefonen. Hvis det skulle være muligt for brugerne at få indsigt i oplysningerne, ville dette kræve, at dele at løsningen blev låst op i strid med den måde, API'et er designet på. Så ved at give muligheden for indsigt, ville det ske på bekostning af den indbyggede beskyttelse, som API'et er designet til at give. Dette ville også kunne medføre, at myndigheder eller andre også ville kunne tilgå data.

Brugeren har selv mulighed for at udøve retten til sletning af de oplysninger, der ligger på brugerens telefon. Dette kan gøres af brugeren ved enten at trække samtykket til lagring af oplysninger tilbage eller ved at slette appen. Det kan også gøres ved, at brugeren manuelt sletter nøglerne for telefonen, men dette vil dog kræve lidt teknisk indsigt. STPS har ikke mulighed for at slette data på brugerens telefon, men API'et er opsat sådan, at allerede registrerede data slettes løbende efter 14 dage.

STPS er dataansvarlig for løsningens centrale behandlingsaktiviteter i forbindelse med smitteverifikation og -notifikation, når personoplysninger transporteres til og fra appen samt lagres centralt hos STPS, jf. nærmere nedenfor vedrørende bekendtgørelsens § 4. STPS er endvidere dataansvarlig for at iagttage reglerne om brud på persondatasikkerheden, for så vidt der er tale om et brud, der vedrører centrale behandlingsaktiviteter. STPS har imidlertid ikke mulighed for at håndtere eventuelle sikkerhedsbrud ved brugerens tab af telefonen, f.eks. ved tyveri, eller hvis brugerne giver uvedkommende adgang til deres app eller installerer programmer på deres telefon, der måtte give uvedkommende adgang til oplysningerne.

Det fremgår af Smittestop-bekendtgørelsens § 4, stk. 1, at STPS, i det omfang det er nødvendigt for at sikre driften af Smittestop-appen, behandler personoplysninger om brugerens NemID-oplysninger (PID-nummer og NemID-certifikat) i forbindelse med verifikation af, om brugeren har COVID-19. STPS behandler også personoplysninger om borgere, der har COVID-19 til brug for smitteverifikation og -notifikation, herunder CPR-nummer, smittestatus, tidspunkt for test, tidspunkt for symptomdebut (oplyst af brugeren eller beregnet af løsningen) og antal smitteverifikationer foretaget af den enkelte bruger inden for de seneste 24 timer. Styrelsen for Patientsikkerhed kan alene behandle brugerens NemID-oplysninger i forbindelse med verifikation af, om brugeren har Coronavirussygdom 2019 (COVID-19). Brugerens helbredsoplysninger må alene behandles til at informere andre brugere om potentiel smittefare, jf. bekendtgørelsens § 4, stk. 4, nr. 3.

Efter bekendtgørelsens § 4, stk. 2, videregiver Statens Serum Institut (SSI) efter fastlagte intervaller til STPS et dataudtræk over personer, der aktuelt er bekræftet smittet med Coronavirussygdom 2019 (COVID-19) med oplysninger om CPR-nummer, smittestatus, tidspunkt for test og beregnet tidspunkt for symptomdebut.

SSI videregiver oplysningerne fra SSI's database benævnt Key to Infectious Diseases (herefter "KID"). KID bygger på oplysninger fra Mikrobiologisk Bank (herefter "MiBA")[12], hvor oplysninger om testresul-

[12] SSI modtager oplysningerne fra laboratorierne, der foretager testen, jf. § 1 i bekendtgørelse nr. 665 af 20. maj 2020 om anmeldelse af COVID-19

tater fra gennemførte COVID-19-tests registreres. KID indeholder således valide oplysninger om, hvorvidt borgerne er smittet med COVID-19, da oplysningerne bygger på konstaterede smittetilfælde ud fra en lægefaglig vurdering og test. Det er SSI, der driver og er dataansvarlig for behandlingen af personoplysninger i KID. Videregivelsen af oplysningerne fra SSI til STPS vil ske gennem Sundhedsdatastyrelsen (herefter "SDS"), der vil stå for integrationen mellem KID og appen. De oplysninger, der modtages fra KID, opbevares af STPS på en server hostet af en underdatabehandler til Sundhedsdatastyrelsen.

De ID'er, som benyttes til kontaktregistrering, oprettes på baggrund af den kryptografiske protokol, som er udviklet af Apple og Google som en del af API'et. ID'erne genereres ud fra en blanding af forskellige parametre, såsom et tidsstempel og et tilfældigt genereret tal, og er sikret med en hash-funktion og AES-kryptering[13]. Protokollen har været offentliggjort med henblik på at sikre transparens i teknologien og give mulighed for review af, at der er tale om en kryptografisk sikker metode.

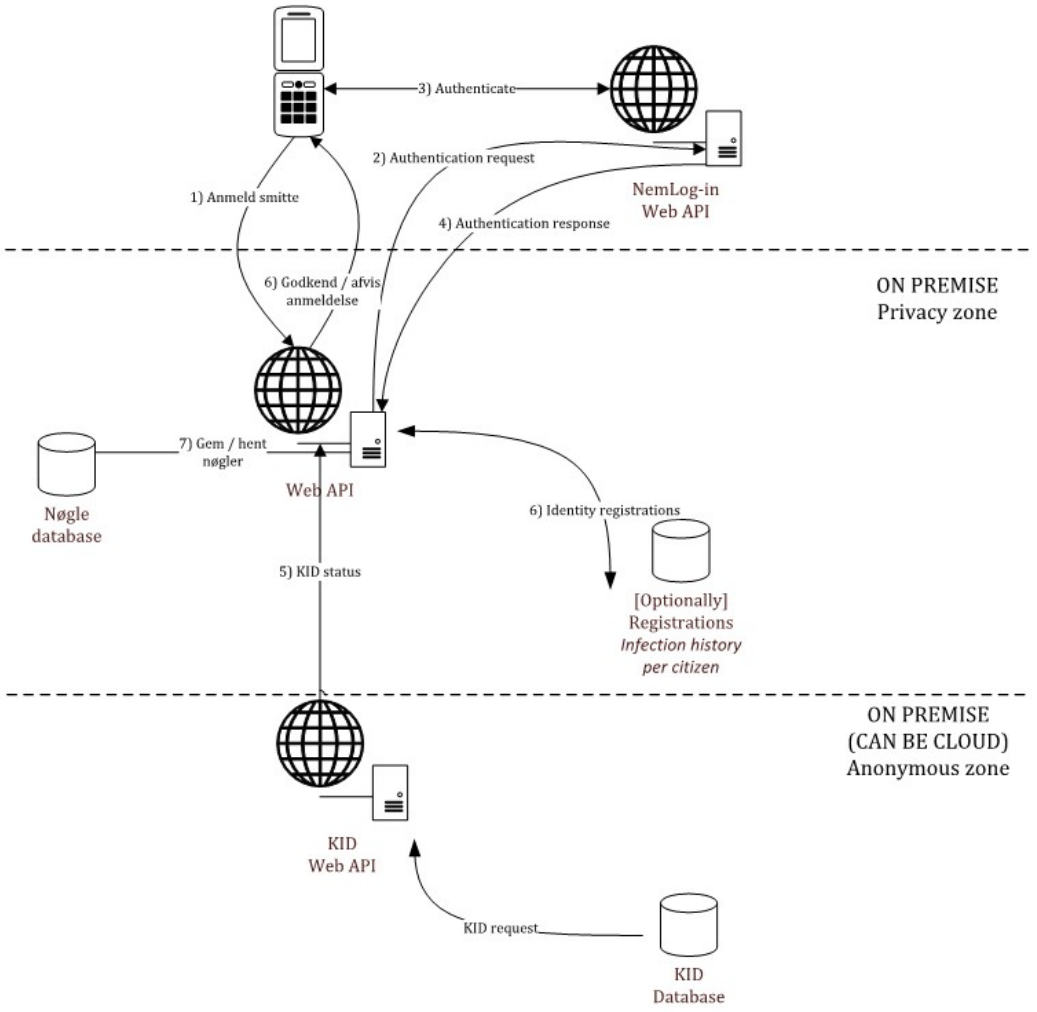
### *4.2.1 Udsendelse af smittenotifikation*

Hvis en bruger bliver smittet, har vedkommende mulighed for at udsende en notifikation til andre brugerem, som vedkommende har være i kontakt med. Når en bruger ønsker at udsende en smittenotifikation, skal vedkommende logge ind med NemID. Dette sker på en browserside. Når brugerens NemID-oplysninger og kode er bekræftet af serveren, foretages der en opslag i udtrækket over smittede. Hvis personen findes på listen over aktuelt smittede, udsteder serveren et "token" til appen. Dette benytter appen til at aktivere udsendelsen af de seneste 14 dages rullende systemgerende ID'er, som er lagret på telefonen. Disse nøgler uploades til en central server, som samler alle de indberettede nøgler, og andre brugeres apps rekvirerer en samlet liste fra serveren.

De øvrige brugere bliver således ikke notificeret direkte af den smittede, men gennem den centrale server.

**Figur 1 - flow for udsendelse af notifikation**

[13] Specifikationen kan findes i Exposure Notification - Cryptography Specification v1.2 (https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf, senest tilgået 11.06.20)



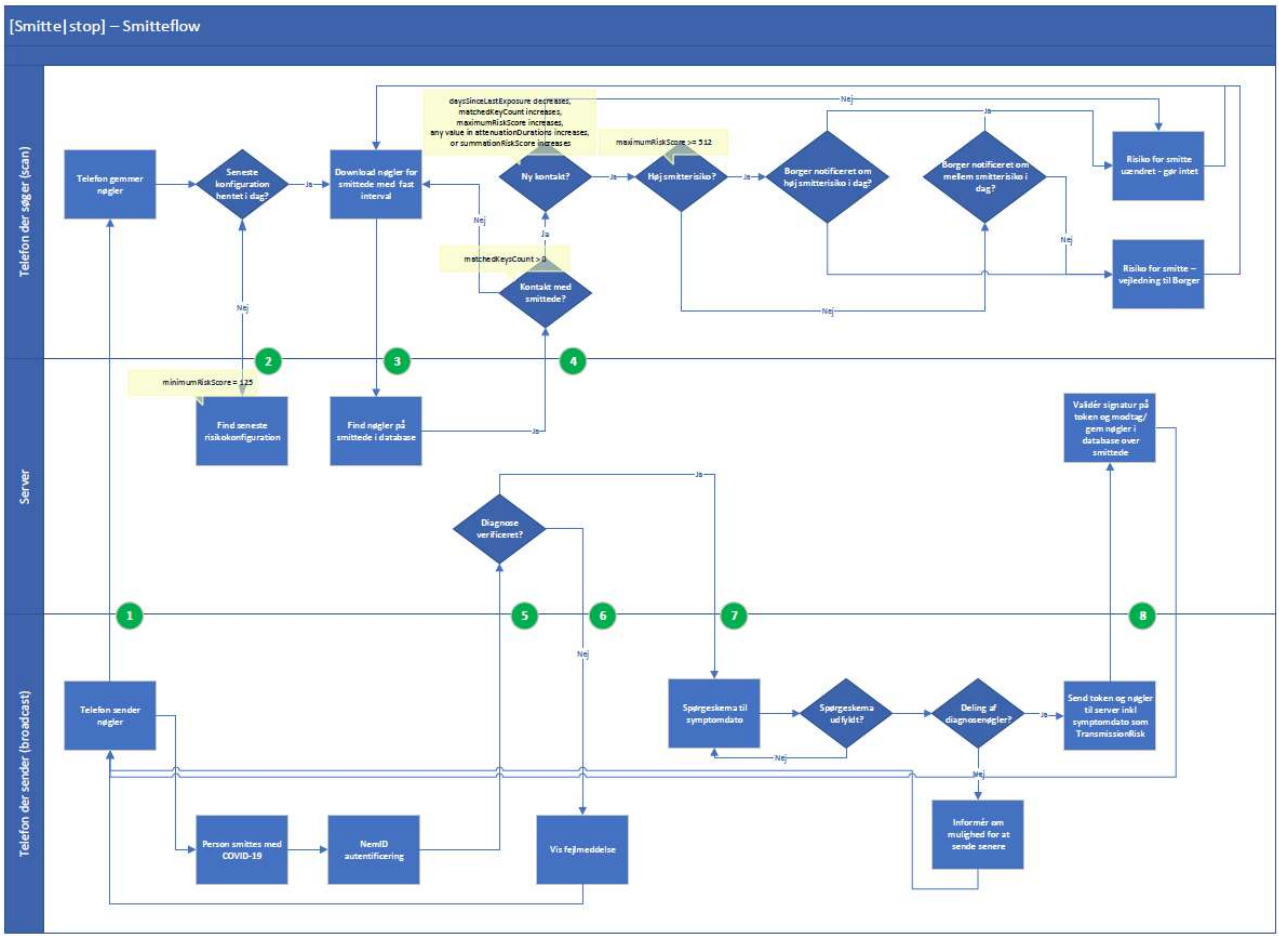

### *4.2.2 Registrering af kontakter og beregning af risiko for smitte*

Når appen anvendes, samles der løbende oplysninger på brugerens telefon om kontakter med andre brugere af appen gennem Bluetooth-kontakt. Alle kontakter med uafbrudt Bluetooth-kontakt over en kort periode registreres på telefonen sammen med oplysninger om tidspunkt, varighed og signalstyrkeværdier. Hvis en kontakt overlapper det tidspunkt, hvor kontaktens rullende ID opdateres, vil dette registreres som en ny kontakt. Varigheden af en kontakt vil derfor ikke kunne overskride 20 minutter, da dette

er det maksimale interval for opdatering af ID'et. Efterfølgende registrering vil oprettes som en ny kontakt.

Når en bruger melder sig smittet, uploades samtlige af brugerens ID'er for de sidste 14 dage til den centrale server, og de enkelte apps henter listen fra serveren. Hvis en brugers app finder et match mellem de ID'er, der er registreret på telefonen, og et ID, der fremgår på listen over smittede, foretager appen en beregning af smitterisikoen. I beregningen indgår varigheden af kontakten, signalstyrken, tiden siden kontakten og tidspunktet for den smittedes symptomdebut. Hvis resultatet af beregningen overskrider en given værdi, modtager brugeren en besked om, at brugeren har været udsat for en risiko for smitte og bør følge myndighedernes anvisninger om hensigtsmæssig adfærd.

**Figur 2 – Kontaktregistrering (Bilag 2)**



## 4.3 Borgernes brug af appen

### *4.3.1 Borgeren ønsker at give smittenotifikation*

Den enkelte borger, der er smittet med virussen, kan i Smittestop-appen frivilligt vælge at *give* besked til borgerens kontakter om, at borgeren er smittet og dermed har udgjort en smitterisiko for de pågældende kontakter (smittenotifikation). Borgeren skal i så fald gå ind i appen og godkende, at der sendes en besked til de app-brugere, som borgeren har været i kontakt med de seneste 14 dage.

I Smittestop-appen vil der således – hvis den enkelte borger ønsker det – blive behandlet personhenførbare helbredsoplysninger i form af borgerens status som smittet med COVID-19 i appen.

Funktionaliteten fungerer således, at borgeren, hvis denne testes positiv for COVID-19, kan vælge at udsende en smittenotifikation. Dette gøres ved at logge ind med NemID, for at foretage en validering af, at brugeren er smittet med COVID-19. Når appen har modtaget en bekræftelse på, at borgeren er smittet, vil appen sende brugerens systemgenerede rullende ID'er for de sidste 14 dage til den centrale database. Disse ID'er tilføjes en samlet liste på den centrale database, og alle apps henter listen fra serveren. Oplysningen om borgerens smittestatus gemmes ikke i appen, og der gives alene en tilladelse til, at appen kan uploade de rullende ID'er.

Funktionaliteten forudsætter som nævnt ovenfor, at borgeren logger ind med NemID for at understøtte den fornødne sikre identifikation af borgeren, samt at der foretages en validering af, at brugeren er smittet. Brugere kan logge ind med alle tilgængelige NemID-løsninger som nøglekort og NemID-app.

For at kunne notificere andre brugere om smittestatus vil brugeren skulle logge ind med NemID, hvilket medfører, at det kun er borgere over 15 år, der kan logge ind og anvende denne funktionalitet. Dette betyder, at borgere, der ikke har NemID, ikke kan anvende denne funktionalitet i Smittestop-appen. Fælles for disse grupper er dog, at de vil kunne bruge kontaktregistreringsfunktionaliteten, og dermed kan modtage notifikationer om, at de har været i kontakt med en person, der er bekræftet smittet med COVID-19. Disse begrænsninger i, hvilke borgere der kan melde sig smittet via Smittestop-appen og dermed sende notifikationer til andre borgere, følger naturligt af, at STPS har valgt, at smitten skal verificeres mod officielle oplysninger om smittestatus, før det er muligt at sende en notifikation til andre brugere. STPS har valgt, at smitten skal verificeres, da det er centralt, at borgeren kan stole på appen, og på at de kun modtager en notifikation om en mulig smitterisiko, når denne risiko faktisk er reel.

### *4.3.2 Brugeren ønsker at modtage smittenotifikation*

Den enkelte bruger vil også i Smittestop-appen *få* besked, hvis de har været i kontakt med en anden bruger, der er blevet smittet med COVID-19 og dermed kan have udgjort en smitterisiko for brugeren selv. Før en bruger modtager en besked, kræver det, at en anden bruger, der har været i kontakt med den pågældende, har udsendt en smittenotifikation. Hvis dette er tilfældet, foretager appen en beregning af, om kontakten udgør en risiko. Beregningen er baseret på varigheden af kontakten, afstanden (baseret på signalstyrken) til kontakten og hvor lang tid siden mødet fandt sted i forhold til kontaktens symptom-debut.

Hvis resultatet af beregningen overstiger en vis værdi, vil borgeren få besked om, at denne har været i tæt kontakt med en person, der er bekræftet smittet med COVID-19. I notifikationen er en besked om, at borgeren har været i nærheden af en person, der er smittet, og der vil være et link til hjemmesiden www.smittestop.dk, hvor borgeren kan læse mere om, hvordan borgeren bør forholde sig. Borgeren får ikke oplysninger om, hvor eller hvornår borgeren har været i kontakt med en person, der er bekræftet smitte og får heller ikke oplysninger om, hvem der har udsendt notifikationen.

Modtagelse af smittenotifikation er en grundfunktionalitet i appen, og er en del af appens primære formål, og det er er derfor ikke muligt at fravælge denne del, når appen er installeret og tændt. Brugeren kan vælge at slå kontaktregistrering fra, hvorefter der ikke vil være registrerede kontakter at modtage notifikation på baggrund af. Brugeren kan også vælge helt at afinstallere appen.

Udsendelse af smittenotifikation er frivillig, og borgeren kan således godt få besked, hvis en af de kontakter, borgeren har haft, er blevet smittet med COVID-19, selv om brugeren ikke selv vælger at dele oplysninger om sin egen smitte med registrerede kontakter.

Målgruppen for Smittestop-appen er den danske befolkning i bred forstand. Smittestop-appen vil blive gjort tilgængelig for download i App Store for borgere med iPhones og i Google Play for borgere med Android-telefoner. Det vil ikke være muligt for STPS at kontrollere, hvilke dele af befolkningen der downloader og tilgår appen, herunder om f.eks. børn downloader og tilgår appen, da det ikke gennem App Store/Google Play, hvor løsningen stilles til rådighed, er muligt at verificere brugerens alder. Det har været overvejet, om en bruger skulle logge ind med NemID inden appen kunne bruges for at verificere, at vedkommende er 15 år. Dette ville dog medføre en betydelig større behandling af personoplysninger, og det ekstra login kunne hindre brugere i at benytte appen og ville bryde med den grundlæggende privatlivsbeskyttelse i den decentrale model. Derfor blev dette ikke implementeret.

For at kunne notificere andre brugere om smittestatus vil brugerne skulle logge ind med NemID, hvilket medfører, at det kun er borgere over 15 år, der kan logge ind og anvende denne funktionalitet. Det er

overvejet, om det skal være muligt for forældre at kunne gives deres børn samtykke gennem NemID til at foretage smittenotifikation. Dette er ikke implementeret, da der er et forholdsvist lille antal af børn under 15, der er smittet med COVID-19. Det er dog muligt, at funktionen på et senere tidspunkt implementeres, hvis det i forbindelse med den løbende evaluering viser sig at være relevant. I så fald opdateres konsekvensanalyse før eventuel implementering.

## 5. VURDERING AF NØDVENDIGHEDEN OG PROPORTIONALITETEN

Det er helt essentielt, at løsningen som helhed, og den behandling af personoplysninger, som den indebærer, er proportional og nødvendig af hensyn til de formål, der forfølges. Heri ligger også, at løsningen skal være egnet til at opnå disse formål. Den globale pandemi har medført en stor trussel mod folkesundheden, og denne trussel har krævet ofte meget indgribende foranstaltninger. I Danmark har vi blandt andet måtte indføre opholdsforbud, hjemmearbejde og forbud mod at samles flere mennesker sammen. Disse indgreb har været begrundet i sundhedsfaglige vurderinger af, hvordan smittespredningen bedst begrænses.

Appen er et værktøj, der medfører et indgreb i de registreredes rettigheder til selv at have kontrol over, hvem der har adgang til deres personoplysninger, og til hvilke formål de kan benyttes. Det er derfor vigtigt at foretage en vurdering af, om de indgreb, som de registrerede må lide, også står til mål med det overordnede formål, der forfølges med løsningen.

Mange EU/EØS-lande er i gang med at udvikle apps til smittesporing. Få apps er allerede udgivet. En af de første var lande til at udgive en app var Norges Folkehelseinstitut. Den norske app har været genstand for stor offentlig diskussion i forhold til appens behandling af personoplysninger. Det er derfor naturligt, at Norges erfaringer med en app, også har indgået i vores tilrettelægning af løsningen.

Senest har det norske Datatilsyn udstedt et midlertidigt forbud mod at behandle oplysninger den norske Folkehelseinstituts app "Smittestopp"[14]. Forbuddet var begrundet i, at appen udgjorde meget stort indgreb, og at dette indgreb ikke var forholdsmæssigt i forhold til det overordnede mål og den samlede effekt af appen. Helsetilsynet havde ikke godt nok dokumenteret, at kravene til proportionalitet var opfyldt.

Den norske løsning er dog ikke direkte sammenlignelig med den danske, da den norske er 1) baseret på en central løsning og 2) indsamler GPS-oplysninger fra borgerne. Ved ikke at benytte lokationsdata og ved at basere løsningen på en decentral model, er der skåret betydeligt ned på de risici, der er for de registrerede. Disse er designvalg, Styrelsen for Patientsikkerhed har truffet, for at sikre, at løsningen udgør et mindre indgreb for brugerne.

[14] https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/midlertidig-stans-av-appen-smittestopp/

Appen har som tidligere beskrevet til formål at understøtte og supplere Styrelsen for Patientsikkerheds smitteopsporing. Baggrunden for selve smitteopsporing er at sikre at personer, der har potentielt har været udsat for smitte, bliver informeret om dette, og selv kan tage forholdsregler. Dette skal både gøre dem mere opmærksomme på symptomer, og undgå at potentielt smittede ikke smitter andre. Et studie om digitale sporingsapps fra Oxford University[15] har vist, at hvis 60% af en befolkning benytter en digital sporingsapp, kan dette være med til helt at stoppe en epidemi uden andre hjælpemidler. Studiet viser også, at digitale sporingsapps kan bidrage til at mindske smittespredningen også selv om kun få procent benytter den. Effekten bliver dog større, jo flere der benytter den, men det er ikke en forudsætning, at er opnås 60% udbredelse, særligt ikke når appen er en del af en bredere indsats.

Effektiviteten af appen og realiseringen af dens formål – samt den dermed forbundne behandling af personoplysninger – er afhængig af, at appen opnår en sådan udbredelse blandt borgerne, at der kan ske brud på smittekæder gennemt kontaktregistreringer blandt appens brugere. Der bliver i de lande, der har og vil idriftsætte apps, gennemført undersøgelser omkring effektivitet contra udbredelse. STPS vil tilsvarende løbende evaluere appen ud fra tilgængelige indikatorer.

Anvendelse af løsningen medfører, at der behandles oplysninger om alle brugere af appen i form af elektroniske kontaktregistreringer, samt at der også behandles oplysninger om en række borgere, der ikke har appen installeret, gennem udtrækket fra Statens Serum Institut. Videregivelsen fra Statens Serum Institut er en behandling, som de registrerede ikke kan modsætte sig, og den er beskrevet i Smittestopbekendtgørelsens § 4, stk. 2. Samtlige behandlinger af personoplysninger i appen har desuden hjemmel i Smittestopbekendtgørelsen.

Ovenstående afbødes til dels af, at brugen af appen er frivillig, hvilket betyder at brugere selv kan vælge, om de ønsker at bruge appen og lade deres personoplysninger behandle[16]. Det har ingen konsekvenser, hvis borgeren ikke ønsker at anvende appen. Samtidig er den behandling og kontaktregistrering der sker, designet på en måde, der sikrer størst mulig beskyttelse af personoplysninger. Selv om de registrerede oplysninger er personoplysninger, er det alligevel næsten umuligt at kunne udlede noget af dem, da de er effektivt pseudonymiserede. Der forventes samtidig at sikre, at løsningen er gennemsigtig, og at de registrerede har mulighed for at få indblik i den overordnede behandling, og at de kan benytte appen på et oplyst grundlag.

Henset til behandlingens karakter og omfang, og at appen har til formål at understøtte væsentlige hensyn til en effektiv bremsning af smittespredningen, vurderer Styrelsen for Patientsikkerhed, at en digital

[15] Effective Configurations of a Digital Contact Tracing App: A report to NHSX, 16. April 2020

[16] Med undtagelse af oplysningerne fra Statens Serum Institut

sporingsapp er egnet og nødvendig af hensyn til arbejdet med smitteopsporing, og at appens behandling af personoplysninger ligger inden for, hvad de registrerede må tåle henset til det samfundskritiske formål.

## 5.1 Hjemmel til behandlingen og princippet om lovlighed, rimelighed og gennemsigtighed

### *5.1.1 Epidemiloven og Smittestop-bekendtgørelsen*

Det følger af § 21 b i lov om foranstaltninger mod smitsomme og andre overførbare sygdomme (epidemiloven)[17], 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.

Bestemmelsen 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 b, 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.

For så vidt angår muligheden for administrativt at fastsætte bestemmelser med hjemmel i epidemilovens § 21 b, bemærkes det, at bestemmelserne er meget bredt formuleret. § 21 b 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.

[17] 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

Bestemmelsen 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. Denne nødvendighedsvurdering skal bl.a. foretages i lyset af, at der er tale om en app, som borgeren frivilligt downloader. Epidemilovens § 21 b giver med andre ord hjemmel til at fastsætte regler om pligter til at oplyse sundhedsmyndighederne, herunder STPS, om visse personoplysninger og behandling af personoplysninger med henblik på bekæmpelse af COVID-19 i det omfang, Danmarks internationale forpligtelser tillader det. Dette ændrer ikke på, at den dataansvarlige for en given behandling af personoplysninger skal sikre, at behandlingen i de konkrete sammenhænge er proportionale med formål og delformål, herunder at behandlingerne er egnede til at opnå disse formål.

For at skabe et solidt hjemmelsgrundlag for løsningen samt sikre en regulering af de øvrige databeskyttelsesretlige rammer for løsningen har Sundheds- og Ældreministeriet fastsat regler om behandlingen af personoplysninger i Smittestop-appen i bekendtgørelse nr. 896 af 17. juni 2020 om behandling af oplysninger om elektronisk registrerede kontakter med henblik på at forebygge og inddæmme udbredelsen af Coronavirussygdom 2019 (COVID-19) ("Smittestop-bekendtgørelsen").

Behandlingen af personoplysninger i løsningen sker således i medfør af reglerne i Smittestop-bekendtgørelsen, jf. også afsnit 4.2 ovenfor, samt reglerne i cookiebekendtgørelsens § 3 og databeskyttelsesforordningen, jf. ndf.

### *5.1.2 Cookiebekendtgørelsen § 3*

Følgende fremgår af Smittestop-bekendtgørelsens § 1, stk. 3:

> *" Lagring af og adgang til oplysninger på brugerens telefon er efter bekendtgørelse nr. 1148 af 9. december 2011 om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugeres terminaludstyr (cookiebekendtgørelsen) betinget af, at brugeren har afgivet samtykke i overensstemmelse med artikel 4, nr. 11, og artikel 7 i databeskyttelsesforordningen. Øvrig behandling af personoplysninger, der foretages i forbindelse med drift og anvendelse af løsningen, er reguleret af denne bekendtgørelse."*

E-databeskyttelsesdirektivet indeholder regler for alle, der ønsker at lagre eller få adgang til oplysninger, der er lagret på terminaludstyr, herunder mobile enheder såsom smartphones, 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 databeskyttelsesdirektivet[18] at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen.

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 databeskyttelsesdirektivet, 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 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 databeskyttelsesdirektivet og databeskyttelsesforordningen eller ej, jf. præmis 71. Der er endvidere i databeskyttelsesforordningens artikel 7 fastsat en række krav til samtykket.

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.

[18] Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

Det Europæiske Databeskyttelsesråd har i en udtalelse af 12. marts 2019[19] 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.

E-databeskyttelsesdirektivets artikel 5, stk. 3, er implementeret i dansk ret i § 3 i cookiebekendtgørelsen[20]. 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.

EU-Domstolen har i Planet 49-dommen fastsat en række supplerende krav til den information, som brugerne skal have, samt krav til hvordan samtykket kan gives. Af dommen fremgår det, at der skal gives information om hvert enkelt formål, der sættes cookies til, og det skal være muligt at give samtykke til eller afslå de enkelte formål. Samtykket skal endvidere være en aktiv handling, og der ikke må herske tvivl om, hvorvidt brugeren har givet samtykket. Dette medfører, at en løsning, hvorved brugeren accepterer cookies ved at "klikke videre", ikke vil anses som værende et gyldigt samtykke, ligesom forudafkrydsede felter ikke vil være udtryk for en aktiv handling fra brugerens side. Et cookiesamtykke skal således altid være et "opt-in"-samtykke. EU-domstolen fastlagde med dommen endvidere, at der skal oplyses en "funktionsvarighed" – dvs. hvor længe de virker – for hver enkelt cookie, der sættes på brugerens terminaludstyr. Endelig fremgår det af dommen, at det skal oplyses om tredjemands mulighed for at få adgang til de cookies, der sættes.

På denne baggrund vil der i Smittestop-appen blive indføjet en funktionalitet, der sikrer, at der kan indhentes et forudgående samtykke fra de registrerede borgere, inden der sker lagring af eller gives adgang til oplysninger på borgernes telefo ved installation og brug af appen. Det vil endvidere sikres, at borgerne får den påkrævede information forud for lagringen af eller adgangen til oplysninger på borgernes smartphones. Dette er uddybet i afsnit 5.6.1.

[19] 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

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

Såfremt borgeren måtte trække sit samtykke efter cookiebekendtgørelsen tilbage, vil alle de registrerede data automatisk slettes fra borgerens telefon, der er gemt af appen. Borgeren vil modtage en advarsel om dette, inden data slettes. Borgeren kan også afinstallere appen med den konsekvens, at oplysningerne, der er lagret i appen, slettes. Samtidig er appen sat op til, at alle registrerede data automatisk slettes løbende 14 dage efter registreringen.

#### *5.1.3 Databeskyttelsesforordningen*

Behandling af almindelige, ikke-følsomme personoplysninger er lovlig, hvis behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra e.

Som beskrevet ovenfor i afsnit 5.1.1, følger det af Smittestopbekendtgørelsens § 1, at STPS stiller Smittestop-appen til rådighed for borgerne, og at STPS kan behandle personoplysninger i den forbindelse. Behandling af personoplysninger er således nødvendig for, at STPS kan udføre en opgave, der henhører under offentlig myndighedsudøvelse, som STPS har fået pålagt, og STPS databeskyttelsesretlige hjemmel for behandlingen af de almindelige, ikke-følsomme personoplysninger er således databeskyttelsesforordningens artikel 6, stk. 1, litra e, for så vidt angår de øvrige behandlinger, der ikke består af lagring af eller adgang til data på brugernes mobile enheder. Derudover foretages der en behandling af ikke-følsomme personoplysninger på borgernes telefon i form af kontaktregistrering og beregning af smitterisiko som beskrevet i Smittestopbekendtgørelsens § 3, stk. 1. Oplysningen om, at en borger har været udsat for en smitterisiko i forbindelse med kontakt med en smittet, er ikke efter STPS' vurdering en så konkret og specifik oplysning, at de udgør en følsom personoplysning i form af helbredsoplysninger omfattet af databeskyttelsesforordningens artikel 9.

Til brug for smitteverifikation – dvs. kontrol af, at en bruger, der ønsker at notificere sine elektroniske kontakter om, at vedkommende er bekræftet smittet med Coronavirussygdom 2019 (COVID-19) – vil STPS også behandle følsomme personoplysninger om de registrerede, jf. Smittestopbekendtgørelsens § 4, stk. 2. Det følger af databeskyttelsesforordningens artikel 9, stk. 1, at behandlingen af følsomme personoplysninger som udgangspunkt er forbudt. Det følger dog af artikel 9, stk. 2, at behandling af følsomme personoplysninger er lovlig, hvis et af de i litra a-j oplistede undtagelser finder anvendelse.

Det følger af databeskyttelsesforordningens artikel 9, stk. 2, litra g, at behandlingen af følsomme personoplysninger er lovlig, hvis behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og speci-

fikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser. Behandlingen af personoplysninger har hjemmel i epidemilovens § 21 b, som udmøntes i *Bekendtgørelse om behandling af oplysninger om elektronisk registrerede kontakter med henblik på at forebygge og inddæmme udbredelsen af Coronavirussygdom 2019 (COVID-19).* Bestemmelsen er herunder implementeret i dansk ret i databeskyttelseslovens § 7, stk. 4, 1. pkt., om væsentlige samfundsinteresser.

Det fremgår af forordningens præambelbetragtning nr. 52, at der bør gives mulighed for at fravige forbuddet mod at behandle følsomme personoplysninger, når det er fastsat i EU-retten eller medlemsstaternes nationale ret og er omfattet af de fornødne garantier, således at personoplysninger og andre grundlæggende rettigheder beskyttes, hvis dette er i samfundets interesse, navnlig behandling af personoplysninger inden for ansættelsesret, socialret, herunder pensioner og med henblik på sundhedssikkerhed, overvågning og varsling, forebyggelse eller kontrol af overførbare sygdomme og andre alvorlige trusler mod sundheden.

Bestemmelsen i databeskyttelseslovens 7, stk. 4, 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., jf. herved Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udgave, Jurist- og Økonomforbundets Forlag, 2020, s. 442.

Det følger af databeskyttelsesforordningens artikel 9, stk. 2, litra i, at behandling af følsomme personoplysninger er lovlig, hvis behandlingen er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet, f.eks. beskyttelse mod alvorlige grænseoverskridende sundhedsrisici eller sikring af høje kvalitets- og sikkerhedsstandarder for sundhedspleje og lægemidler eller medicinsk udstyr på grundlag af EU-retten eller medlemsstaternes nationale ret, som fastsætter passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder, navnlig tavshedspligt.

Det fremgår af forordningens præambelbetragtning nr. 54 bl.a., at behandling af særlige kategorier af personoplysninger kan være nødvendig af hensyn til samfundsinteresser, hvad angår folkesundhed uden den registreredes samtykke. En sådan behandling bør være underlagt passende og specifikke foranstaltninger med henblik på at beskytte fysiske personers rettigheder og frihedsrettigheder. I denne sammenhæng fortolkes »folkesundhed« som defineret i Europa-Parlamentets og Rådets forordning (EF) nr. 1338/2008 (11), dvs. alle elementer vedrørende sundhed, nemlig helbredstilstand, herunder sygelighed og invaliditet, determinanter med en indvirkning på helbredstilstanden, behov for sundhedspleje, ressourcer tildelt sundhedsplejen, ydelse af og almen adgang til sundhedspleje, udgifter til og finansiering af sundhedspleje samt dødsårsager.

Det må således lægges til grund, at STPS kan anvende artikel 9, stk. 2, litra g og i, smh. databeskyttelseslovens § 7, stk. 4, 1. pkt., som hjemmel til behandlingen af følsomme personoplysninger, idet det er STPS' vurdering, at denne behandling er nødvendig med henblik på, at STPS kan udføre opgaven med smitteopsporing, som STPS har fået pålagt i medfør af Smittestop-bekendtgørelsen.

Det fremgår af databeskyttelseslovens § 11, at offentlige myndigheder bl.a. kan behandle personnumre med henblik på en entydig identifikation af den registrerede. Det er nødvendigt for STPS' behandling af personoplysninger i forbindelse med smitteverifikation, at STPS entydigt kan identificere borgeren, da STPS skal sikre en korrekt smitteverifikation.

### 5.2 Princippet om formålsbegrænsning

Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra b, 1. led.

Som nærmere beskrevet i afsnit 4.1 er Smittestop-appens formål smitteopsporing, hvor appen skal fungere som et digitalt supplement til manuel smitteopsporing.

Det fremgår videre af § 1, stk. 4, i bekendtgørelsen, at STPS ikke må behandle oplysninger, som styrelsen registrerer i medfør af bekendtgørelsen til andre formål end de formål, der er nævnt i bekendtgørelsen. For at sikre, at oplysningerne ikke bruges til eksempelvis overvågning eller til at pålægge borgerne foranstaltninger, er der i bekendtgørelsen indsat en udtømmende liste over de formål, de indsamlede oplysninger må anvendes til.

Det fremgår således direkte af retsgrundlaget, hvilket formål som personoplysningerne må behandles til. STPS må alene behandle personoplysninger i løsningen inden for rammerne af disse formål samt de forudsætninger, der politisk ligger til grund for løsningen. Alle de behandlede oplysninger slettes samtidig automatisk efter 14 dage. Dette sikrer endvidere, at oplysningerne ikke kan viderebehandles til andre formål.

### 5.3 Princippet om dataminimering

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.

Ved vurderingen af appens nødvendighed må der overordnet set lægges vægt på, at appen og den dermed forbundne behandling af oplysninger tjener aktuelle og tungtvejende samfundsmæssige hensyn til sygdomsbekæmpelse og i sidste ende befolkningens sundhed og liv. Disse hensyn finder klar støtte i databeskyttelsesforordningen og -loven, lov om foranstaltninger mod smitsomme og andre overførbare sygdomme samt Smittestop-bekendtgørelsen, ligesom appen er opbygget i overensstemmelse med de principper, som er fastlagt i den brede politiske aftale mellem regeringen og en række partier den 15. maj 2020.

I løsningen sker der tre primære behandlinger af personoplysninger: Verifikation af smittestatus, registrering af elektroniske kontakter på brugerens telefon og opbevaring/videresendelse af ID'er for smittede brugere.

### *5.3.1 Verifikation af smittestatus*

Til brug for verifikation af, om en bruger aktuelt er smittet, skal brugeren logge ind med NemID. Dette login benytter de oplysninger, der tilhører NemID-løsningen: CPR-nummer, PID-nummer (pseudonymiseret identitetsangivelse), NemID-nummer. Dette er nødvendigt for at validere selve brugere og loginet. Når brugeren udsender en smittenotifikation, skal vedkommende samtidig oplyse om tidspunkter for, hvornår vedkommende udviklede symptomer, da dette har betydning for, hvilke brugere der skal modtage smittenotifikation. Denne oplysning indlejres som metadata i de rullende systemgenerede ID, og krypteres derefter.

Til brug for bekræftelse af smitte videregiver Statens Serum Institut til STPS hvert 5. minut en liste over alle de personer i Danmark, der aktuelt er vurderet smittede med COVID-19, jf. Smittestopbekendtgørelsens § 4, stk. 2. De korte intervaller skyldes, at der er behov for en liste, der altid er korrekt og opdateret. Der foretages en søgning på, at brugerens CPR-nummer findes på denne liste. Hvis det gør, godkendes smitteverifikationsprocessen.

Da videregivelsen omfatter hele datasættet over smittede, vil der potentielt behandles oplysninger om personer, der enten ikke benytter løsningen eller ikke har til hensigt at udsende en smittenotifikation. Dette er nødvendigt, da STPS ikke har kendskab til, hvem der har downloadet appen og dermed potentielt skal smittenotificere.

Da datasættet er forholdsvist begrænset, er det vurderes, at dette ikke overstiger, hvad der er nødvendigt. Dette skal også henses til, at der er tale om en offentlig myndighed, der er underlagt regler om tavshedspligt, og at oplysningerne gennem bekendtgørelsen er begrænset, således at de i løsningen kun må anvendes til de specifikt angivne formål.

### *5.3.2 Registrering af elektroniske kontakter på brugerens telefon*

For så vidt angår registreringen af elektroniske kontakter er det underliggende API udviklet af Google og Apple indrettet således, at alle vedvarende kontakter med uafbrudt Bluetooth-kontakt over en kort periode registreres. Det er ikke muligt at ændre på dette, da denne konfiguration er en del af grundfunktionaliteten. Dette kan betyde, at der reelt registreres flere oplysninger om elektroniske kontakter, end løsningen reelt har brug for, for at foretage en smittenotifikation.

Grunden til, at der registreres oplysninger om alle kontakter er, at det ikke på forhånd er muligt at vide, om en given person er smittet. Personen kan enten være smittet uden at været testet, eller smittet uden selv at vide det. Det er derfor nødvendigt at indsamle oplysninger om alle kontakter, da alle kontakter potentielt kan udgøre en smittekilde.

Oplysningerne om kontakterne er dog pseudonymiserede, og det vil derfor ikke være umiddelbart muligt for den enkelte bruger at udlede, hvilke fysiske personer de enkelte registreringer tilhører. Der vil dog i sjældne tilfælde kunne forekomme, at borgerne i forbindelse med en smittenotifikation vil kunne identificere den smittede, der har valgt at notificere sine kontakter herom. Det gælder i de tilfælde, hvor en borger, der modtager en smittenotifikation i appen, alene har haft en enkelt eller få elektroniske kontakter (herunder med den smittede) i løbet af en periode på 14 dage og er bevidst herom. Denne risiko og de mitigerende foranstaltninger i form af oplysning til borgerne herom er beskrevet nærmere nedenfor i afsnit 6.

### *5.3.3 Registrering af ID'er indsendt i forbindelse med en brugers smittenotifikation*

Når en bruger gennemfører en smitteverifikation, uploades brugerens ID'er for de seneste 14 dage til en central server. Formålet med dette er at have et centralt sæt af samtlige nøgler tilhørende smittede brugere. Dette sæt at nøgler hentes ligeledes af alle brugere af appen for at foretage sammenstilling med de kontaktregistreringer, den enkelte bruger har. Alle nøglerne er pseudonymiserede, og det er ikke muligt for STPS at koble nøglerne til en specifik bruger, efter nøglen er udstedt.

Den centrale database med smittede ID'er er essentiel for løsningen, da det er den eneste måde, hvorpå det kan sikres, at brugere af appen kan modtage smittenotifikationer. Da alle nøglerne er pseudonymiserede, vurderes det at være en hensigtsmæssig måde at håndtere det forholdsvis store datasæt på.

### *5.3.4 Nødvendigheden af behandlingen*

Brug af data og teknologi såsom lignende apps er anerkendt af både Det Europæiske Databeskyttelsesråd og EU-Kommissionen i kampen mod virussen. Oxford University har den 16. april 2020 offentliggjort et

studie[21], der viser, at sporing af digital kontakt kan bremse eller endda stoppe spredningen af COVID-19 og dermed bidrage til en hurtigere genåbning. Der er med andre ord videnskabelig støtte for brugen af sådan teknologi, og brugen af lignende apps er da også implementeret i flere lande i Europa. Brugen af apps har løbende været drøftet i størstedelen af EU-landene, og mange andre lande inden for EU har igangsat arbejdet med at udvikle apps, da de har vurderet, at der er tale om et effektivt værktøj til kontaktopsporing.

Brugen af appen står ikke alene, men indgår som et væsentligt element i en samlet strategi for bekæmpelse af virussen og genåbningen af Danmark, der også omfatter bl.a. manuel kontaktopsporing, øget brug af test m.v.

I vurderingen af proportionaliteten af appen må det endvidere tillægges vægt, at download af appen og brugen af dens funktionaliteter bygger på frivillighed og brugerkontrol.

STPS har generelt ved udviklingen af appen haft stort fokus på, at der alene indsamles og lagres de absolut nødvendige oplysninger i lyset af formålene med løsningen.

Personoplysningerne i forbindelse med denne kontaktregistrering lagres således alene lokalt på brugerens telefon – STPS lagrer med andre ord ikke kontaktoplysningerne på en central server (backend) – og den teknologiske løsning er således baseret på decentral kontaktregistrering, hvor brugeres kontakter kun gemmes på telefonen, og hvor matchingen mellem kontakter og smittede også sker decentralt. Der sker kun en overførsel af oplysninger, hvis borgeren vælger at melde sig smittet via appen (smitteverifikation og smittenotifikation). I dette tilfælde udveksles der alene de oplysninger, der er nødvendige for, at STPS kan bekræfte borgerens smittestatus. STPS har endvidere udarbejdet løsningen således, at den ikke registrerer oplysninger om borgernes lokalitet.

### 5.4 Princippet om rigtighed

Personoplysninger skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra d.

Det er *for det første* afgørende for appens funktionalitet og pålidelighed, at de indsamlede oplysninger om borgernes kontakter er korrekte. Som beskrevet ovenfor i afsnit 4.2 indsamles der gennem appen pålidelige data om brugernes kontakter med andre brugere gennem Bluetooth-teknologi, dvs. de pågældende smartphones' fysiske afstand til hinanden, varigheden af kontakten og tidsstempel for kontakten.

[21] Effective Configurations of a Digital Contact Tracing App: A report to NHSX, 16. April 2020

Når der er kontakt mellem to brugere med uafbrudt Bluetooth-kontakt over en kort periode, registreres oplysninger om signalstyrken af BlueTooth-forbindelse med de to telefoner samt varigheden. Signalstyrken måles løbende, og der lagres en gennemsnitsværdi. Signalstyrkeværdien danner grundlaget for vurderingen af, hvor tæt en kontakt har været. Eksempelvis vil signalstyrken forringes, hvis afstanden er stor eller hvis der er vægge eller lignende imellem. Dette fører samlet set til en lavere gennemsnitlig signalstyrkeværdi, og dermed en lavere *score* for, hvor tæt kontakten har været.

Det er endvidere *for det andet* væsentligt, at oplysningerne om, hvorvidt borgerne er blevet smittet med COVID-19, er valide, dvs. at der sker den fornødne smitteverifikation.

Hvis oplysningerne om smitte ikke er valide, vil det – i tilfælde af *falske positive* – skabe unødig stress og ængstelighed for borgeren, som igennem appen bliver notificeret om, at de har været i kontakt med en smittet. Dette kan tillige skabe en unødig belastning af sundhedsvæsenet.

Hvis der er tale om *falske negative*, vil borgerne ikke i overensstemmelse med formålet med appen blive adviseret om smitte eller smitterisiko, hvilket vil skabe falsk tryghed og kan føre til, at borgeren ikke tager de nødvendige forholdsregler over for sig selv eller andre.

STPS har i denne forbindelse overvejet, om STPS skal lade borgerne i appen selv registrere deres status som smittet eller ikke smittet. STPS har fravalgt denne mulighed, da STPS fra andre lande har fået oplyst eksempler, hvor borgere bevidst "forurener appen" med falske oplysninger om smittestatus med de ovenfor nævnte negative konsekvenser til følge.

STPS har derfor som et alternativ til selvindberetning valgt, at oplysningerne om smittestatus – hvis borgerne ønsker det – verificeres op imod data fra SSI via KID, der indeholder valide data om smittestatus, da oplysningerne herom bygger på test af borgeren.

Endvidere har STPS *for det tredje* valgt at benytte NemID i forbindelse med verifikation af smittestatus, da det er den etablerede måde for borgere entydigt at identificere sig overfor offentlige myndigheder i Danmark. Verifikationen har til formål at sikre, at det kun er brugere, der aktuelt er smittet, der logger ind. Samtidig vil det heller ikke være muligt for børn under 15 år at benytte denne funktion.

*For det fjerde* er det væsentligt, at brugere, der modtager en notifikation om, at de har været i nærheden af en smittet, også kan stole på rigtigheden af denne oplysning. Til sikring af dette er der udarbejdet en algoritme. Denne algoritme har til formål at beregne den risiko for smitte, som brugeren af appen har været udsat for. I beregningen indgår signalstyrkeværdien (som udtryk for afstand), længden af kontakten og hvornår kontakten skete i relation til, hvornår den smittede udviklede symptomer (kontakter er

mere smittefarlige i tiden tæt på symptomdebuten). Algoritmen er udarbejdet i samarbejde med teknikere og sundhedsfaglige for at sikre, at den er udtryk for et relevant risikoberegning. Hvis værdien af beregningen overstiger en vis værdi, modtager brugeren en på telefonen genereret besked om, at vedkommende har opholdt sig tæt på en anden bruger, der er smittet. Algoritmen evalueres og justeres løbende for at sikre, at den er retvisende.

Endelig er det *for det femte* vigtigt, at den vejledning og smittenotifikation, som borgeren gives af STPS gennem appen, hvis de er konstateret smittet eller har været i tæt kontakt med en smittet, er korrekte og fyldestgørende. STPS har i den forbindelse valgt, at borgeren, når denne notificeres, føres videre til hjemmesiden www.smittestop.dk. På denne side kan borgerne læse mere om, hvordan de skal forholde sig, hvis de modtager en smittenotifikation, og hvad der skal være opmærksomme på. Samtidig vil der på siden være kontaktoplysninger på den manuelle kontaktopsporing samt retningslinjer for, hvordan man skal forholde sig, hvis man udviser symptomer.

### 5.5 Princippet om opbevaringsbegrænsning

Efter princippet om opbevaringsbegrænsning i databeskyttelsesforordningens artikel 5, stk. 1, litra e, skal personoplysninger opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles.

Spørgsmålet om sletning af personoplysninger i løsningen er reguleret af Smittestopbekendtgørelsens § 3, stk. 2 og § 5 vedrørende henholdsvis sletning på brugerens telefon og sletning af personoplysninger, der er registreret hos STPS og implementeres i driftsaftalerne med driftsleverandørerne og gennem STPS' egne leverandørstyringsprocesser.

#### *5.5.1 Sletning af oplysninger på brugerens telefon*

Oplysninger lagret på brugerens telefon efter Smittestopbekendtgørelsens § 3, stk. 1, jf. afsnit 4.2 ovenfor, slettes efter bekendtgørelsens § 3, stk. automatisk på følgende måde:

1. Elektroniske kontakter registreret på brugerens telefon slettes automatisk 14 dage efter registreringen på telefonen.
2. Oplysning om hvilke systemgenererede nøgler, der er knyttet til en bruger, der har Coronavirussygdom 2019 (COVID-19) slettes automatisk efter 14 dage.
3. Oplysning om, at brugeren på grundlag af varigheden af kontakten, signalstyrke, den tidsmæssige afstand mellem kontakten og smittedebut sandsynligvis ud fra en epidemiologisk vurdering

er i kvalificeret risiko for at kunne være smittet med Coronavirussygdom 2019 (COVID-19), slettes automatisk 14 dage efter, at brugeren har modtaget notifikationen på telefonen.

4. Alle oplysninger registreret i løsningen slettes, når brugeren afinstallerer løsningen.

Oplysningerne opbevares således lokalt på telefonen i 14 dage med det formål at gøre det muligt for borgeren at kunne sende notifikationer til registrerede kontakter, hvis borgeren bekræftes smittet med COVID-19 og modtage notifikationer fra registrerede kontakter, hvis en af borgerens kontakter bliver bekræftet smittet med COVID-19. Sletning af data på telefonen er styret af API'et, og det er ikke muligt at ændre på dette.

Alle oplysninger registreret på telefonen i Smittestop-appen slettes, når brugeren afinstallerer appen, jf. Smittestop-bekendtgørelsens § 3, nr. 1, eller når brugeren i gennem appen trækker sit samtykke tilbage.

### *5.5.2 Sletning af oplysninger hos STPS*

Brugerens Nem-ID-oplysninger slettes automatisk hos STPS 24 timer efter, at STPS har foretaget verifikation af, om en bruger har Coronavirussygdom 2019 (COVID-19), jf. Smittestop-bekendtgørelsens § 5, stk. 1, nr. 1. Opbevaringen sker af hensyn til korrekt sikring af verifikation.

Oplysning om, hvor mange smittestatus-verifikationer, der er udstedt for en given bruger, opbevares af STPS i 24 timer, jf. bekendtgørelsens § 5, stk. 1, nr. 2.Opbevaringen skyldes behovet for at kunne sikre, at en enkelt bruger ikke udsender mange notifikationer fra telefoner, der ikke tilhører den pågældende og således undgå urigtige notifikationer. Der kan f.eks. tænkes en situation, hvor en bruger melder sig smittet på andres telefoner, hvorefter der sendes en notifikation til deres kontakter.

Oplysning om brugere, der har Coronavirussygdom 2019 (COVID-19), jf. § 3, stk. 2, nr. 2, slettes løbende hos Styrelsen for Patientsikkerhed i takt med, at smittestatus ikke længere er relevant, jf. bekendtgørelsens § 5, stk. 1, nr. 3. SSI fastlægger, hvad der menes med "relevant" ud fra en epidemiologisk vurdering. I takt med, at SSI ændrer på vurderingen af, hvornår en given person kan betragtes som smittet, vil dette også kunne føre til, at slettefristerne for oplysningerne enten forlænges eller forkortes.

Oplysning om, hvilke systemgenererede nøgler, der er anvendt af brugere, der har gennemført positiv smitteverifikation, slettes automatisk efter 14 dage, jf. bekendtgørelsens § 5, stk. 1, nr. 4.

Al behandling af data har gennem bekendtgørelsen fastlagt en slettefrist. Dette sikrer, at der ikke vil ligge data tilbage, når løsningen ikke længere benyttet. Lagringen af kontaktoplysninger i løsningen slettes automatisk efter 14 dage, eller når brugeren sletter løsningen på sin telefon.

Smittestopbekendtgørelsen ophæves den 31. oktober 2020, jf. bekendtgørelsens § 6, stk. 2.

## 5.6 De registreredes rettigheder

### *5.6.1 Oplysningspligten*

STPS vil i appens design understøtte fornøden information af brugerne om behandlingen af oplysningerne i appen, ligesom Sundheds- og Ældreministeriet vil informere offentligheden bredt om appens funktioner og behandlinger m.v., herunder ved offentliggørelse af information på www.smittestop.dk.

Styrelsen vil sørge for at give borgerne fyldestgørende information i overensstemmelse med cookiebekendtgørelsens § 1, stk. 3.

STPS vil både behandle personoplysninger, der er indsamlet fra den registrerede selv og fra andre, da oplysningerne delvist indsamles via borgerens smartphone og delvist fra SSI via KID.

Det følger af reglerne om oplysningspligt i databeskyttelsesforordningens artikel 13-14, at de registrerede som udgangspunkt skal underrettes om den dataansvarliges behandling af personoplysninger.

STPS vil opfylde oplysningspligten i forbindelse med borgernes installation af appen. Således vil STPS informere brugerne om behandlingen af deres personoplysninger decentralt på telefonen samt centralt i forbindelse med smitteverifikation og -notifikation. Se endvidere nedenfor vedrørende STPS' information til brugerne om, hvordan kontaktregistreringen fungerer. Oplysningsteksten gøres endvidere tilgængelig via App Store og Google Play gennem et link til STPS' hjemmeside, hvor teksten findes.

Ovennævnte information om behandlingen af oplysningerne i appen efter cookiebekendtgørelsens § 3 og databeskyttelsesforordningens artikel 13-14 vil vedvarende være tilgængelig i selve appen, så borgeren altid kan genbesøge og læse informationen, når borgerne ønsker dette. Informationen vil være tilgængelig gennem et link til den side, hvor informationen ligger.

STPS indsamler som nævnt endvidere personoplysninger fra KID vedrørende personer, der er smittet med COVID-19, og som ikke har downloadet appen. Det er vurderingen, at STPS for så vidt angår indsamlingen af disse personoplysninger vil være undtaget fra opfyldelse af oplysningspligten, idet STPS' indsamling af disse oplysninger udtrykkelig er fastsat i Smittestopbekendtgørelsens § 4, stk. 2, således at oplysningspligten ikke finder anvendelse, jf. databeskyttelsesforordningens artikel 14, stk. 5, litra c. Orienteringen om dette vil dog stadig være tilgængelig på siden www.smittestop.dk, for at sikre transparens.

### *5.6.2 Øvrige rettigheder*

Som nævnt ovenfor i afsnit 4.2, er det ikke muligt for STPS at håndtere brugernes eventuelle anmodninger om at udøve deres rettigheder i form af f.eks. anmodninger om indsigt i eller sletning af oplysninger lagret på brugerens telefon, da STPS ikke har adgang til disse oplysninger på brugernes telefoner i den decentrale løsning. STPS har derfor indrettet løsningen således, at borgeren selv har kontrol over sletning af oplysningerne.

Hvis de registrerede ønsker at udøve deres rettigheder, ville dette primært være for de data, der modtages fra Statens Serum Institut (oplysninger om aktuelt COVID-19-smittede) og i oplysningerne, der registreres i forbindelse med NemID-login, da disse er de primære behandlinger af personoplysninger hos STPS. Det vil være muligt at bede om indsigt i begge disse databehandlinger. Da udtrækket indeholder et forholdsvist begrænset antal personer, vil anmodninger fra de registrerede håndteres manuelt ved at de registrerede kontakter STPS. Herefter vil deres anmodninger blive behandlet af en sagsbehandler. Hvis det viser sig, at der modtages flere anmodninger, end det er muligt at behandle inden for tidsfristerne, er det muligt at afsætte flere ressourcer til dette. Bistand fra databehandleren er reguleret af de respektive databehandleraftaler.

Retten til dataportabilitet (artikel 20) finder ikke anvendelse, idet behandlingen ikke er baseret på et databeskyttelsesretligt samtykke eller på en kontrakt.

STPS har overvejet, om oplysningerne til brugerne af appen i form af smittenotifikationer, der genereres til brugerne ved brugernes kontaktregistreringer med smittede brugere, udgør automatiske individuelle afgørelser, der er omfattet af databeskyttelsesforordningens artikel 22.

Efter forordningens artikel 22, stk. 1, har den registrerede ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende.

Det anføres om bestemmelsen i Justitsministeriets betænkning 1565, s. 376, at der – ligesom tilfældet var efter den dagældende persondatalovs § 39 – skal være tale om afgørelser, der kan gøres gældende over for den registrerede, og som har konsekvenser for den pågældende. Den omstændighed, at der f.eks. udsendes materiale af oplysende karakter til en række personer, der står opført på en liste, vil ikke udgøre en afgørelse i artikel 22's forstand, idet der ikke træffes en afgørelse, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende. Det anføres endvidere, at eksempelvis markedsføring, i hvert fald af generel karakter, endvidere ikke vil være omfattet af bestemmelsen, idet der ikke i den forbindelse træffes en afgørelse i artikel 22's forstand, jf. herved også s. 23 i Det Europæiske Databeskyttelsesråd, Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning

2016/679, WP251rev.01, af 6. februar 2018. Dette forhold er endvidere bekræftet af Datatilsynet, der i en afgørelse af 2. juni 2020 udtalte, at en dansk virksomheds udarbejdelse af prediktive modeller med henblik på at målrette eventuel senere markedsføring ikke udgjorde en afgørelse omfattet af artikel 22, da de udarbejdede prediktive modeller ikke kunne anses for at have haft retsvirkning eller på tilsvarende vis betydeligt have påvirket klager (Datatilsynets j.nr. 2019-31-1713).

Løsningen indebærer ikke, at der træffes afgørelser over for de enkelte brugere i forbindelse med, at der i appen gives oplysninger til brugerne af appen i form af smittenotifikationer, der genereres til brugerne ved brugernes kontaktregistreringer med smittede brugere. Derimod har smittenotifikationerne karakter af information og vejledning til brugerne. Den egentlige afgørelse af, hvorvidt en bruger, der har modtaget en smittenotifikation i appen, er smittet, foretages i forbindelse med den efterfølgende test, hvis brugeren måtte ønske at få foretaget en sådan test.

Det er på denne baggrund STPS' vurdering, at kontaktregistreringen samt funktionaliteten i løsningen i form af smittenotifikation ikke er omfattet af artikel 22, allerede fordi løsningen ikke indebærer en afgørelse over for de registrerede, som er et krav efter ordlyden af bestemmelsen.

STPS vil dog – for at understøtte en gennemsigtig behandling – sørge for, at brugerne af appen i forbindelse med opfyldelse af oplysningspligten, jf. afsnit 5.6.1 ovenfor, modtager meningsfulde oplysninger om logikken i løsningen samt betydningen og de forventede konsekvenser af en sådan behandling for de registrerede svarende databeskyttelsesforordningens artikel 13, stk. 2, litra f. Brugerne vil med andre ord modtage oplysninger om, hvordan løsningen fungerer, herunder hvilke parametre og beregninger der ligger til grund for kontaktregistreringen.

## 5.7 Behandlingssikkerhed

Forhold vedrørende behandlingssikkerhed er beskrevet i risikovurderingen (Bilag 1 – Risikovurdering). Nedenfor er et kort resume af indholdet fra risikovurderingen.

### *5.7.1 Forretningsmæssigkonsekvensvurdering og screening af risikoen for registrerede*

Under screeningen blev det blev vurderet, at en kompromittering af "Smittestop" kan lede til alvorlige konsekvenser for både koncernen og de registrerede. På grund af den høje risiko og de mulige konsekvenser, behandlingsaktiviteterne kan have for de registrerede, er det et krav, at der udarbejdes en risikovurdering, der understøtter implementering af passende og tidssvarende tekniske og organisatoriske kontroller.

### *5.7.2 Databeskyttelse*

Risikovurderingens omfang er afgrænset til risici, der relaterer sig til udvikling og drift af den samlede "Smittestop"-løsning mens risici, der knytter sig til behandlingsaktiviteternes proportionalitet og nødvendighed, hjemmel, dataminimering, datakvalitet, opbevaringsbegrænsning, håndtering af databehandlere og underdatabehandlere og håndtering af registrerede rettigheder, vurderes og håndteres i det selvstændige dokument "Konsekvensanalysen vedr. databeskyttelse – smittestop app".

### *5.7.3 Risikovurdering*

Der er identificeret, analyseret og vurderet 27 risici for løsningen. Heraf er ingen vurderet til være opsættende for go-live. 8 risici er elimineret i løbet af udviklingen af løsningen.

Der er ingen risici med opsættende virkning for idriftsættelse. For 5 risici anbefales det, at der kort tid efter go-live fastsættes datoer for afklaring/udbedring. De 5 risici er ved kontrollen vurderet som utilstrækkelige og med mangler. Det drejer sig om beskrivelsen vedr. governance og processer for samarbejdet mellem de mange parter omkring denne komplekse løsning samt endelig verifikation af udbedrede alvorligere findings fra penetrationstest og sikkerhedsreview.

Generelt er der her tale om en høj-risiko løsning med stor offentlig og politisk interesse og flere risici, der derfor kan have store konsekvenser for forretningen og den registrerede, såfremt de indtræffer. Sandsynligheden for at de indtræffer, er i projektet reduceret til utænkelig/usandsynlig, hvorfor disse risici kan accepteres.

## 5.8 Forholdet til databehandlere

Som beskrevet ovenfor er STPS dataansvarlig for den behandling af personoplysninger, der sker Smittestop-appen. STPS har indgået en databehandleraftale med Digitaliseringsstyrelsen (herefter "DIGST"), der på vegne af STPS har indgået en aftale med Netcompany om udvikling og drift af appen. DIGST er således databehandler for STPS, og underdatabehandler til DIGST. Netcompany og DIGST varetager opbevaringen af de systemgenererede rullende ID'er, der indsendes, når en bruger melder sig smittet. De varetager også udsendelsen af ID'erne til brugere af appen til brug for smitteverifikation.

Derudover benytter STPS Sundhedsdatastyrelsen som databehandler for smittestatusverifikationen gennem NemID. Til denne behandling benyttes Trifork som underdatabehandler. Trifork leverer integrationen til NemID, og indhentning og opbevaring af oplysninger om smittestatus fra SSI. Samtidig foretager Trifork valideringen af, om en bruger der melder sig smittet fremgår af oplysningerne om smittede fra SSI. Trifork benytter Netic som underunderdatabehandler.

Det følger af Smittestop-bekendtgørelsens § 4, stk. 3, at STPS og en eventuel databehandler, der på styrelsens vegne varetager driften af registrerede kontakter, har adgang til de i stk. 2 nævnte oplysninger, når det er påkrævet af driftstekniske grunde eller følger af Styrelsen for Patientsikkerheds forpligtelser som dataansvarlig.

Der er indgået en databehandleraftale mellem STPS som dataansvarlig og DIGST som databehandler. STPS fører i henhold til databehandleraftalen løbende tilsyn med DIGST og den behandling af personoplysninger, som DIGST foretager på STPS' vegne. DIGST har indgået en underdatabehandleraftale med Netcompany og fører tilsyn med Netcompany og virksomhedens behandling af oplysninger og personoplysninger på vegne af STPS.

STPS har desuden indgået en databehandleraftale med Sundhedsdatastyrelsen for den del af behandlingen, som de foretager. Sundhedsdatastyrelsen har indgået en databehandleraftale med Trifork, som igen har indgået en underdatabehandleraftale med Netic.

Alle aftalerne indeholder bestemmelser om tilsyn, bistand til den dataansvarlige, underretning af den dataansvarlige i tilfælde af brud mv. Aftalerne er baseret på Datatilsynets seneste skabelon samt STPS' risikovurdering af løsningen.

### 5.9 Overførsel af personoplysninger til tredjelande og internationale organisationer

Det er for nuværende ikke hensigten, at personoplysningerne vil blive overført til tredjelande eller internationale organisationer. Endvidere er der stillet krav til databehandlerne i databehandleraftalerne om, at de ikke må overføre personoplysninger omfattet af projektet til tredjelande eller internationale organisationer. Såfremt en sådan overførsel til tredjelande eller internationale organisationer måtte blive aktuelt, vil der ske en revidering af denne konsekvensanalyse med henblik på forudgående at sikre det fornødne lovlige overførselsgrundlag samt hjemmelsgrundlag for overførslen, samt at den i øvrigt vil ske på en sikkerhedsmæssig forsvarlig måde.

Der er i samtlige databehandleraftaler indskrevet, at der ikke må ske overførsel af oplysninger til tredjelande, og at persondata ikke må tilgås fra personer uden for EU/EØS.

### 5.10 Løbende evaluering af appen

Bekæmpelsen af COVID-19 og smittespredningen i samfundet i takt med genåbningen er dynamisk, og der kommer kontinuerligt nye erfaringer, tiltag og forskning på området.

STPS vil følge udviklingen nøje, ligesom STPS vil følge udviklingen og erfaringerne i andre lande med lignende løsninger.

For at sikre, at Smittestop-appen vedvarende er nødvendig og lever op til dens formål, vil STPS i lyset heraf foretage løbende evalueringer af appen og dens effekt, funktionalitet og datakilder/datakvalitet på baggrund af udviklingen i smittespredningen i samfundet, tilslutningsprocenten i befolkningen til appen og den nationale strategi for genåbningen af Danmark. Evalueringerne indeholder også stillingtagen til de nedenfor i afsnit 6 identificerede risici og foranstaltninger til at håndtere disse samt ændringer i risikobilledet.

Evalueringerne sker under inddragelse af det nedsatte Advisory Board bestående af forskere, sikkerhedseksperter og medlemmer fra Dataetisk Råd, der skal rådgive og vejlede myndighederne om hensyn til bl.a. datasikkerhed og privatlivsbeskyttelse i udviklingen af appen. Samtidig vil evaluering af appen altid være baseret på den seneste epidemiologiske viden omkring COVID-19, samt anbefalinger fra sundhedsmyndigheder og forskere.

Evalueringerne vil blive foretaget af STPS efter behov, dog mindst kvartalsvist og vil blive dokumenteret skriftligt.

## 6. IDENTIFIKATION OG EVALUERING AF RISICI SAMT FORANSTALTNINGER TIL AT HÅNDTERE RISICI

### 6.1 Indledning

Næste skridt er at identificere risici for de registreredes rettigheder og frihedsrettigheder (risikoidentifikation) samt at evaluere disse risici ud fra deres sandsynlighed og alvor (risikoevaluering), jf. databeskyttelsesforordningens artikel 35, stk. 7, litra c. Nærmere bestemt skal der navnlig foretages en vurdering af risikoens oprindelse, karakter, særegenhed og alvorlighedsgrad, jf. databeskyttelsesforordningens præambelbetragtninger 84 og 90. Vurderingen skal foretages for hver enkelt identificeret risiko set ud fra den registreredes perspektiv, men på et objektivt grundlag.

En risiko kan defineres som et scenarie, der beskriver en hændelse og konsekvenserne heraf, som vurderes i forhold til alvor og sandsynlighed.[22]

Eksempler på konsekvenser for den registrerede kan f.eks. være fysisk, materiel eller immateriel skade, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af fortrolighed for

[22] EDPB, WP 248, rev. 01, s. 7

personoplysninger, der er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser, samt hvis de registrerede kan blive berøvet deres rettigheder og frihedsrettigheder eller forhindret i at udøve kontrol med deres personoplysninger, jf. præambelbetragtning 75.

Efter at have identificeret og evalueret de forskellige risici er næste skridt at identificere foranstaltninger for at kunne håndtere disse risici. Formålet er at nedbringe konsekvenserne af de identificerede risici til et acceptabelt niveau. De typiske risikostyringsstrategier vil være at enten eliminere, reducere eller acceptere den identificerede risiko. Det skal for hver enkelt identificeret risiko – der er vurderet som høj eller medium – fremgå af konsekvensanalysen, hvorvidt risikoen er elimineret, reduceret eller accepteret. Det skal også konkluderes, om den samlede restrisiko fortsat vil være høj, såfremt de påtænkte foranstaltninger implementeres, da Datatilsynet i så fald skal høres, jf. databeskyttelsesforordningens artikel 36.

### 6.2 Valg af evalueringskriterier for sandsynlighed og konsekvens

I denne konsekvensanalyse anvendes følgende evalueringskriterier for sandsynlighed:

**Tabel 1. Evalueringskriterier for sandsynlighed**

| | |
|---|---|
| **4** | **Forventet**: Det forventes, at hændelsen vil forekomme, herunder f.eks.:<br>- Man har erfaring med hændelsen inden for de sidste 12 måneder.<br>- Hænder jævnligt hos andre offentlige myndigheder og private virksomheder (omtales ofte i pressen). |
| **3** | **Moderat sandsynligt**: Det er moderat sandsynligt, at hændelsen vil forekomme, herunder f.eks.:<br>- Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder.<br>- Kendes fra andre offentlige myndigheder og private virksomheder i Danmark (omtales årligt i pressen). |
| **2** | **Mindre sandsynligt**: Hændelsen forventes ikke at forekomme, herunder f.eks.:<br>- Ingen erfaring med hændelsen.<br>- Kendes fra få andre offentlige myndigheder og private virksomheder, men ikke i Danmark. |
| **1** | **Usandsynligt**: Det anses for næsten udelukket, at hændelsen nogensinde kan forekomme, herunder f.eks.:<br>- Ingen erfaring med hændelsen.<br>- Kendes fra få andre offentlige myndigheder og private virksomheder, men ikke i Danmark. |

I denne konsekvensanalyse anvendes følgende evalueringskriterier for konsekvens[23]:

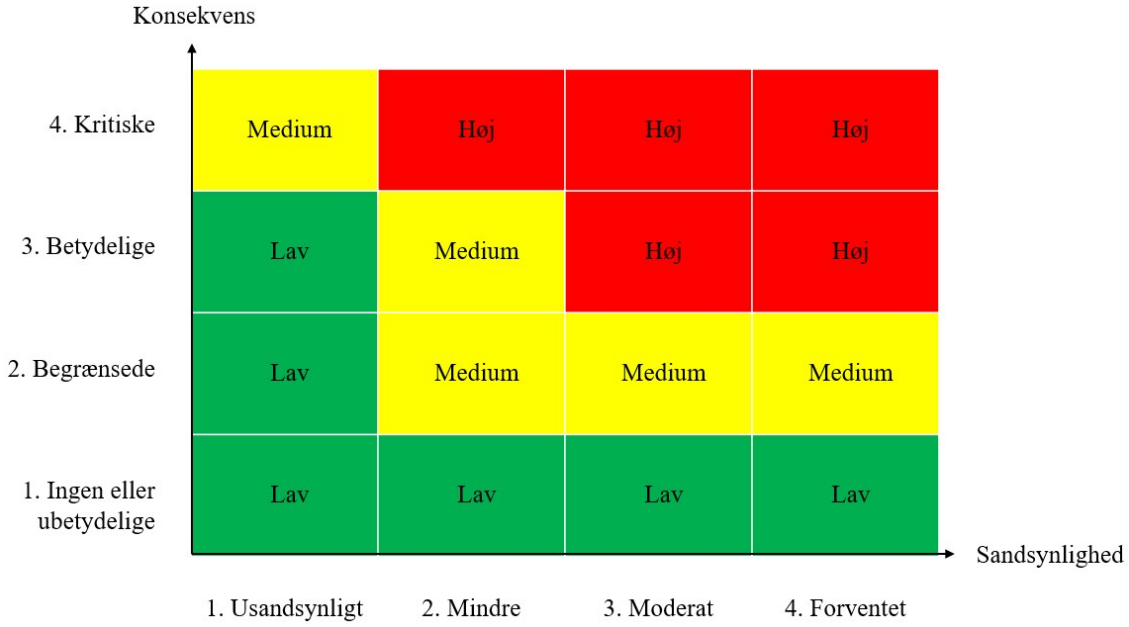
**Tabel 2. Evalueringskriterier for konsekvens**

| | |
|---|---|
| **4** | **Kritiske konsekvenser**: De registrerede kan opleve kritiske konsekvenser, som de ikke nødvendigvis kan overvinde, f.eks. økonomisk nød som betydelig gæld eller manglende evne til at arbejde, langsigtede psykiske eller fysiske lidelser, død m.v. |
| **3** | **Betydelige konsekvenser**: De registrerede oplever betydelige konsekvenser, som de kan overvinde om end med alvorlige vanskeligheder, f.eks. identitetstyveri eller -svig, finansielle tab, blacklisting af banker, ejendomsskade, tab af beskæftigelse, stævning, forværring af sundhedstilstanden, tab af fortrolighed af personoplysninger, der er omfattet af tavshedspligt m.v. |
| **2** | **Begrænsede konsekvenser**: De registrerede oplever begrænsede konsekvenser, som de vil være i stand til at overvinde med få vanskeligheder, f.eks. ekstra omkostninger, nægtelse af adgang til forretningstjenester, manglende forståelse, frygt, stress, mindre fysiske påvirkninger m.v. |
| **1** | **Ingen eller ubetydelige konsekvenser**: De registrerede bliver enten ikke påvirket eller udsættes alene for få generende konsekvenser, som de uden problemer kan håndtere, f.eks. tidsforbrug brugt på at genindtaste oplysninger, irritationer, dårlig brugeroplevelse m.v. |

Når evalueringskriterierne for sandsynlighed og konsekvens er fastlagt, kan hver enkelt identificeret risiko vurderes og kortlægges på et såkaldt risikokort. I denne konsekvensanalyse anvendes følgende risikokort:

**Figur 3 Risikokort**

[23] Se f.eks. punkt A.2 i Annex A til ISO/IEC 29134:2017; Datatilsynet m.fl., Vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger, juni 2018, s. 9; Digitaliseringsstyrelsen, Vejledning i vurdering af offentlige it-projekters potentielle konsekvenser for privatlivet, maj 2013, s. 12




### 6.3 Identifikation, evaluering og håndtering af risici

Identifikationen af risici for de registreredes rettigheder og frihedsrettigheder tager sit udgangspunkt i det forhold, at STPS som led i projektet behandler følsomme helbredsoplysninger for et potentielt stort antal borgere og at behandlingen til dels sker i et decentralt app-miljø og et centralt lagringsmiljø. Risikobilledet skal også ses i lyset af, at STPS løbende foretager evalueringer af appen, jf. afsnit 5.10 ovenfor, herunder af risiciene for de registrerede.

De væsentligste risici i løsningen udgøres af risikoen for, at borgeren ikke kan overskue konsekvenserne af sin accept til at dele information om smittestatus med andre (smittenotifikation) samt risikoen for manglende eller tab af pseudonymisering af personoplysninger i løsningen.

Nedenfor foretages en gennemgang af de i projektet identificerede risici efter tur, idet det bemærkes, at der for så vidt angår risici vedrørende manglende eller begrænset behandlingssikkerhed, henvises til risikovurderingen vedrørende behandlingssikkerhed, jf. Bilag 1 – Risikovurdering.

Det bemærkes, at samtlige risici og de identificerede foranstaltninger er genstand for løbende overvågning og evaluering, jf. nærmere afsnit 5.10 ovenfor.

### *6.3.1 Risiko 1: Manglende informationer i forbindelse med afgivelse af e-privacy-samtykke*

#### *6.3.1.1 Beskrivelse af risikoen*

Cookiebekendtgørelsens § 3 oplister som nævnt i afsnit 5.1.2 en række minimumskrav til den information, som borgeren skal have, før der må lagres eller opnås adgang til oplysninger, herunder personoplysninger, på borgerens telefon. Er den information, der gives til borgeren i forbindelse med download af appen, ikke fyldestgørende, risikerer borgeren at samtykke til forhold, som borgeren reelt set ikke ønsker at samtykke til.

#### *6.3.1.2 Foranstaltninger til at håndtere risikoen*

Denne risiko er forsøgt reduceret ved, at STPS udarbejder en fyldestgørende information til borgeren, som præsenteres for borgeren i løsningen i forbindelse med samtykkeafgivelsen. I øvrigt vil informationen være vedvarende tilgængelig for borgeren i løsningen og på www.smittestop.dk/databeskyttelse, så borgeren til enhver tid kan se informationen.

### *6.3.2 Risiko 2: Manglende evne til at overskue konsekvenserne af accept til at dele information om smittestatus med andre*

#### *6.3.2.1 Beskrivelse af risiko*

Borgeren bliver givet muligheden for at dele oplysninger om smittestatus med de kontakter, som borgeren har haft inden for de seneste 14 dage, såfremt borgeren bliver testet positiv for COVID-19 (smittenotifikation). Det udgør en risiko for borgeren, at borgeren ikke fuldt ud kan overskue konsekvenserne af borgerens accept, herunder at borgeren i nogle tilfælde vil kunne identificeres (se hertil risiko 7), da borgeren i så fald risikerer at give accept til en behandling, som borgeren reelt ikke ønsker.

#### *6.3.2.2 Foranstaltninger til at håndtere risikoen*

Denne risiko er forsøgt reduceret ved – forud for borgerens accept af smittenotifikationen – at give borgeren information om, at oplysninger om smittestatus deles med kontakterne i pseudonymiseret form, men at der en risiko for identifikation i særlige tilfælde, og at borgeren dermed, før accepten gives, er oplyst om, at der er en risiko for, at borgeren kan blive identificeret som smittet af andre. Denne risiko fremgår at vores orienteringstekst om behandling af personoplysninger.

### *6.3.3 Risiko 3: Tilsidesættelse af princippet om formålsbegrænsning*

#### *6.3.3.1 Beskrivelse af risiko*

En af forudsætningerne for Smittestop-appen er, at data ikke vil blive brugt på individniveau til at pålægge enkelte borgere restriktioner eller foretage overvågning af enkeltindividers overholdelse af regler, jf. nærmere ovenfor i afsnit 4.1. Det udgør en integritetskrænkelse af den enkelte borger, hvis STPS, anvender data til at gøre konkrete indgreb over for borgeren, da borgeren i forbindelse med download af appen, er blevet lovet, at dette ikke vil finde sted.

#### *6.3.3.2 Foranstaltninger til at håndtere risikoen*

Denne risiko er reduceret ved, at der – som nærmere beskrevet i afsnit 4.1 – i Smittestop-bekendtgørelsens § 1, stk. 4, er fastsat klare regler om, at STPS ikke må behandle oplysninger, som styrelsen registrerer i medfør af bekendtgørelsen til andre formål end de formål, der er nævnt i bekendtgørelsen, herunder at oplysningerne i løsningen ikke må anvendes til brug for styrelsens beslutning om påbud i medfør af § 5, stk. 1, i lov om foranstaltninger mod smitsomme og andre overførbare sygdomme, jf. bekendtgørelse om undersøgelse, indlæggelse eller isolation og tvangsmæssig behandling i medfør af lov om foranstaltninger mod smitsomme og andre overførbare sygdomme i forbindelse med håndtering af Coronavirussygdom 2019 (COVID-19).

Hertil kommer, at STPS har reduceret risikoen for tilsidesættelse af princippet om formålsbegrænsning ved at designe løsningen, således at kontaktregistreringerne foregår lokalt på brugernes telefoner, og STPS ikke har adgang til oplysningerne om elektroniske kontakter på brugernes telefoner. STPS har alene adgang til ID'erne på de personer, der melder sig smittede.

For så vidt angår de personoplysninger, som STPS har adgang til i forbindelse med de centrale behandlingsaktiviteter i form af smitteverifikation og -notifikation og lagringen af disse oplysninger i denne forbindelse, vil STPS reducere risikoen for at bruge disse oplysninger til uvedkommende formål ved brug af løbende sletning og organisatoriske foranstaltninger i form af interne retningslinjer herom.

### *6.3.4 Risiko 4: Tilsidesættelse af princippet om dataminimering*

#### *6.3.4.1 Beskrivelse af risiko*

Det er en velkendt risiko ved behandling af personoplysninger i apps, at der kan indsamles oplysninger om borgerne uden deres vidende, som ikke er nødvendige i lyset af formålet med behandlingen. Indsamler

Smittestop-appen andre oplysninger end det nødvendige, vil det udgøre en risiko for borgeren, da borgeren i så fald ikke er vidende om, hvilke oplysninger som myndighederne faktisk har adgang til.

#### *6.3.4.2 Foranstaltninger til at håndtere risikoen*

Foranstaltningerne for at sikre overholdelse af princippet om dataminimering er nærmere beskrevet i afsnit 5.3 ovenfor, hvortil der henvises. Desuden har der i hele projektet været inddraget personer med sundhedsfaglig baggrund med henblik på at kvalificere, hvilke oplysninger der er nødvendige for at foretage en effektiv smitteopsporing.

STPS har valgt en decentral løsning, hvor personoplysningerne i forbindelse med kontaktregistrering alene lagres lokalt på brugerens telefon. STPS lagrer med andre ord ikke disse oplysninger på en central server (backend), og den teknologiske løsning er således baseret på decentral kontaktregistrering, hvor brugeres kontakter kun gemmes på telefonen, og hvor matchingen mellem kontakter og smittede også sker decentralt. Der sker kun en overførsel af oplysninger, hvis borgeren vælger at melde sig smittet via appen (smitteverifikation og smittenotifikation). I dette tilfælde udveksles der alene de oplysninger, der er nødvendige for, at STPS kan bekræfte borgerens identitet og smittestatus. STPS har endvidere designet løsningen, så der ikke registreres oplysninger om borgernes lokalitet.

### *6.3.5 Risiko 5: Risiko for unøjagtige data (manglende rigtighed)*

#### *6.3.5.1 Beskrivelse af risiko*

Da borgerne bruger appen til at få oplysninger om, hvorvidt borgeren har været udsat for smitterisiko gennem sine kontakter, dels kan vælge at dele information om sin status som smittet, må der ikke spredes forkerte oplysninger i appen. Dette gælder både falske positive, dvs. hvor der fejlagtigt spredes oplysninger om, at en person er smittet, selvom vedkommende ikke er det, og falske negative, dvs. hvor det omvendte er tilfældet.

Som beskrevet i afsnit 5.4 ovenfor vedrørende princippet om rigtighed, vil det potentielt skabe unødig stress og ængstelighed for borgeren, som igennem appen bliver notificeret om, at de har været i kontakt med en smittet, hvis oplysningerne om smitte ikke er valide.

Hvis der er tale om *falske negative*, vil borgerne ikke i overensstemmelse med formålet med appen blive adviseret om smitte eller smitterisiko, hvilket vil skabe falsk tryghed og kan føre til, at borgeren ikke tager de nødvendige forholdsregler over for sig selv eller andre. Hvis der er tale om *falske positiver*, vil dette kunne skabe utryghed blandt brugerne, og eventuelt medførere, at visse brugere går unødigt i selvkarantæne.

#### *6.3.5.2 Foranstaltninger til at håndtere risikoen*

Foranstaltningerne for at sikre den fornødne datakvalitet er nærmere beskrevet i afsnit 5.4 ovenfor, hvortil der henvises.

Der sikres en pålidelig kontaktregistrering ved brug af Bluetooth-teknologi, dvs. de pågældende telefoners fysiske afstand til hinanden, varigheden af kontakten og tidsstempel for kontakten. Samtidig har en række sundhedsfaglige med viden om epidemiologi rådgivet om, hvilke parametre der bør udløse en smittenotifikation.

For at sikre valide data om smitte i forbindelse med smittenotifikation har STPS valgt at sikre den fornødne smitteverifikation ved, at oplysningerne om smittestatus – hvis borgerne ønsker det – indhentes fra SSI via KID. Dette register indeholder valide data om smittestatus, da oplysningerne herom bygger på test af borgeren. Endvidere har STPS valgt at benytte NemID for at skabe sikkerhed for, at der sker den fornødne sikre identifikation af borgerne.

### *6.3.6 Risiko 6: Risiko for reidentifikation af personoplysninger*

#### *6.3.6.1 Beskrivelse af risiko*

Som nævnt ovenfor vil personoplysningerne, der behandles i løsningen, i vid udstrækning behandles i pseudonymiseret form, hvormed identificeringspotentialet af den enkelte borger er søgt reduceret.

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

Det udgør en risiko, at personoplysningerne ikke pseudonymiseres, eller at pseudonymiserede data mister deres pseudonyme karakter, således at borgerne kan identificeres.

Risikoen for, at en borger kan identificere en anden borger som smittet i forbindelse med kontaktregistreringen på brugernes telefon, er nærmere behandlet som risiko nr. 8 nedenfor.

#### *6.3.6.2 Foranstaltninger til at håndtere risikoen*

Grundet løsningens udformning er det ikke muligt at omgøre selve pseudonymiseringen, da den er designet til at være uigenkaldelig. Dette medfører, at der ikke eksisterer en egentlig nøgle til at omgøre pseudonymiseringen. Dette udgør i sig selv den vigtigste foranstaltning. Hvis det efterfølgende viser sig, at pseudonymiseringen ikke har være sikker nok, vil der foretages en ændring af den underliggende metode. Samtidig er der implementeret slettefrister som gør, at selv hvis pseudonymiseringen brydes, vil der automatisk være begrænsning på, hvor mange persondata, der er omfattet.

Pseudonymiseringen finder sted på brugerens telefon gennem API'et. Metoden, hvorpå pseudonymiseringen foregå, er offentliggjort, og er anerkendt som en sikker metode.

### *6.3.7 Risiko 7: Risiko for, at borgere kan identificere smittede i forbindelse med smittenotifikation*

#### *6.3.7.1 Beskrivelse af risiko*

Borgerne, der bruger appen, vil ikke i forbindelse med smittenotifikation få oplyst, hvilken(n) kontakt(er) der har udgjort en smitterisiko for borgeren, hvis borgeren måtte få en notifikation om, at borgeren har været i kontakt med en smittet, idet oplysningerne behandles i pseudonymiseret form. Hvis borgeren kun har været i kontakt med én anden person inden for de foregående 14 dage, vil borgeren potentielt kunne udlede, hvem den smittede person er. Denne risiko har sammenhæng med risiko 2 om manglende evne til at overskue konsekvenserne af accept til at dele information om smittestatus med andre.

#### *6.3.7.2 Foranstaltninger til at håndtere risiko*

Denne risiko synes uundgåelig – og vil i sagens natur være en følge af enhver kontaktregistrerings- og smitteopsporingsapp – og kan blive realiseret i forhold til de brugere, der alene har ganske få kontakter.[24]

Risikoen vil dog blive søgt reduceret ved, at STPS i appen forud for borgerens samtykke informeres om, at en sådan risiko for identifikation af borgeren foreligger. Derudover indeholder notifikationen til borgeren alene oplysninger om, at borgeren har været i kontakt med en person, der er bekræftet smittet, men ikke oplysninger om tidspunkt eller dato for kontakten. Desuden er der tale om en risiko, der kun vil kunne findes sted i meget få tilfælde og under helt særlige omstændigheder.

[24] Denne risiko synes også anerkendt af Det Europæiske Databeskyttelsesråd i rådets Retningslinjer 04/2020 om brug af lokaliseringsdata og kontaktopsporingsredskaber i forbindelse med covid-19- udbruddet, vedtaget den 21. april 2020, s. 17, hvor følgende anføres: *"PRIV-7 Applikationen bør kun give brugeren viden om, hvorvidt han eller hun er blevet eksponeret for virusset, og — så vidt muligt uden at afsløre noget om andre brugere — hvor mange gange og på hvilke datoer han eller hun er blevet eksponeret."*

### *6.3.8 Risiko 8: Risiko for manglende ophør af behandlingen*

#### *6.3.8.1 Beskrivelse af risiko*

Som beskrevet ovenfor i afsnit **5.5.2** skal alle data slettes, når formålet med Smittestop-appen ikke længere er aktuelt, eller når bekendtgørelse nr. 896 af 17. juni 2020 ophæves. På nuværende tidspunkt ophæves bekendtgørelsen den 31. oktober 2020. Såfremt STPS ikke på dette tidspunkt sørger for at deaktivere appen og slette de oplysninger, der er gemt i backenden, vil dette udgøre en risiko for de registrerede, da der i så fald vil blive behandlet personoplysninger om dem uden deres viden, og dermed uden de har mulighed for at modsætte sig behandlingen. Tilsvarende gælder, hvis kontaktregistreringerne på brugernes telefoner fortsætter på tidspunktet efter, at løsningen ikke længere er aktuel.

#### *6.3.8.2 Foranstaltninger til at håndtere risikoen*

I forbindelse med lukning af løsningen vil der blive gennemført sletning af løsningen i driftsmiljøer, således at der sker et effektivt ophør af behandlingen. Samtidig er der implementeret funktioner som sørger for, at oplysningerne løbende slettes. Data vil derfor automatisk slettes senest 14 dage efter den seneste indsamling.

### *6.3.9 Risiko 9: Manglende opnåelse af formålet med appen*

#### *6.3.9.1 Beskrivelse af risiko*

For at Smittestop-appen er effektiv i forhold til dens formål, nemlig at bidrage til at forebygge og inddæmme udbredelse af COVID-19 ved at bryde smittekæder gennem kontaktregistrering og smittenotifikationer, vil det kræve, at en vis andel af befolkningen downloader og benytter appen. Den påkrævede tilslutningsprocent er dog forbundet med en ikke uvæsentlig usikkerhed. Er tilslutningsprocenten ikke høj nok, vil der være risiko for, at den behandling af personoplysninger, der sker som led i borgernes brug af appen, vil være uforholdsmæssig, fordi formålet med appen ikke opnås i tilstrækkeligt omfang.

#### *6.3.9.2 Foranstaltninger til at håndtere risikoen*

Forud for lanceringen af appen, har STPS foretaget vurderinger af, hvorvidt digitale sporingsapps udgør et effektivt værktøj, og har fundet, at dette er tilfældet. Samtidig har undersøgelse vist, at apps selv ved en lav tilslutningsgrad vil have en positiv effekt. Som beskrevet i afsnit 5.10 vil STPS løbende foretage evalueringer af appen og dens effekt, funktionalitet og datakilder/datakvalitet på baggrund af udviklingen i smitte-spredningen i samfundet, tilslutningsprocenten i befolkningen til appen og den nationale

strategi for genåbningen af Danmark. Fører denne evaluering til, at det i en længere periode må konstateres, at Smittestop-appen ikke lever op til dens formål, vil STPS deaktivere appen og fjerne den fra App Store og Google Play.

#### *6.3.10 Risiko 10: Utilstrækkelige sikkerhedsforanstaltninger*

##### *6.3.10.1 Beskrivelse af risiko*

Se Bilag 1 – Risikovurdering.

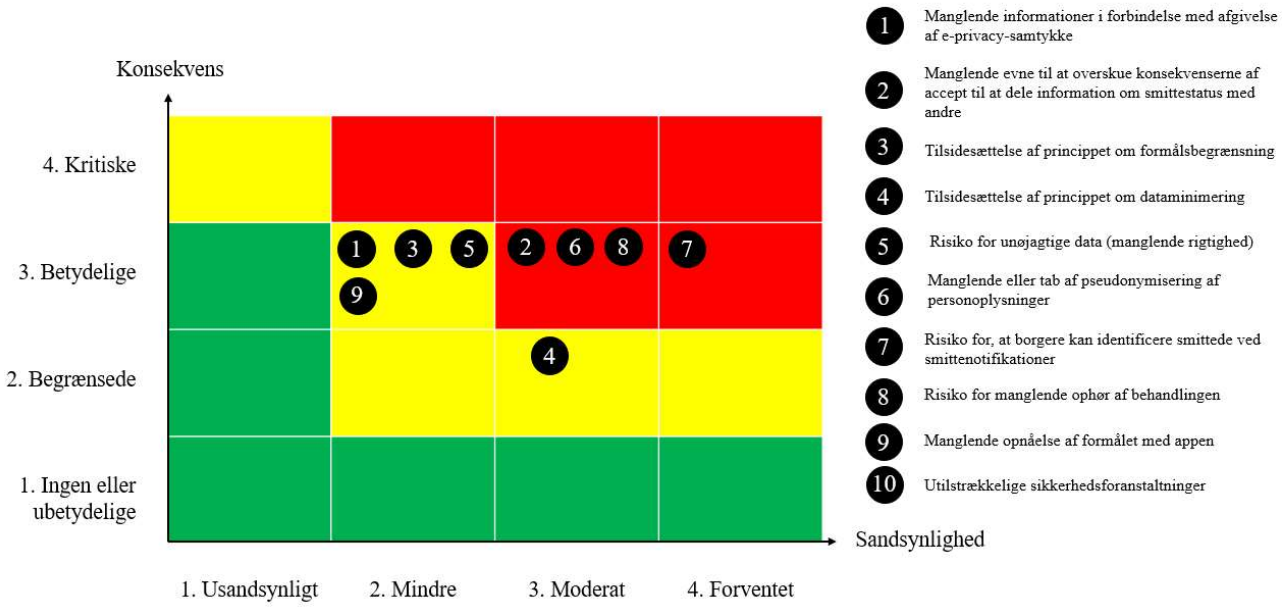
##### *6.3.10.2 Foranstaltninger til at håndtere risikoen*

Se Bilag 1 - Risikovurdering

### 6.4 Evaluering af risici

STPS har herefter evalueret de ovennævnte risici hver især i forhold til deres konsekvenser for de registrerede og sandsynligheden for, at følgerne af risiciene indtræffer. Dette er sket ved brug af evalueringskriterierne nævnt i tabel 1 og 2 i afsnit 6.2 ovenfor. Resultatet af denne vurdering fremgår af risikokortet i figur 4 straks nedenfor.

**Figur 4 Risikokort med overblik over evaluering af risici *før* implementering af mitigerende foranstaltninger**



### 6.5 Overblik over evaluering og håndtering af risici

De ovennævnte risici i risikokortet i figur 4 kan evalueres og håndteres som følger:

*Tabel 3. Overblik over evaluering af risici samt residualrisiko efter implementering af mitigerende foranstaltninger*

| **Risiko nr.** | **Risiko** | **Valg af foranstaltning for at håndtere risiko** | **Effekt på risiko** | **Restrisiko** | **Foranstaltningen er implementeret /under implementering?** |
|---|---|---|---|---|---|
| 1 | Manglende informationer i forbindelse med afgivelse af e-privacy samtykke | Fyldestgørende information til borgeren, som præsenteres for borgeren i løsningen i forbindelse med samtykkeafgivelsen. I øvrigt vil informationen være vedvarende tilgængelig for borgeren i løsningen, så borgeren til enhver tid kan se informationen. | Reduceret | Lav | Vil være implementeret, når appen releases. |
| 2 | Manglende evne til at overskue konsekvenserne af accept til at dele information om smittestatus med andre | Ved accept af delingen gives borgeren oplysninger om, at oplysninger om smittestatus deles med kontakterne i pseudonymiseret form, men at der en risiko for identifikation. Borgeren er dermed, før accepten gives, oplyst om, at der er en risiko for, at borgeren af andre kan identificeres som smittet i forbindelse med smittenotifikationer. | Reduceret | Medium | Vil være implementeret, når appen releases. |

| | | | | | |
|---|---|---|---|---|---|
| 3 | Tilsidesættelse af princippet om formålsbegrænsning | (1) Klare regler om formålsbegrænsning i Smittestop-bekendtgørelse. (2) Design af løsningen som en decentral løsning, hvor kontaktregistrering sker lokalt på brugernes telefoner, uden at STPS har adgang til oplysninger om kontaktregistreringer. (3) Implementering af interne retningslinjer om formålsbegrænsning for så vidt angår de personoplysninger, som STPS har adgang til i forbindelse med de centrale behandlingsaktiviteter i form af smitteverifikation og -notifikation og lagringen af disse oplysninger i denne forbindelse. | Reduceret | Lav | Vil være implementeret, når appen releases. |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Tilsidesættelse af princippet om dataminimering | (1) Design af løsningen som en decentral løsning, hvor kontaktregistrering sker lokalt på brugernes telefoner, uden at STPS har adgang til oplysninger om kontaktregistreringer. (2) Fokus på dataminimering i forbindelse med design af løsningen, herunder i forbindelse med kontaktregistreringen og behandling af personoplysninger centralt hos STPS i forbindelse med smitteverifikation og -notifikation. (3) Ingen behandling af lokationsdata. | Reduceret | Lav | Vil være implementeret, når appen releases. |
| 5 | Risiko for unøjagtige data (manglende rigtighed) | Design af løsningen med indbygget smitteverifikation, hvorefter oplysning om en brugers smittestatus importeres fra KID, der er den database, hvor smittestatus for alle borgere i landet registreres. Smittestatus bygger hermed på lægefaglig vurdering / test. | Reduceret | Lav | Vil være implementeret, når appen releases. |

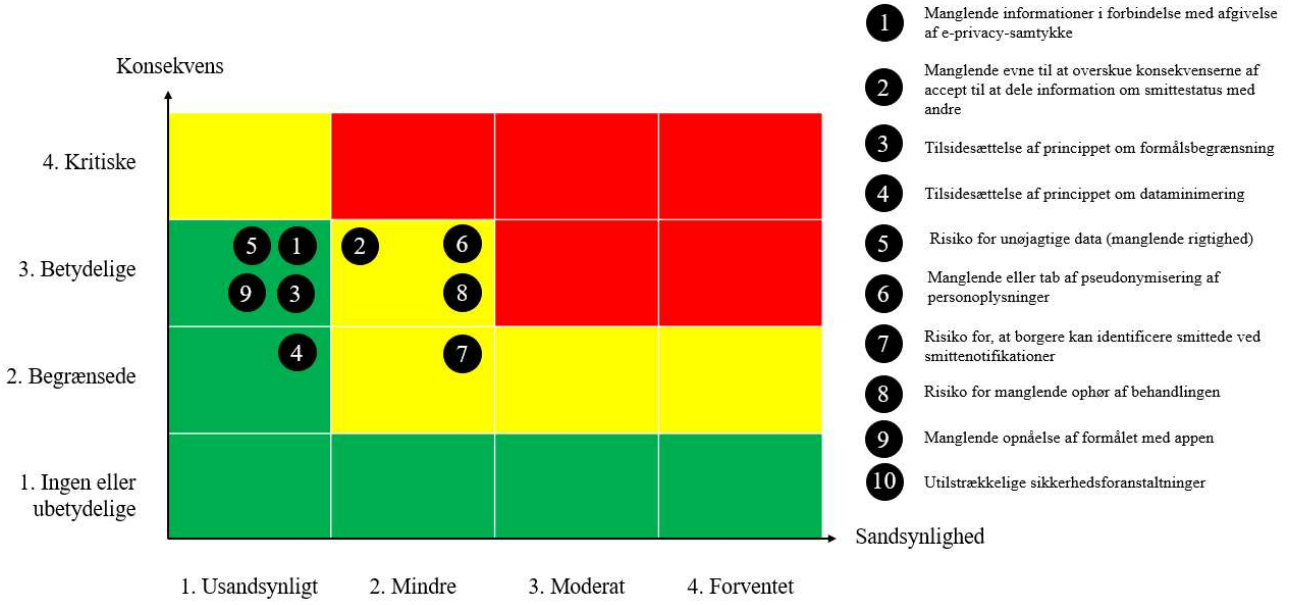
| | | | | | |
|---|---|---|---|---|---|
| 6 | Reidentifikation af personoplysninger | Grundet løsningens udformning er det ikke muligt at omgøre selve pseudonymiseringen, da den er designet til at være uigenkaldelig. Dette medfører, at der ikke eksisterer en egentlig nøgle til at omgøre pseudonymiseringen. Dette udgør i sig selv den vigtigste foranstaltning. Hvis det efterfølgende viser sig, at pseudonymiseringen ikke har være sikker nok, vil der foretages en ændring af den underliggende metode. Samtidig er der implementeret slettefristrer som gør, at selv hvis pseudonymiseringen brydes, vil der være begrænsning på, hvor mange persondata, der er omfattet. | Undgået | Lav | Vil være implementeret, når appen releases. |

| | | | | | |
|---|---|---|---|---|---|
| 7 | Risiko for, at borgeren kan identificere andre smittede | STPS vil i appen forud for borgerens samtykke informeres om, at en sådan risiko for identifikation af borgeren foreligger. Derudover indeholder notifikationen til borgeren alene oplysninger om, at borgeren har været i kontakt med en person, der er bekræftet smittet, men ikke oplysninger om tidspunkt eller dato for kontakten. | Accepteret | Medium | Vil være implementeret, når appen releases. |
| 8 | Risiko for manglende ophør af behandlingen | I forbindelse med lukning af løsningen gennemføres fjernelse fra App Store og Google Play, løsningen afinstalleres og data slettes i back end. Data på brugernes telefoner slettes i overensstemmelse med sletteprocedurerne. | | Lav | Vil gennemføres, når appen lukkes. |

| | | | | | |
|---|---|---|---|---|---|
| 9 | Manglende opnåelse af formålet med appen | STPS vil løbende foretage evaluering af appen og dens effekt, funktionalitet og datakilder/datakvalitet på baggrund af udviklingen i smitte-spredningen i samfundet, tilslutningsprocenten i befolkningen til appen og den nationale strategi for genåbningen af Danmark. Fører denne evaluering til, at det i en længere periode må konstateres, at Smittestop-appen ikke lever op til dens formål, vil STPS deaktivere appen og fjerne den fra App Store og Google Play. | Reduceret | Lav | Vil ske forudgående for lancering og løbende i appens levetid. |

Således vil risikokortet for de ovennævnte risici *efter* implementering af mitigerende foranstaltninger efter STPS' vurdering se ud som følger:

**Figur 5 Risikokort med overblik over evaluering af risici *efter* implementering af mitigerende foranstaltninger**




Det er således STPS' vurdering, at samtlige risici efter risikomitigeringen er reduceret i et tilstrækkeligt omfang, således at der ikke (længere) er tale om en høj risiko for de registrerede. De ovennævnte foranstaltninger vil blive implementeret hurtigst muligt og inden idriftsættelse af løsningen. Dog vil endelig sletning af app og data først gennemføres, når appen ikke længere skal anvendes.

### 6.6 Samlet residualrisiko

Som det fremgår af tabel 3 i punkt 6.5 ovenfor, er den samlede residualrisiko forbundet med behandlingen af personoplysningerne i Smittestop-appen **lav-mellem**. Tilsvarende gælder residualrisikoen i risikovurderingen vedrørende behandlingssikkerhed efter databeskyttelsesforordningens artikel 32 (**Bilag 1 - Risikovurdering**), hvor residualrisikoen for den registrerede samlet set er **lav-mellem**.

## 7. EVENTUEL HØRING AF DATATILSYNET VED HØJ RESIDUALRISIKO

Den dataansvarlige har pligt til at foretage en forudgående høring af Datatilsynet, inden påbegyndelsen af en påtænkt behandling af personoplysninger, hvis konsekvensanalysen viser, at behandlingen vil føre til en høj risiko, og den dataansvarlige ikke kan begrænse denne høje risiko ved indførelse af passende foranstaltninger, jf. databeskyttelsesforordningens artikel 36.

Som det fremgår ovenfor i punkt 6.6, er det STPS' vurdering, at den samlede residualrisiko – dvs. risikobilledet *efter* implementering af foranstaltninger til at imødegå de identificerede risici – er **lav-mellem**. Der er således ingen risici i løsningen, der fortsat er høj, efter STPS' mitigering af risici.

Det er på denne baggrund STPS' vurdering, at STPS ikke har pligt til at foretage en forudgående høring af Datatilsynet.

## 8. DOKUMENTATION AF DPO'ENS SYNSPUNKTER

Databeskyttelsesrådgiveren for Sundheds- og Ældreministeriet har været inddraget i processen med udarbejdelsen af denne konsekvensanalyse vedrørende databeskyttelse med bilag og har kommet med en række kommentarer hertil, som STPS løbende har forholdt sig til og inddraget i vurderingen.

Databeskyttelsesrådgiveren har løbende givet bemærkninger til de forskellige udkast og versioner af DPIA'en.

## 9. LEDELSENS GODKENDELSE AF KONSEKVENSANALYSEN

Ledelsens beslutning vedrørende konsekvensanalysen:

*Tabel 4. Ledelsens godkendelsesskema*

| **Beslutning** | **Beskrivelse** | **Sæt kryds** |
|---|---|---|
| **Godkendt** | Behandlingen kan herefter påbegyndes, såfremt de i konsekvensanalysen mitigerende foranstaltninger bliver implementeret. | |
| **Betinget godkendt** | Behandlingen kan alene påbegyndes, såfremt nærmere beskrevne ændringer foretages. Der skal derfor fremlægges en revideret konsekvensanalysen for ledelsen med henblik på endelig godkendelse. | |
| **Ikke godkendt** | Behandlingen gennemføres ikke. | |

## 10. VEDLIGEHOLDELSE OG AJOURFØRING AF KONSEKVENSANALYSEN

STPS skal som dataansvarlig regelmæssigt gennemgå konsekvensanalysen vedrørende databeskyttelse og de behandlingsaktiviteter, som vurderes i denne, jf. databeskyttelsesforordningens artikel 35, stk. 11. Det skal som minimum ske, når der sker en ændring af risikoen ved behandlingen af aktiviteten. For at kunne leve op til det grundlæggende princip om ansvarlighed, skal det dokumenteres i konsekvensanalysen, hvem der er ansvarlig for at revidere og ajourføre konsekvensanalysen. Derudover skal det regelmæssigt anføres i konsekvensanalysen, hvilken kontrol og ajourføring der er sket. DPO'en bør også involveres i ajourføringen.

Denne konsekvensanalyse vil løbende blive revideret og ajourført i lyset af ovenstående samt som følge af de skriftlige evalueringer af appen, der løbende vil blive foretaget af STPS, jf. nærmere herom ovenfor afsnit 5.11.

Konsekvensanalysen vil endvidere blive revideret, såfremt STPS måtte beslutte at introducere nye releases med yderligere funktionaliteter i appen.

Denne konsekvensanalyse vedrørende databeskyttelse ajourføres af (navn og titel):
Mads Rugård Lerstrup, DPA

## 11. BILAG

Bilag 1: Risikovurdering
Bilag 2: Smitteflow.pdf
Bilag 3: Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf
Bilag 4: EN App dataflow.pdf
Bilag 5: Kommissorium for Advisory Board